UNIVERSITÀ DEGLI STUDI DI SASSARI
DIPARTIMENTO DI GIURISPRUDENZA
Dottorato di Ricerca in Scienze Giuridiche

Ciclo XXXVII

INTELLIGENZA ARTIFICIALE E RESPONSABILITÀ PENALE:

tra tutela dei diritti fondamentali e nuove forme di colpevolezza.

Tutor

Prof. Gian Paolo Demuro

Candidata

Chiara Cuccuru

A.A. 2023/2024

SOMMARIO

Introduzione

Viviamo in un'epoca in cui l'attenzione verso le tecnologie di intelligenza artificiale è al suo apice, alimentata dai progressi raggiunti nella seconda metà del decennio scorso. Un tempo ritenuta un concetto esclusivamente fantascientifico, l'IA ha ormai raggiunto una diffusione tale da impattare diversi settori della società, compreso quello giuridico. Questa pervasività ha portato a numerosi interrogativi sulla sua compatibilità con il diritto, in particolare con quello penale, dove l'intelligenza artificiale solleva problematiche di notevole rilevanza.

Il crescente interesse per l'IA non proviene solo dai *media*, i quali talvolta abusano del termine applicandolo a tecnologie che non sono propriamente intelligenti, ma coinvolge anche il mondo accademico e scientifico, dove l'IA è al centro di studi non solo tecnologici e ingegneristici, ma anche antropologici, filosofici, psicologici e giuridici.

La progressiva automazione di attività tradizionalmente svolte dall'essere umano e la diffusione di tecnologie nei contesti più vari - dalla mobilità alla sanità, dalla giustizia al mondo produttivo - pongono una serie di interrogativi complessi nell'ambito del diritto: come qualificare giuridicamente le condotte realizzate da sistemi di IA, soprattutto quando queste possono arrecare danni a persone o beni?

Il presente lavoro si inserisce proprio in questo contesto, esaminando le conseguenze dell'avvento dell'intelligenza artificiale sul diritto, iniziando da un'analisi delle sue possibili definizioni, della storia e delle principali caratteristiche tecniche.

Parallelamente, è stato necessario esaminare il lavoro dei gruppi di esperti incaricati di esplorare le implicazioni etiche, giuridiche e sociali che potrebbero derivare dallo sviluppo dell'intelligenza artificiale. Le Linee guida etiche per un'IA affidabile, emanate dalla Commissione Europea, rappresentano un esempio di come esperti di diverse discipline siano coinvolti in un dibattito che mira a regolare l'uso delle nuove tecnologie in modo responsabile.

La tesi si divide in tre parti. La prima è dedicata alla ricostruzione storica e tecnica dell'intelligenza artificiale e alla presentazione delle principali proposte di regolamentazione.

L'IA è generalmente definita come l'insieme di sistemi capaci di simulare processi cognitivi umani come l'apprendimento, il ragionamento e la risoluzione dei problemi. Al contrario di altre forme di automazione che operano su base predefinita, è in grado di adattarsi autonomamente e di migliorare le proprie *performance* attraverso l'esperienza. Questo elemento distintivo crea una netta frattura tra l'IA e le tecnologie tradizionali, rendendo molto più complessa la regolamentazione di questi nuovi sistemi.

Dal punto di vista storico, possiamo notare che con l'industrializzazione il diritto ha dovuto affrontare nuove questioni legate alla responsabilità per i difetti dei prodotti e per le macchine pericolose. In modo analogo, il progresso tecnologico odierno, guidato dall'IA, sta costringendo il diritto penale a ripensare le proprie categorie fondamentali.

L'Unione Europea è uno degli attori principali nella pianificazione normativa di questo settore. Il Regolamento generale sulla protezione dei dati (GDPR)[1] e il Regolamento sull'intelligenza artificiale (*AI Act*)[2] rappresentano due importanti iniziative in questo ambito, che mirano a disciplinare l'uso delle tecnologie basate sull'IA in modo da garantire la tutela dei diritti degli individui.

Il GDPR, in particolare, dedica attenzione al tema del processo decisionale automatizzato nell'art. 22 e nel Considerando 71, dove vengono stabilite alcune garanzie per gli individui sottoposti a decisioni prese con l'ausilio di sistemi intelligenti. L'*AI Act*, invece, affronta la questione in modo più dettagliato, concentrandosi sugli *standard* tecnici e sulle procedure di controllo per ridurre al minimo i rischi di discriminazione e di errore. Stabilisce, inoltre, che i sistemi di intelligenza artificiale debbano essere progettati in modo da rispettare determinati requisiti, come l'uso di *dataset* di

[1] Regolamento UE n. 2016/679, adottato il 27 aprile 2016.

[2] Regolamento UE n. 2024/1689, adottato il 13 giugno 2024.

qualità e l'implementazione di misure volte a minimizzare i *bias*[3]. Questo approccio si concentra principalmente sulla prevenzione dei rischi a monte, attraverso una regolamentazione più stringente dei processi di sviluppo e implementazione delle tecnologie di IA.

Entrambi i regolamenti citati, tuttavia, presentano alcune limitazioni. Il GDPR non risolve il problema dell'opacità degli algoritmi e della difficoltà, per gli operatori umani, di comprendere pienamente il funzionamento dei sistemi di IA. Inoltre, le eccezioni previste dal citato art. 22, che consentono l'uso di decisioni totalmente automatizzate in alcuni casi, possono minare la protezione offerta agli individui. D'altra parte, l'*AI Act*, pur puntando a minimizzare i rischi attraverso norme tecniche, non affronta completamente la questione del controllo umano, né garantisce una piena trasparenza nel funzionamento degli algoritmi utilizzati.

Uno degli aspetti tecnici più problematici che verrà analizzato nel primo capitolo riguarda proprio il fatto che i meccanismi che operano all'interno di questi sistemi artificiali il più delle volte non sono di facile interpretazione. Questa mancanza di trasparenza rende estremamente difficile valutare la validità delle decisioni prese dall'algoritmo, sollevando dubbi sulla legittimità di un loro impiego nei procedimenti legali.

La seconda parte esplora le sfide che l'IA determina con riguardo ai diritti fondamentali, rivolgendo l'attenzione, inizialmente, verso la sfera dell'identità personale. Le tecnologie intelligenti sembrano esercitare una forma di condizionamento inedita sulla formazione della personalità, influenzando gusti, preferenze e comportamenti dell'individuo. La profilazione degli utenti e la personalizzazione dei contenuti rappresentano solo alcuni degli strumenti attraverso i quali l'IA sta modificando il modo in cui le persone interagiscono con il mondo circostante, sollevando preoccupazioni riguardo alla libertà di sviluppo della personalità.

[3] Come verrà spiegato in seguito, il *bias* può essere definito come qualsiasi deviazione da un punto di vista imparziale o da uno *standard* di oggettività. Si tratta di pregiudizi che portano a una visione distorta o parziale della realtà, influenzando il giudizio o il comportamento. In particolare, *bias* algoritmici si riferiscono a pregiudizi o distorsioni che emergono durante lo sviluppo e l'utilizzo di sistemi di intelligenza artificiale, idonei a influenzare il funzionamento degli algoritmi e portare a decisioni o risultati distorti, spesso senza che gli sviluppatori o gli utenti ne siano consapevoli.

Si esaminerà anche l'impatto dell'intelligenza artificiale sulla libertà di espressione. Molti ritennero che l'avvento delle prime forme di *internet* interattivo, che consentivano la diffusione di contenuti generati o condivisi dagli utenti, costituissero una nuova forma di libertà espressiva per l'individuo, capace di raggiungere un pubblico vasto e globale, impensabile prima dell'era digitale. Tuttavia, lo sviluppo dei *social network* ha mostrato un altro aspetto della questione: la ripetuta diffusione di notizie false e contenuti problematici – in alcuni casi apertamente illegali – ha compromesso i tradizionali meccanismi di credibilità che caratterizzavano il mercato dell'informazione.

A partire da questa constatazione, il lavoro esamina il quadro prescrittivo attuale, che esonera gli intermediari di *internet* da una responsabilità generalizzata per i contenuti pubblicati dagli utenti. Lo studio, inoltre, esplora le strategie normative che potrebbero essere adottate per adeguare la legislazione alla nuova realtà descritta, allo scopo di garantire, da un lato, l'effettiva libertà di espressione, e, dall'altro, la protezione dell'ordine pubblico e della tenuta del sistema democratico, minacciati dalle manipolazioni del discorso pubblico sui *social network*.

La seconda parte del presente lavoro analizza anche l'impatto delle tecnologie intelligenti sulla realizzazione del principio di uguaglianza. Al centro di questo approfondimento vi è il concetto di *bias* algoritmico, che ha attirato sempre più l'attenzione della letteratura scientifica, e identifica ogni forma di discriminazione che nasce dall'impiego di sistemi di IA, generalmente basati sull'analisi dei dati attraverso strumenti di apprendimento automatico.

Questi effetti discriminatori possono essere il risultato di molteplici fattori, come errori nella progettazione o la presenza, nei dati utilizzati per addestrare l'algoritmo, di distorsioni che riflettono quelle già presenti nella società. Così, un sistema intelligente che viene addestrato su dati raccolti in una società diseguale finirà inevitabilmente per riprodurre tali disuguaglianze con l'accuratezza che caratterizza i suoi risultati. Tali discriminazioni possono inoltre risultare difficili da individuare, poiché coperte dalla percezione di oggettività che spesso circonda le tecnologie avanzate.

Un esempio che verrà citato nel corso del lavoro è quello degli algoritmi utilizzati negli Stati Uniti per valutare il rischio di recidiva da parte dei detenuti. È stato

dimostrato che tali sistemi tendono a sovrastimare il rischio di recidiva per gli imputati afroamericani rispetto a quelli caucasici, a parità di circostanze. Questo accade perché i dati utilizzati per addestrare il sistema riflettono una storia di ingiustizie razziali, che l'algoritmo non è in grado di correggere autonomamente.

Il terzo capitolo, infine, esplora il tema della responsabilità penale in relazione alla mobilità avanzata. Viene analizzato lo stato dell'arte e le conseguenze etiche e legali che derivano dall'uso di queste tecnologie. Si discute anche della configurabilità di una responsabilità penale per i sistemi di intelligenza artificiale e delle teorie dottrinali al riguardo, come l'interrogativo "*machina delinquere potest?*" e la possibilità di configurare responsabilità diretta per sistemi autonomi.

Nella prospettiva del diritto penale, l'utilizzo di sistemi di intelligenza artificiale pone, infatti alcune questioni fondamentali: chi è il responsabile per le azioni compiute da una macchina? In che misura l'autonomia di un sistema può influire sulla valutazione della colpevolezza? Può l'IA essere imputabile di un reato? Si tratta di domande che richiedono risposte dettagliate e che, allo stato attuale, non trovano soluzioni soddisfacenti all'interno dei quadri normativi vigenti.

Il diritto penale, tradizionalmente strutturato attorno alla responsabilità personale dell'individuo per i propri atti, si trova oggi di fronte ad una sfida. I sistemi di IA possono operare in modo apparentemente autonomo, con scelte che possono avere conseguenze molto gravi per gli individui, come dimostrato dai numerosi casi di *bias* algoritmico e di decisioni discriminatorie emerse negli ultimi anni.

A livello teorico, il dibattito si divide tra chi propone di estendere le attuali categorie di responsabilità penale, includendo chi crea o utilizza sistemi di IA, e chi, come il giurista Gabriel Hallevy, ha proposto modelli alternativi per inquadrare la responsabilità penale in contesti di IA, distinguendo tra situazioni in cui la tecnologia è uno strumento utilizzato da un essere umano per commettere un reato e casi in cui agisce in maniera autonoma, sollevando il problema dell'attribuzione di responsabilità in assenza di un chiaro coinvolgimento diretto dell'uomo.

Il concetto di autonomia decisionale è alla base delle sfide giuridiche poste dall'IA. Un algoritmo che decide autonomamente come risolvere un problema non è

soltanto uno strumento nelle mani di chi lo utilizza; ci si deve chiedere se esso diventi, in una certa misura, un soggetto di diritto.

A differenza delle tecnologie tradizionali, che si limitano ad eseguire istruzioni predefinite, i sistemi di IA hanno la capacità di apprendere e adattarsi. Questo aspetto li rende molto più complessi da regolamentare rispetto a macchinari o *software standard*. Ad esempio, un veicolo autonomo dotato di IA può prendere decisioni immediate basate su *input* esterni (traffico, condizioni metereologiche, etc.), che non erano state previste in fase di programmazione.

Questo aspetto è di fondamentale importanza nel contesto giuridico. La responsabilità penale richiede non solo l'accertamento di un atto illecito, ma anche la dimostrazione della colpevolezza dell'autore. Nel caso di un algoritmo, non esiste una colpevolezza in senso stretto, poiché il sistema allo stato attuale non ha la capacità di comprendere le conseguenze morali delle proprie azioni.

Tuttavia, vi è il rischio che le decisioni prese dall'IA possano avere conseguenze molto gravi per gli individui coinvolti, e necessitano, pertanto, di un adeguato quadro sanzionatorio. Per questo motivo, è opportuno trovare un equilibrio tra il riconoscimento dell'indipendenza decisionale dell'IA e l'attribuzione della responsabilità per gli errori commessi dai sistemi autonomi.

Capitolo 1
L'intelligenza artificiale. Storia e fonti.

1. Nascita e sviluppo dell'intelligenza artificiale

L'intelligenza artificiale (IA) rappresenta una delle innovazioni tecnologiche più significative del nostro tempo. La sua evoluzione, iniziata nella metà del XX secolo, ha portato ad una trasformazione radicale in numerosi settori, sollevando contestualmente questioni giuridiche complesse.

Dal punto di vista dell'informatica, l'intelligenza artificiale è quella disciplina che si occupa dello studio e della progettazione di sistemi *hardware* e *software* capaci di eseguire compiti che normalmente sono prerogativa dell'intelligenza umana. Questo comprende l'apprendimento, il ragionamento, la pianificazione, la comprensione del linguaggio naturale, il riconoscimento visivo, e molto altro.

Quanto al termine stesso «intelligenza artificiale», viene utilizzato e coniato per la prima volta nel 1956, durante una conferenza organizzata presso il Dartmouth College negli Stati Uniti, dove uno degli organizzatori, John McCarthy[1] parlò per la prima volta di *artificial intelligence*. Tuttavia, la storia dell'intelligenza artificiale non inizia solo dopo il 1956, ma include anche la cibernetica e i primi calcolatori elettronici.

Il primo esempio di IA è rappresentato dalla macchina aritmetica inventata nel 1642 da Blaise Pascal[2]. Questo strumento, pensato per semplificare i calcoli contabili,

[1] John McCarthy è stato un informatico statunitense che vinse il Premio Turing nel 1971 per i suoi contributi nel campo dell'intelligenza artificiale, della quale è considerato il fondatore proprio per averne coniato il termine. Fu una delle figure più rilevanti per lo studio e lo sviluppo dell'intera materia.

[2] Blaise Pascal fu un matematico, fisico, e filosofo francese, noto soprattutto per il «triangolo di Pascal» in matematica e i suoi studi sulla pressione in fisica. È anche ricordato per i suoi scritti filosofici e teologici, come i «Pensieri». Per un approfondimento sulla macchina aritmetica e sulla figura di Pascal si veda P. GRAZIANI, M. SANGOI, *La macchina aritmetica di Blaise Pascal*, in *Isonomia*, Istituto di Filosofia dell'Università di Urbino, 2005.

permetteva di eseguire operazioni matematiche senza la necessità di conoscere le regole dell'aritmetica e con un ridotto margine di errore.

Già prima della conferenza del '56 gli studiosi cercarono di creare sistemi artificiali capaci di emulare i fenomeni dell'intelligenza umana, e questo sistema venne inizialmente chiamato elaboratore. Alla base dell'elaboratore vi è il concetto di macchina di Turing[3], un modello teorico che può simulare qualsiasi algoritmo o processo computabile, ed è considerato un precursore dei *computer* moderni.

Il contributo di Turing all'intelligenza artificiale è significativo non solo per i fondamenti dell'informatica, ma anche per il dibattito filosofico sui limiti e le potenzialità delle macchine pensanti. In un celebre articolo del 1950, dal titolo «*Computing Machinery and Intelligence*», Turing propose il test che porta il suo nome per verificare la presenza di intelligenza in una macchina e capire se essa fosse in grado di pensare e ragionare come un essere umano[4].

È importante riconoscere come l'intelligenza artificiale abbia ereditato molte idee, punti di vista e tecniche da altre discipline, in particolare dalla filosofia, dalla matematica e dalla psicologia. Dalla filosofia derivano i risultati relativi al dibattito sulla natura dell'intelligenza e della razionalità; dalla matematica l'approccio formale basato sulla logica; dalla psicologia l'analisi delle relazioni tra conoscenza e azione.

Fino al ventesimo secolo la formalizzazione delle scienze e della matematica creò le condizioni per lo studio dell'intelligenza e delle sue possibili artificializzazioni.

---

[3] Alan Turing è stato un matematico britannico, considerato uno dei padri fondatori dell'informatica moderna e dell'intelligenza artificiale. Nel 1936 introdusse il concetto di una macchina astratta, nota oggi come macchina di Turing, che è alla base della teoria della computazione. Si tratta di un sistema teorico in grado di eseguire un numero limitato di azioni, permettendo di esprimere qualsiasi tipo di procedura definita. La macchina di Turing è costituita da un nastro infinito suddiviso in celle, che vengono lette da una testina capace di muoversi avanti o indietro, e da un'unità di controllo che legge il simbolo presente nella cella sotto la testina. In ogni momento, l'azione della macchina è determinata dal simbolo letto e dallo stato attuale della macchina. Dopo aver letto il simbolo, la testina può compiere due operazioni alternative: lasciare il simbolo intatto oppure cancellarlo e sostituirlo con un altro simbolo. Il concetto di algoritmo si può ricondurre alla sequenza di operazioni eseguite dalla macchina di Turing. Quest'ultimo ha dimostrato che alcuni problemi matematici sono non computabili, ovvero non possono essere risolti attraverso un algoritmo. Per un approfondimento si veda M. CAPPELLI, voce *Macchina di Turing*, in *Enc. della Scienza e della Tecnica*, 2008.

[4] Cfr. A.M. TURING, *Computing machinery and intelligence*, in *Mind – A Quarterly Review of Psychology and Philosophy*, LIX, 236, 1950, p. 433 ss.

Tuttavia, fu solo con l'avvento dei primi elaboratori elettronici, durante la Seconda guerra mondiale, che questo interesse prese una direzione concreta.

Negli anni '40 la cibernetica iniziò a studiare sistematicamente i processi di comunicazione e controllo negli animali e nelle macchine. Nel 1943, Warren S. McCulloch e Walter Pitts proposero il primo modello di neuroni artificiali[5], basato sulla fisiologia neuronale, la logica proposizionale e la teoria della computabilità di Alan Turing. L'idea era di studiare i meccanismi di autoregolazione e controllo negli organismi viventi e nelle macchine con retroazione, capaci di rispondere in modo adattativo alle sollecitazioni ambientali. Uno dei risultati più significativi mostrò che ogni funzione calcolabile poteva essere elaborata da una rete di neuroni connessi. Nel 1949, Donald O. Hebb dimostrò come una semplice regola di aggiornamento delle connessioni neuronali potesse portare a processi di apprendimento[6].

Vi furono anche esempi di sistemi intelligenti utilizzati a scopi bellici. ENIAC (*Electronic Numerical Integrator and Computer*) è stato il primo computer elettronico *general-purpose*[7], costruito negli Stati Uniti e completato nel 1945. Progettato per eseguire calcoli balistici per l'esercito durante la Seconda Guerra Mondiale, l'ENIAC era una macchina di grandi dimensioni e molto complessa, composta da oltre 17.000 valvole termoioniche. Rappresenta una pietra miliare nella storia dell'informatica, segnando l'inizio dell'era dei computer digitali.

Nonostante questi successi, la cibernetica perse rilevanza negli anni Cinquanta a causa delle crescenti prestazioni dell'informatica e della limitazione degli obiettivi iniziali, e di conseguenza le risorse furono dirottate sull'intelligenza artificiale.

Il passo successivo fu la già citata conferenza del 1956. Nell'estate di quell'anno, un gruppo di studiosi si riunì al Dartmouth College con l'obiettivo di esaminare la

---

[5] W.S. MCCULLOCH, W. PITTS, *A logical calculus of the ideas immanent in nervous activity*, in *Bulletin of Mathematical Biophysics*, 5/1943, p. 115 ss.

[6] D.O. HEBB, *The organization of behavior; a neuropsychological theory*, Wiley, New York, 1949.

[7] *General-purpose* significa a scopo generale o per uso generale. Nel contesto dell'informatica, un dispositivo o un sistema *general-purpose* è progettato per eseguire una vasta gamma di compiti o applicazioni, anziché essere limitato a una funzione specifica. Un *computer general-purpose*, come l'ENIAC, può eseguire qualsiasi tipo di calcolo o processo per cui sia stato programmato, fattore che lo rende versatile e adattabile a diverse esigenze.

congettura, espressa nella proposta del seminario redatta l'anno precedente, secondo cui ogni aspetto dell'intelligenza potesse essere descritto in modo così preciso da permettere a una macchina di simularlo. Durante questa conferenza, per la prima volta, fu proposto di studiare la possibilità che le macchine potessero risolvere problemi che, fino a quel momento, erano stati considerati esclusivo appannaggio dell'intelligenza umana. Questa data segnò l'inizio ufficiale di una nuova disciplina, che il matematico John McCarthy propose di chiamare intelligenza artificiale[8].

Il seminario aveva le caratteristiche di un *brainstorming*, ossia di un dibattito aperto e poco strutturato, dal quale emerse un nuovo approccio teorico volto a definire la possibilità di riprodurre l'intelligenza mediante un elaboratore elettronico. Inoltre, il seminario si proponeva di raccogliere e analizzare programmi con prestazioni definibili come intelligenti, come il *Logic Theorist* (LT) di Allen Newell, Bernard Shaw e Herbert A. Simon, capace di dimostrare teoremi della logica del primo ordine[9]. Gli organizzatori fissarono anche una serie di obiettivi ambiziosi, che avrebbero dovuto essere verificati in un nuovo incontro dieci anni dopo.

Negli anni successivi alla conferenza di Dartmouth gli studiosi dell'IA si concentrarono sulla creazione di sistemi intelligenti che riproducessero i processi cognitivi in modo quanto più fedele possibile all'intelligenza umana.

Possiamo ricordare, ad esempio, il sistema *ELIZA* di Joseph Weizenbaum, un programma di elaborazione del linguaggio naturale che agiva come se fosse uno psicoterapeuta. Alcuni pazienti furono ingannati dalla macchina, in quanto convinti di parlare con un essere umano e non con un *computer*. Tuttavia, il programma non era capace davvero di assimilare le questioni poste dai pazienti, ma forniva risposte preimpostate che si basavano su alcune parole chiave[10]. Dopo questa esperienza si iniziò a

[8] Gli altri organizzatori erano Marvin Minsky, ricercatore di matematica e neurologia ad Harvard; Nathaniel Rochester, direttore della ricerca sull'informazione presso un centro ricerche dell'IBM; e Claude E. Shannon, il matematico già celebre per la teoria dell'informazione.

[9] *Logic Theorist* è stato il primo programma progettato appositamente per eseguire un ragionamento automatico, ha dimostrato 38 dei primi 52 teoremi di *Principia Mathematica,* il lavoro di tre volumi sulle basi della matematica scritto da matematico-filosofi Alfred North Whitehead e Bertrand Russell e pubblicato nel 1910, 1912 e 1913.

[10] J. WEIZENBAUM, *ELIZA – a computer program for the study of natural language communication between man and machine,* Massachussets Istitute of Technology, Cambridge, Mass, 1966. Nel testo viene

pensare che fosse ancora troppo presto per replicare il pensiero e il ragionamento umano. Nonostante l'ottimismo iniziale, infatti, le limitazioni tecnologiche dell'epoca presto divennero evidenti. I *computer* erano lenti e avevano una capacità di memoria molto limitata rispetto agli *standard* odierni. Le aspettative iniziali si scontrarono con la complessità dei problemi da risolvere e la limitata capacità computazionale disponibile. Questo portò a un periodo di riflessione e ridimensionamento delle ambizioni, noto come «Inverno dell'IA», un periodo durante il quale i finanziamenti e l'interesse per l'intelligenza artificiale diminuirono significativamente[11].

Nonostante le difficoltà, la ricerca continuò, ma gli studiosi si concentrarono su sistemi più semplici e specifici per ogni settore, con compiti più limitati e basati sull'elaborazione dei dati.

Durante questo periodo, una delle innovazioni più significative fu lo sviluppo dei sistemi esperti, progettati per emulare il processo decisionale di un esperto umano in un campo specifico, e quindi risolvere problemi complessi o prendere decisioni in un determinato settore. I sistemi esperti erano programmi progettati. Uno dei primi e più noti fu *MYCIN*, una macchina creata negli anni 70 per scomporre i dati relativi alle analisi del sangue ed effettuare diagnosi specifiche sulle infezioni batteriche, proponendo anche un'ipotesi di terapia[12].

---

esplicato il funzionamento del sistema: «*ELIZA is a program operating within the MAC time-sharing system at MIT which makes certain kinds of natural language conversation between man and computer possible. Input sentences are analyzed on the basis of decomposition rules which are triggered by key words appearing in the input text. Responses are generated by reassembly rules associated with selected decomposition rules. The fundamental technical problems with which ELIZA is concerned are: 1) the identification of key words, 2) the discovery of minimal context, 3) the choice of appropriate transformations, 4) generation of responses in the absence of key words, and 5) the provision of an editing capability for ELIZA "scripts". A discussion of some psychological issues relevant to the ELIZA approach as well as of future developments concludes the paper*».

[11] L'espressione «inverno dell'IA» («*AI winter*») è stata utilizzata per la prima volta negli anni '80, ed è attribuita a ricercatori e osservatori del settore per descrivere periodi di declino o disillusione nella ricerca sull'intelligenza artificiale. Uno dei primi ad usarla è stato John McCarthy, ma non è chiaro se sia stato lui a coniare il termine, anche se è noto per aver discusso apertamente delle sfide dell'IA. Il termine è diventato popolare proprio per descrivere il contrasto tra l'euforia iniziale e la successiva mancanza di progressi significativi, portando a una riduzione dell'interesse e degli investimenti nel campo.

[12] *MYCIN* è un famoso sistema esperto sviluppato nei primi anni '70 presso la Stanford *University* per aiutare i medici a diagnosticare e trattare infezioni batteriche, in particolare la meningite e la sepsi. È uno dei primi esempi di successo nell'applicazione dell'intelligenza artificiale alla medicina.

I sistemi esperti rappresentarono una svolta significativa perché dimostrarono che l'IA poteva essere applicata con successo a problemi reali e complessi, anche se in domini ristretti. Questo approccio si basava su regole e conoscenze specifiche inserite nel sistema, piuttosto che su algoritmi generali di apprendimento.

L'utilizzo di sistemi esperti negli anni '70 e '80, accompagnato dall'introduzione delle reti neurali[13], contribuì a riaccendere l'interesse per l'IA e a dimostrare il suo potenziale pratico.

Negli anni 90 l'interesse per l'IA riprende ulteriormente vigore con l'aumento delle capacità computazionali e il miglioramento degli algoritmi. *IBM Deep Blue* sconfigge il campione mondiale di scacchi Garry Kasparov nel 1997. Si sviluppano applicazioni pratiche di IA come i motori di ricerca e i sistemi di raccomandazione.

Questo periodo vide anche il passaggio da un approccio fondato su regole a uno basato sull'apprendimento. Invece di programmare esplicitamente le regole per risolvere un problema, i ricercatori iniziarono a sviluppare algoritmi che permettevano ai *computer* di apprendere dai dati. Negli anni 2000 tutto cambia con l'avvento dei *Big Data* e l'aumento della potenza di calcolo. Le tecniche di apprendimento automatico rivoluzionano il campo, in particolare il *machine learning* che, grazie all'utilizzo delle reti

MYCIN era in grado di identificare il batterio responsabile dell'infezione analizzando i sintomi e i risultati dei test medici. Una volta identificato il batterio, suggeriva il trattamento antibiotico più adatto, includendo dosi e durata della terapia. Alla base del sistema vi erano circa 600 regole «se-allora», che riflettevano le pratiche e le conoscenze mediche di esperti nel campo delle malattie infettive. *MYCIN* utilizzava un motore di inferenza per analizzare i dati medici inseriti dall'utente (ad esempio, i risultati dei test di laboratorio) e, sulla base delle regole della sua base di conoscenza, suggeriva una diagnosi e un trattamento. I medici potevano interagire con il sistema inserendo dati clinici, ai quali il sistema rispondeva con domande mirate per perfezionare la diagnosi. Alla fine, forniva una spiegazione del suo processo decisionale. Per questioni legali ed etiche non è mai stato utilizzato su pazienti reali. Per un approfondimento su *MYCIN* e sui sistemi esperti in generale si veda S. RUSSELL, P. NORVIG, *Artificial Intelligence: A Modern Approach*, Pearson, Londra, 2014; J. GIARRATANO, G. RILEY, *Expert Systems: Principles and Programming*, Brooks/Cole, Salt Lake City, 1989.

[13] Le reti neurali, ispirate alla struttura del cervello umano, sono composte da unità di elaborazione interconnesse che lavorano insieme per risolvere problemi complessi. Negli anni '90, le reti neurali soffrirono di alcuni limiti, come la difficoltà di addestramento e la mancanza di potenza computazionale, che ne limitarono l'applicabilità. Per un approfondimento v. G. MARTINELLI, voce *Reti neurali*, in *Enc. Treccani*, V Appendice, 1994.

neurali, ha permesso di affrontare problemi complessi come il riconoscimento delle immagini, la traduzione automatica e la comprensione del linguaggio naturale[14].

Oggi, l'IA è presente in quasi tutti gli aspetti della vita quotidiana. Assistenti vocali come *Siri*, *Alexa* e *Google Assistant* la utilizzano per comprendere e rispondere alle richieste degli utenti. I motori di ricerca come *Google* usano l'IA per migliorare la pertinenza dei risultati di ricerca. L'IA è anche utilizzata nella diagnostica medica, dove algoritmi avanzati possono analizzare immagini e identificare segni di malattie con un'accuratezza spesso superiore a quella dei medici umani.

Nel settore dei trasporti, i veicoli autonomi sono una delle applicazioni più promettenti dell'IA. Essi utilizzano una combinazione di sensori, algoritmi di *machine learning* e reti neurali per navigare e prendere decisioni in tempo reale. *Tesla*, *Waymo* e altre aziende stanno sviluppando tecnologie di guida autonoma che promettono di rivoluzionare il modo in cui ci spostiamo.

L'IA è anche utilizzata nell'industria finanziaria per il *trading* algoritmico, l'analisi del rischio e la prevenzione delle frodi. Algoritmi avanzati possono analizzare grandi quantità di dati in tempo reale, identificare *pattern* e fare previsioni accurate. Questo ha portato a una maggiore efficienza e precisione nelle decisioni finanziarie.

L'IA continua a evolversi rapidamente, con progressi nel campo dell'apprendimento non supervisionato, dell'IA spiegabile, e dell'etica dell'IA. Le applicazioni spaziano dalla medicina all'energia, dalla finanza all'intrattenimento, sollevando anche importanti questioni etiche e sociali riguardanti la *privacy*, il lavoro e la sicurezza.

---

[14] I concetti di *machine learning* e di *big data* saranno analizzati rispettivamente nei paragrafi 3 e 4 del presente capitolo. Alcuni esempi di letture per introdurre la tematica del presente lavoro: R. GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Giuffrè, Milano, 2022; T. NUMERICO, *Big date e algoritmi*, Carocci Editore, Roma, 2021, p. 25 ss.; C. FONTANA, *Definizioni e lineamenti tecnici essenziali dell'intelligenza artificiale: cenni al quadro regolamentare e ai principali problemi giuridici*, in G.C. Ferroni, C. Fontana, E.C. Raffiotta (a cura di), *AI Anthology, Profili giuridici, economici e sociali dell'intelligenza artificiale*, Il Mulino, Bologna, 2022, p. 65 ss.; G.F. ITALIANO, *Le sfide interdisciplinari dell'intelligenza artificiale*, in *Analisi giuridica dell'economia,* 2019, p. 9 ss.; P. MCCORDUCK, *Machines Who Think. A Personal Inquiry into the History and Prospects of Artificial Intelligence*, A.K. Peters, 2004.

2. Una definizione di intelligenza artificiale

Quando si parla di intelligenza artificiale viene da pensare subito ad un *robot* che imita l'essere umano in tutte le sue funzioni. Sebbene questa sia solo una delle possibili applicazioni dell'IA, e forse la più spettacolare dal punto di vista mediatico, non rappresenta necessariamente la più importante o pratica nell'attuale fase di sviluppo tecnologico. In realtà, l'IA oggi è principalmente costituita da *software* e algoritmi che lavorano silenziosamente, migliorando una vasta gamma di processi[15].

Ancora non si è arrivati ad una definizione univoca e universalmente riconosciuta di intelligenza artificiale[16]. Alcuni la ritengono una copia di quella umana.

Tuttavia, il termine intelligenza artificiale appare intrinsecamente contraddittorio, considerando che l'intelligenza è tipicamente associata esclusivamente all'essere umano. A questo proposito, in dottrina è stato affermato che «La locuzione "intelligenza artificiale" è un evidente ossimoro, in quanto attribuisce all'"artificiale" qualcosa che è essenzialmente "naturale" in quanto è la prerogativa più gelosa della natura umana: l'intelligenza. E l'ossimoro è piuttosto provocatorio, poiché c'è chi molto

[15] F. BASILE, *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione,* in F. Basile, M. Caterini, S. Romano (a cura di), *Il sistema penale ai confini delle hard sciences. Percorsi epistemologici tra neuroscienze e intelligenza artificiale*, Pacini Editore, Pisa, 2021, p. 3 ss.; C. TREVISI, *La regolamentazione in materia di Intelligenza artificiale, robot, automazione: a che punto siamo*, in *Medialaws*, 2/2018, p. 447 ss.; L. FLORIDI, *What the Near Future of Artificial Intelligence Could Be*, in *Philosophy & Technology*, 32/2019, p. 11 ss.; E. LO MONTE, *Intelligenza artificiale e diritto penale: le categorie dommatiche alla prova del futuribile*, in F. Basile, M. Caterini, S. Romano (a cura di), *Il sistema penale ai confini delle hard sciences,* cit., p. 41.

[16] Sul punto si può fare riferimento ai tentativi di definizione operati dalla dottrina: M. SOMALVICO, *L'intelligenza artificiale*, Hewlett-Packard, Milano, 1987; R. CORDESCHI, *L'Intelligenza Artificiale* in *La Scienza*, 2005, originariamente pubblicata in E. Bellone, C. Mangione (a cura di), *Storia del pensiero filosofico e scientifico. Il Novecento*, vol. 8, III, Milano, 1996, p. 145 ss.; F. AMIGONI, V. SCHIAFFONATI, M. SOMALVICO, voce *Intelligenza Artificiale*, in *Enc. Treccani*, 2008; S. RUSSELL, P. NORVIG, *Artificial intelligence: a modern approach*, cit.; P. WANG, *On defining artificial intelligence*, in *Journal of General Artificial Intelligence*, 10/2019, p. 1-37; D. MONETT, C.W.P. LEWIS, *Getting clarity by defining Artificial Intelligence - A Survey*, in V.C. Muller, *Philosophy and Theory of Artificial Intelligence*, Springer, Berlino, 2017, p. 212 ss.; N.J. NILSSON, *The Quest for Artificial Intelligence: A History of Ideas and Achievements*, Cambridge University Press, Cambridge, 2009.

seriamente si domanda se la macchina possa essere davvero "intelligente", nel senso in cui questo termine è attribuito alla mente dell'uomo»[17].

Negli ultimi decenni scienziati e ricercatori hanno parlato di intelligenza artificiale per descrivere tecnologie molto diverse, con premesse e obiettivi spesso divergenti. Ad esempio, Stuart Russell e Peter Norvig, nel loro manuale introduttivo *Artificial Intelligence - A Modern Approach*, elencano una serie di applicazioni dell'IA come robotica, *computer vision*, *machine learning*, ragionamento automatico, *knowledge representation* ed elaborazione del linguaggio naturale[18].

Recentemente, l'ambiguità semantica del termine è aumentata a causa dell'entusiasmo per i rapidi progressi tecnologici e dell'attenzione mediatica verso i sistemi intelligenti. Diversi osservatori hanno sottolineato la tendenza a etichettare come intelligenza artificiale prodotti che, in realtà, non lo sono, o lo sono solo in minima parte, con l'obiettivo di sfruttare commercialmente l'attuale interesse per il settore[19].

Nonostante le diversità che emergono nel dibattito tecnico-scientifico, è stato correttamente evidenziato che l'elaborazione di una definizione convenzionale è necessaria in primo luogo per una corretta gestione della materia. La crescente presenza di sistemi intelligenti nella vita quotidiana delle persone rende sempre più urgente lo sviluppo di sistemi di regolazione a vari livelli, il cui oggetto deve essere chiaramente delimitato.

---

[17] P. MELLO, voce *Intelligenza artificiale*, in *Dizionario Interdisciplinare di Scienza e Fede. Cultura scientifica, filosofia e teologia*, Roma, 2002.

[18] S. RUSSELL, P. NORVIG, *Artificial intelligence,* cit., p. 2.

[19] B. KARDON, *Is every company really an AI company?*, in *AdAge*, 2019, consultabile sul sito *web* www.adage.com. La fama dell'IA è stata accresciuta anche dai successi ottenuti da alcuni sistemi che imitano l'intelligenza umana, come ad esempio la vittoria a *Go* del programma di *Google DeepMindAlphaGo* contro il campione sudcoreano Lee Sedol, nel 2016; la vittoria, nel 2011, del sistema esperto *IBM Watson* contro Ken Jennings e Brad Rutter, due dei migliori concorrenti del game show statunitense *Jepoardy*; la sconfitta, risalente al 1997, del maestro di scacchi russo Garry Kasparov contro *IBM Deep Blue*; la vittoria del programma *Pluribus* in un torneo di poker contro alcuni dei migliori giocatori professionisti del mondo. Sul punto si veda B. MARR, *Man vs. machine: the 6 greatest AI challenge to showcase the power of artificial intelligence*, in *Forbes* (*online*), 21 gennaio 2021.

Il legislatore europeo[20] ha precisato che la nozione di IA debba essere definita in modo da garantire la certezza del diritto e nello stesso tempo la flessibilità necessaria per accogliere i futuri sviluppi tecnologici.

L'AI Act prevede anche un allegato che può essere modificato alla luce del costante e progressivo cambiamento della tecnologia[21] e individua diversi gruppi di sistemi: *machine learning* e *deep learning*; tecnologie basate sulla logica e sulla conoscenza, sulla programmazione (logica) induttiva, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti.

Si tratta di tecnologie differenti tra loro, ma che sono accomunate dal fatto di riuscire ad analizzare molti più dati e più variabili rispetto alla mente umana.

Gli algoritmi più semplici, sia deterministici che probabilistici, si basano su calcoli, statistiche e istruzioni di base. La loro caratteristica principale è che, a ogni passo del processo corrisponde una soluzione univoca, un solo percorso; ciò significa che, partendo da dati specifici, si giunge sempre allo stesso risultato, rendendolo prevedibile[22]. La scelta del modello matematico e del rapporto tra i dati assume, quindi, un'importanza cruciale e deve essere attentamente valutata in fase preliminare, poiché influisce direttamente sul contenuto della decisione finale.

La risposta generata dal sistema non fa altro che amplificare le capacità di elaborazione umana, basandosi su una formulazione matematica del problema che lo scompone in una realtà numerica, rendendolo calcolabile, prevedibile e replicabile. Questo processo rientra nel concetto di calcolabilità giuridica, che rappresenta la

---

[20] Articolo 3 del Regolamento della Commissione europea sull'intelligenza artificiale (*AI Act*).

[21] Il Regolamento prevede infatti che i sistemi di IA possano essere progettati per funzionare con diversi livelli di autonomia ed essere utilizzati in modo autonomo o come componente di un prodotto, indipendentemente dal fatto che il sistema sia fisicamente integrato come parte del prodotto finale (incorporato) o serva la funzionalità del prodotto senza essere integrato (non incorporato). Inoltre, il Regolamento prevede, all'art. 3, che «per sistema di IA si intende quel software sviluppato in una o più delle modalità e approcci di cui all'Allegato I del Regolamento e che presenti alcune caratteristiche funzionali, in particolare esso deve essere in grado di generare una serie di risultati come contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagisce alla luce degli obiettivi definiti dall'uomo».

[22] G. AVANZINI, *Intelligenza artificiale, machine learning e istruttoria procedimentale: vantaggi limiti ed esigenze di una corretta Data governance*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Volume 2, Quaderni ASTRID, Bologna, 2022, p. 80.

possibilità di applicare strumenti algoritmici e matematici a problemi giuridici, garantendo una certa uniformità e prevedibilità nelle decisioni[23].

La capacità di questi strumenti di analizzare enormi quantità di dati modifica in modo sostanziale il processo cognitivo tradizionale: la realtà, o la porzione di realtà su cui si basa una decisione, viene rielaborata attraverso una serie di elementi decontestualizzati che assumono un nuovo e autonomo significato. Sebbene questi algoritmi abbiano una capacità ordinante e siano in grado di individuare relazioni tra i dati, essi non possiedono la capacità di attribuire un significato semantico ai risultati, poiché non si basano su una comprensione previa delle cause sottostanti ai fenomeni analizzati[24].

Una recente sentenza del Consiglio di Stato ha precisato che l'intelligenza artificiale, a differenza di un normale algoritmo, contempla meccanismi di *machine learning* e crea un sistema che non si limita solo ad applicare le regole *software* e i parametri preimpostati ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, sfruttando un processo di apprendimento automatico[25].

Un altro tentativo di definizione arriva dall'OCSE, che identifica come sistema di intelligenza artificiale qualsiasi modello di implementazione basato su una macchina in grado di dedurre dall'*input* che riceve una serie di dati processabili finalizzati a

---

[23] N. IRTI, *Per un dialogo sulla calcolabilità giuridica*, in A. Carleo (a cura di), *Calcolabilità giuridica*, Il Mulino, Bologna, 2017, p. 17 ss.

[24] Sul punto si veda M. DURANTE, *Potere computazionale. L'impatto delle ITC*, in *Diritto, società, sapere*, Meltemi, Milano, 2019; L. FLORIDI, *Semantic Capital: Its Nature, Value and Curation*, in *Philosophy and Technology*, 31/2018, p. 481 ss.

[25] V. Cons. Stato, sez. III, 25/11/2021, n. 7891 che precisamente afferma che «la nozione comune e generale di algoritmo riporti alla mente semplicemente una sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato (...). Nondimeno si osserva che la nozione, quando è applicata a sistemi tecnologici, è ineludibilmente collegata al concetto di automazione ossia ai sistemi di azione e controllo idonei a ridurre l'intervento umano. Il grado e la frequenza dell'intervento umano dipendono dalla complessità e dall'accuratezza dell'algoritmo che la macchina è chiamata a processare. Cosa diversa è l'intelligenza artificiale. In questo caso l'algoritmo contempla meccanismi di *machine learning* e crea un sistema che non si limita solo ad applicare le regole *software* 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».

generare svariati *output* (come, ad esempio, previsioni, raccomandazioni, contenuti, decisioni, ecc.), suscettibili di influenzare ambienti fisici o virtuali, tenuto conto di un insieme di obiettivi espliciti o impliciti concretamente perseguiti, a seconda che siano programmati direttamente da uno sviluppatore umano, oppure definiti mediante il ricorso a tecniche di auto-apprendimento algoritmico[26].

Anche l'*AI Act* adotta una definizione di intelligenza artificiale allineata a quella dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE). Questa scelta ha lo scopo di fornire criteri precisi per riconoscere i sistemi di IA e distinguerli da tecnologie più semplici, assicurando così un'adeguata regolamentazione dell'IA rispetto ai rischi e alle complessità che comporta, soprattutto in termini di sicurezza, affidabilità e rispetto dei diritti fondamentali[27].

3. Il *machine learning*

La Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi[28], definisce così il concetto di *machine learning*: «L'apprendimento automatico consente di costruire, a partire dai dati, un modello matematico che include un gran numero di variabili non conosciute in anticipo. I parametri si configurano gradualmente durante la fase di apprendimento, che utilizza insiemi di dati di addestramento per reperire e classificare i collegamenti. I diversi metodi di apprendimento automatico sono scelti dai progettisti a seconda della natura dei compiti da svolgere (raggruppamento). Tali metodi sono generalmente classificati in tre

[26] La definizione fornita dall'OCSE, peraltro costantemente aggiornata, è consultabile sul sito *web* https://oecd.ai/en/wonk/ai-system-definition-update.

[27] L'*AI Act* è il Regolamento (UE) 2024/1689 che stabilisce norme armonizzate sull'intelligenza artificiale. Verrà approfondito nel capitolo 2.

[28] La Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi è stata adottata nei giorni 3-4 dicembre 2018 dalla Commissione europea per l'efficienza della giustizia (CEPEJ), istituita dal Comitato dei ministri del Consiglio d'Europa nel 2002 (v. paragrafo 5).

categorie: apprendimento supervisionato (da un essere umano), apprendimento non supervisionato e apprendimento per rinforzo».

Il *machine learning*, o apprendimento automatico, è dunque la capacità di un sistema di apprendere e migliorare senza una programmazione predefinita. Questo processo si basa su tecniche come le reti neurali ispirate al funzionamento del cervello umano: il sistema è composto da unità interconnesse, simili ai neuroni, che elaborano le informazioni in risposta a *input* esterni e le trasmettono ad altre unità. Grazie ad algoritmi che analizzano i dati, il sistema è in grado di imparare autonomamente, correggere gli errori e fare previsioni, con l'apprendimento che avviene attraverso l'analisi di grandi volumi di dati.

Grazie alle tecniche di *machine learning*[29] l'intelligenza artificiale è in grado di apprendere autonomamente dall'ambiente circostante, raccogliendo e analizzando dati per migliorare continuamente le proprie prestazioni. In sostanza, il *software* di IA evolve nel tempo, adattandosi e riprogrammandosi in modo da raggiungere in modo più efficace gli obiettivi per cui è stato progettato.

Esistono diverse tipologie di *machine learning*[30]. Tra queste, di particolare interesse è il c.d. apprendimento supervisionato (*supervisioned learning*), in cui un modello viene addestrato utilizzando un insieme di dati etichettati, cioè dati per i quali conosciamo già la risposta corretta. L'obiettivo è quello di insegnare al modello a fare previsioni o

---

[29] Sul *machine learning* v. U. RUFFOLO, *Intelligenza Artificiale, "machine learning" e responsabilità da algoritmo*, in *Giur. it.*, 7/2019, p. 1689 ss.; G. UBERTIS, *Processo penale telematico, intelligenza artificiale e costituzione - telematic criminal proceedings, artificial intelligence and the constitution*, in *Cass. pen.*, 2/2024, p. 439 ss.; L. PICOTTI, *Intelligenza artificiale e diritto penale: le sfide ad alcune categorie tradizionali*, in *Dir. pen. e proc.*, 3/2024, p. 293 ss.; C. COLAPIETRO, A. MORETTI, *L'intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, in *BioLaw Journal*, 3/2020, p. 365 ss. Per una prospettiva tecnica si veda anche S. RUSSELL, P. NORVIG, *Artificial Intelligence: A Modern Approach,* cit., p. 634 ss.; L. FLORIDI, *What the Near Future of Artificial Intelligence Could Be*, cit., p. 4 ss.; P. DOMINGOS, *L'algoritmo definitivo: la macchina che impara da sola e il futuro del nostro mondo*, Bollati Boringhieri, Torino, 2016; K. HAO, *What is machine learning*, in *MIT Technology Review*, 17 novembre 2018; H. SURDEN, *Machine Learning and Law*, in *Washington Law Review*, 2014, p. 87 ss.; S. QUINTARELLI, *Forum AI and Law*, in *BioLaw Journal*, 1/2020, p. 493 ss.

[30] Per una disamina dettagliata v. *L'impatto dell'Intelligenza Artificiale (AI Artificial Intelligence) sul ciclo di intelligence e sugli strumenti a disposizione per i pianificatori militari e le forze dell'ordine*, a cura del Centro Alti Studi per la Difesa – Istituto Alti Studi per la Difesa, 71a Sessione di studio IASD 2019-2020, pubblicazione a cura del Centro Militare di Studi Strategici.

classificazioni basate su questi dati. L'algoritmo impara a mappare gli *input* agli *output*, e una volta addestrato, può applicare ciò che ha imparato a dati non etichettati.

Diverso è il c.d. apprendimento non supervisionato (*unsupervisioned learning*) in cui i dati di addestramento non sono etichettati. Qui, l'obiettivo è scoprire strutture, modelli o relazioni sottostanti all'interno dei dati senza avere informazioni precedenti sui risultati attesi. L'algoritmo non ha accesso agli *output* corretti durante l'addestramento, un esempio è il *clustering*, in cui il sistema raggruppa dati simili senza sapere in anticipo quali gruppi dovrebbero esistere[31].

Un'ultima tipologia di *machine learning* è l'apprendimento per rinforzo (*reinforcement learning*) ispirato alla psicologia comportamentale, in cui un agente artificiale impara a prendere decisioni ottimali attraverso l'interazione con un ambiente. Diversamente dall'apprendimento supervisionato e non supervisionato, in cui i modelli imparano da dati etichettati, l'apprendimento per rinforzo si concentra sull'ottimizzazione di una sequenza di azioni in un contesto dinamico. In questo modello, l'algoritmo interagisce con un ambiente attivo e riceve *feedback* in base alle azioni che compie[32].

Quella che forse è la più importante tra le tipologie di apprendimento è il *deep learning*[33], un metodo che permette alle macchine di elaborare informazioni su più livelli, in modo sempre più complesso e profondo, emulando così il comportamento e le capacità di apprendimento della mente umana. Il sistema, dunque, impara a

---

[31] Questo metodo viene utilizzato spesso per segmentare i clienti in base ai loro comportamenti d'acquisto. Il *clustering* verrà esaminato nel secondo capitolo.

[32] È il tipo di apprendimento utilizzato, ad esempio, nei giochi: l'algoritmo impara attraverso prove ed errori quale strategia adottare per vincere.

[33] Un esempio notevole del potere del *deep learning* è il sistema *AlphaGo*, sviluppato da *DeepMind*, una società di *Google*. *AlphaGo* nel 2016 ha sconfitto il campione mondiale di Go, un gioco estremamente complesso, dimostrando la capacità dell'IA di superare l'intelligenza umana in contesti specifici. Tra i più rilevanti lavori sul *deep learning* si veda: P. TRAVERSO, *Breve introduzione tecnica all'Intelligenza Artificiale*, in *DPCE online*, 1/2022, p. 155 ss.; U. RUFFOLO, *Intelligenza Artificiale, "machine learning" e responsabilità da algoritmo*, cit.; G. CARULLO, *Large Language Models for Transparent and Intelligible AI-Assisted Public Decision-Making*, in *CERIDAP – Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche*, 3/2023, p. 1 ss.; C. CASONATO, *Unlocking the Synergy: Artificial Intelligence and (old and new) Human Rights*, in *BioLaw Journal*, 3/2023, p. 233 ss.; C. PISTILLI, *L'utilizzo dell'intelligenza artificiale nel campo delle attività investigative delle forze dell'ordine: tra prospettive di sviluppo ed esigenze di coordinamento,* in F. Basile, M. Caterini, S. Romano (a cura di), *Il sistema penale ai confini delle hard sciences,* cit., p. 148 ss.

classificare i dati in modo autonomo e strutturarli gerarchicamente, distinguendo quelli più utili o rilevanti per risolvere specifici problemi.

Questo processo consente alle macchine di apprendere continuamente, migliorando progressivamente le loro prestazioni. Il *deep learning* permette infatti di analizzare grandi quantità di dati, riconoscere schemi complessi e affinare i risultati attraverso l'esperienza, rendendo i sistemi sempre più precisi ed efficaci man mano che acquisiscono nuove informazioni.

A questo punto si pone una riflessione sulla singolarità dell'algoritmo che fornisce capacità di apprendimento all'intelligenza artificiale. L'algoritmo conferisce all'AI la capacità di modificarsi autonomamente, perfezionarsi e, in alcuni casi, creare versioni evolute di sé stessa, capaci a loro volta di autocorreggersi e rigenerarsi. Questa caratteristica distingue tali algoritmi dai *software* tradizionali, poiché non si limitano a eseguire istruzioni fisse, ma permettono all'AI di apprendere e adattarsi. In ragione della sua influenza sul comportamento e sulle capacità dell'AI, l'algoritmo dovrebbe essere considerato parte integrante della entità intelligente stessa.

In questo scenario, una delle maggiori preoccupazioni riguarda il fatto che la capacità di autoapprendimento delle macchine potrebbe portare, nel tempo, allo sviluppo di attitudini e comportamenti imprevedibili e incontrollabili. Man mano che il sistema acquisisce nuove competenze vi è il rischio che inizi a operare in modi non pianificati o immaginati, generando situazioni difficili da gestire o addirittura pericolose, poiché non sarebbero state contemplate nei processi di sviluppo iniziali.

Questo rende necessaria una riflessione sulla responsabilità di chi progetta e implementa tali algoritmi, poiché le conseguenze di un comportamento non previsto potrebbero avere impatti significativi, sia in ambito sociale che legale. L'evoluzione autonoma di un'AI può quindi sollevare questioni su come monitorare, controllare e limitare il comportamento delle macchine, così da evitare che questi sviluppi portino a conseguenze indesiderate[34].

[34] Di conseguenza si apre il problema della responsabilità del creatore dell'algoritmo (il quale potrebbe essere persona diversa rispetto al costruttore del sistema) che potrebbe essere chiamato a rispondere dei danni causati dall'IA che ha ricevuto la capacità di apprendere e comportarsi in modo autonomo. Nel caso di un'IA dotata di capacità di autoapprendimento, ma priva di adeguati

Il *machine learning* sta evolvendo rapidamente, grazie anche alla crescita della potenza di calcolo e alla disponibilità di dati su larga scala. Il suo impatto è destinato a crescere ulteriormente, non solo in ambiti come il riconoscimento delle immagini e del linguaggio, ma anche in settori come l'intelligenza artificiale generativa, che permette ai sistemi di creare contenuti nuovi, come testi, immagini o musica.

In futuro, il *machine learning* potrebbe portare a macchine sempre più autonome, capaci di risolvere problemi complessi, adattarsi rapidamente a nuovi contesti e prendere decisioni sempre più sofisticate. Tuttavia, questo sviluppo richiede anche un'attenta riflessione su questioni etiche, legali e sociali, per garantire che tali tecnologie vengano utilizzate in modo equo e trasparente.

Uno dei limiti per il corretto funzionamento di questi sistemi di apprendimento è la qualità delle informazioni. Gli algoritmi, per funzionare adeguatamente, dipendono fortemente dai dati, i quali, se inaccurati, incompleti o distorti possono portare a modelli fuorvianti[35]. La qualità dei dati è quindi fondamentale per ottenere risultati validi. Se, ad esempio, le informazioni utilizzate per addestrare i sistemi contengono pregiudizi (come discriminazioni di genere o razza), gli algoritmi possono riprodurre e persino amplificare tali *bias*. È quindi cruciale vigilare sull'etica e l'equità dei modelli sviluppati.

4. Il ruolo dei dati

L'utilizzo di strumenti informatici sempre più avanzati per l'analisi di grandi quantità di dati permette di ampliare la conoscenza dei fenomeni, valorizzando il processo istruttorio nella ricostruzione dei fatti e migliorando l'equilibrio tra istruzione e

meccanismi in grado di inibire comportamenti malevoli o devianti, si pone non solo la questione della responsabilità del produttore e dell'ideatore dell'algoritmo, ma anche quella delle responsabilità, almeno concorrenti, di chi addestra l'intelligenza artificiale o la espone a esperienze che possono influenzarne il comportamento o orientarne lo sviluppo. Sul punto si veda U. RUFFOLO, *Intelligenza Artificiale, "machine learning" e responsabilità da algoritmo*, cit., p. 1691.

[35] C. BISHOP, *Pattern Recognition and Machine Learning,* Springer, Berlino, 2006.

decisione, rappresentando un vantaggio significativo. In questo contesto, i dati alla base degli algoritmi diventano cruciali, poiché la rappresentazione della realtà e il significato attribuito ad essa sono il risultato di un accertamento sintetico che deriva dall'analisi matematica e informatica degli *input*. È importante considerare che i *dataset* utilizzati possono variare notevolmente sia in termini quantitativi che qualitativi.

I sistemi meno sofisticati di intelligenza artificiale lavorano su dati strutturati, che sono stati preventivamente selezionati da operatori umani. In questo contesto, la qualità, l'aggiornamento e l'adeguatezza dei dati rispetto agli obiettivi perseguiti sono caratteristiche fondamentali, poiché queste possono essere controllate e contestate, essendo il frutto di una preparazione che segue un ordine logico definito.

Nell'ambito dell'IA si parla spesso di *big data*, ovvero grandi quantità di informazioni che vengono generate, raccolte e analizzate da varie fonti digitali in tutto il mondo. Questi dati possono provenire da una vasta gamma di fonti, tra cui *social media*, dispositivi connessi a *internet*, sensori, transazioni finanziarie, ricerche *web*, applicazioni mobili, e molto altro. Il termine non si riferisce solo al volume di dati, ma anche alle tecnologie e alle metodologie utilizzate per gestire e analizzare queste grandi quantità di informazioni[36].

I *big data* sono caratterizzati dalle cosiddette 5V[37], che ne delineano le principali peculiarità:

1. Volume: si riferisce alla quantità enorme di dati generati quotidianamente. Con l'aumento delle tecnologie digitali, essi sono prodotti in una scala senza precedenti, richiedendo infrastrutture adeguate alla loro gestione e analisi.
2. Velocità: indica la rapidità con cui i dati vengono generati, elaborati e analizzati. Le tecnologie moderne permettono di raccogliere dati in tempo reale o quasi, consentendo alle organizzazioni di reagire tempestivamente.

[36] I *big data* sono definiti dalla stessa Commissione europea come «una grande quantità di tipi diversi di dati prodotti con un'alta velocità da un grande numero di fonti di diverso tipo. La gestione di tali aggregati di dati richiede oggi nuovi strumenti e metodi, come processori potenti, *software* e algoritmi». Si veda COM (2014) 442 Final.

[37] L. ALGERI, *Intelligenza artificiale e polizia predittiva,* in *Dir. pen. e proc.,* 6/2021.

3. Varietà: rimanda alla diversità delle fonti da cui provengono i dati. Essi possono avere formati differenti (testo, immagini, video, dati strutturati e non strutturati) e provenire da diverse piattaforme, come social media, sensori IoT, transazioni finanziarie e altro.
4. Veridicità: sottolinea l'importanza di stabilire l'autenticità dei dati. Poiché i big data possono includere informazioni provenienti da fonti non verificate, è fondamentale valutarne la qualità e l'affidabilità per evitare analisi fuorvianti.
5. Variabilità: riguarda la mutevolezza e la dinamicità dei dati, che possono assumere significati diversi a seconda del contesto in cui vengono utilizzati. Questo aspetto è cruciale quando si interpretano le informazioni, poiché il loro valore può variare in base alle circostanze e al tempo.

I sistemi di IA partono dal presupposto che all'interno di grandi volumi di dati risieda un valore cognitivo intrinseco, specifico e diverso da quello che potrebbe essere estratto da insiemi di dati più ridotti. Il loro processo di analisi si focalizza nel far emergere il significato dai dati attraverso numerose e diverse correlazioni, che non seguono un percorso lineare né una logica tradizionale[38].

Spesso i *Big data,* con riferimento a sistemi di intelligenza artificiale più avanzati, dotati di capacità di autoapprendimento, sono raccolti per essere elaborati nei cosiddetti *data lakes*[39]. Questi grandi volumi di dati sono cruciali per migliorare le

[38] G. AVANZINI, *Decisioni amministrative e algoritmi informativi, predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Editoriale Scientifica, Napoli, 2019, p. 133 ss.

[39] Un *data lake* è un vasto archivio di dati grezzi, strutturati e non strutturati, conservati nel loro formato originale. Questo tipo di archiviazione permette di raccogliere dati provenienti da diverse fonti senza una finalità d'uso predefinita, offrendo flessibilità per future analisi e applicazioni. I *data lakes* supportano tecnologie avanzate di analisi dei dati, come il *machine learning* e l'analisi predittiva, consentendo l'elaborazione di grandi volumi di informazioni eterogenee. La gestione efficace di un *data lake* richiede una solida *governance* per assicurare che i dati rimangano accessibili, pertinenti e utilizzabili per gli scopi desiderati. Per un approfondimento si veda H.J. WATSON, *Data Lakes, Data Labs, and Sandboxes*, in *Business Intelligence Journal*, vol. 20, 1/2020; F. RAVAT, *Data Lakes: Trends and Perspectives, Lecture Notes in Computer Science*, in *Database and Expert Systems Applications 30th International Conference*, 2019, p. 304 ss.; IAEME PUBLICATION, *Exploring data lakes: a cornerstone of big data engineering*, in *International Journal of Advanced Research in Engineering and Technology (IJARET)*, Vol. 15, Issue 3, May-June, 2024, p. 211 ss.; M. KLETTKE, U. STÖRL, S. SCHERZINGER, *Uncovering the Evolution History of Data Lakes*, in *IEEE International Conference on Big Data (BIGDATA)*, 2017.

prestazioni del sistema, specialmente quando vengono utilizzate tecniche che richiedono l'addestramento di modelli, garantendo così che il sistema operi in modo previsto e sicuro. I *data lakes* possono essere descritti come archivi destinati alla memorizzazione, analisi e correlazione di dati sia strutturati che non strutturati, conservati nel loro formato originale, indipendentemente dalla loro natura o provenienza, che spaziano dai *post* sui *social media* a informazioni provenienti dai sensori di vari dispositivi o macchinari industriali. Questi vasti bacini di dati sono alimentati da molteplici fonti senza uno scopo d'uso prestabilito, consentendo di supportare una vasta gamma di applicazioni analitiche generiche.

Tali informazioni grezze e non strutturate permettono di sfruttare le più recenti tecnologie di analisi avanzata, come il *machine learning*, la scoperta dei dati e l'analisi predittiva, per generare previsioni in tempo reale o fornire informazioni utili. Tuttavia, la creazione di *data lakes* richiede una *governance* solida dei dati, non solo per evitare che le informazioni diventino inaccessibili, ma anche per garantire che le stesse siano adeguate e pertinenti rispetto agli obiettivi che si intendono raggiungere.

In questo contesto, la vastità dei dati può supplire alla mancanza di qualità, ma l'eterogeneità degli stessi introduce nuove problematiche, specialmente nella sfera pubblica. I risultati prodotti da tali sistemi, infatti, possono essere imprevedibili e inesplicabili persino per i programmatori che li hanno sviluppati, trasformandosi in vere e proprie *black boxes*, ossia scatole nere il cui funzionamento interno è oscuro e poco trasparente[40].

[40] Il termine *black box* si riferisce a un sistema il cui comportamento esterno è osservabile, ma il cui funzionamento interno rimane sconosciuto o nascosto. Questo tipo di modello è caratterizzato dal fatto che possiamo analizzarlo solo in base alle sue risposte (*output*) a determinati stimoli o *input*, senza avere visibilità o comprensione dei processi interni che producono tali risposte. La definizione di *black box* deriva dall'idea che, soprattutto in contesti dove più sistemi sono interconnessi, ciò che conta davvero a livello macroscopico e per scopi pratici è il comportamento esterno del sistema, piuttosto che i meccanismi interni che lo determinano. Per un approfondimento si veda E. TROISI, *Decisione algoritmica, "Black-Box" e AI etica: il diritto di accesso come diritto a ottenere una spiegazione*, in *Jus civile*, 4/2022, p. 953 ss.; L. ZAPPALÀ, *Transparency and Comprehensibility of Working Conditions and Automated Decisions: Is It Possible to Open the Black Box?*, in *The Italian Law Journal*, 2/2023, p. 623 ss.; G. LO SAPIO, *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*, in *Federalismi.it*, 16/2021, p. 114 ss.; S. ARDUINI, *La "scatola nera" della decisione giudiziaria: tra giudizio umano e giudizio algoritmico*, in *BioLaw Journal*, 2/2021, p. 453 ss.; F. PASQUALE, *The Black Box Society. The Secret*

Un ulteriore scenario reso possibile dalle tecnologie avanzate per l'elaborazione dei dati personali è rappresentato dai cosiddetti sistemi di credito sociale[41]. Con l'accumulo crescente di informazioni sugli individui da parte di enti pubblici e privati, diventa possibile classificarli in base alla loro adesione a determinati codici di condotta.

Sistemi di valutazione numerica delle informazioni relative a un individuo esistono già da tempo, specialmente in ambito privato, come i sistemi di *credit scoring* che influenzano l'accesso al credito basandosi sulla storia finanziaria dell'individuo.

Nella società digitale, è teoricamente possibile centralizzare un'enorme quantità di dati provenienti da fonti diverse, come *social network*, sistemi di pagamento elettronico, cartelle cliniche digitali e procedure amministrative informatizzate. L'analisi di questi dati consente di formulare valutazioni sempre più precise sulla conformità dei cittadini a un modello ideale, sintetizzando tali valutazioni in un punteggio numerico che riflette la vicinanza dell'individuo agli *standard* considerati ottimali.

Le tecnologie di apprendimento automatico permettono di migliorare e aggiornare continuamente il sistema, adattando le valutazioni ai cambiamenti comportamentali dei soggetti coinvolti. Inoltre, i *feedback* necessari per perfezionare il sistema potrebbero provenire direttamente dagli altri partecipanti, chiamati a esprimere un

---

Algorithms that Control Money and Information, Harvard Univ Pr, Cambridge (Mass), 2016; E. PELLECCHIA, *Profilazione e decisioni automatizzate al tempo della "Black Box Society": qualità dei dati e leggibilità dell'algoritmo nella cornice della "responsible research and innovation"*, in *Nuove leg. civ. comm.*, 5/2018, p. 1209 ss.

[41] Sul punto si veda T. ARMSTRONG, *Social Credit modernism*, in *Special Issue: Modernism Reloaded*, Vol. 55, Issue 2, July 2013; O. BAZINA, *Human rights and biometric data protection. Social credit system*, in *European Studies Quarterly*, 4/2020, p. 39 ss.; M. NORAZMI NORDIN, *Social Credit System Improvement Via Technology Mediation*, in *Turkish Online Journal of Qualitative Inquiry (TOJQI)*, Vol. 12, Issue4, July 2014; S. SONMEZ, *The emergence of Social Credit System*, in *Digital Politics Final Essay*, Université catholique de Louvain, 2018; A. DEVEREAUX, L. PENG, *Give us a little social credit: to design or to discover personal ratings in the era of Big Data*, in *Journal of Institutional Economics*, 16/2020, p. 369 ss.; R. BOTSMAN, *Who can you trust? How technology brought us together and why it might drive us apart*, PublicAffairs, New York, 2017; E. P. STRINGHAM (a cura di), *Private governance: creating order in economic and social life*, Oxford University Press, Oxford, 2015. In particolare, per quanto riguarda l'esperienza della Cina si veda Y. CHEN, A. S. CHEUNG, *The trasparent self under big data profiling: privacy and chinese legislation on the social credit system*, in *The journal of comparative law*, 12/2017, p. 356 ss.; R. CREEMERS, *China's social credit system: an evolving practice of control*, in *SSRN Papers*, 2018; S. HOFFMAN, *Managing the state: social credit, surveillance and CCP's plan for China*, in N. Wright (a cura di), *AI, China, Russia and the global order: technological, political, global and creative*, *Independently published*, 2019, p. 48 ss.

giudizio sul comportamento altrui. Ottenere un punteggio elevato porterebbe a vantaggi come l'accesso agevolato al credito, la possibilità di ricoprire incarichi pubblici o ruoli di responsabilità. Al contrario, un punteggio basso potrebbe comportare svantaggi concreti o vere e proprie sanzioni, come limitazioni nei viaggi, nell'accesso a locali pubblici o l'esclusione da determinate professioni[42].

I sostenitori di questa prospettiva ritengono che l'adozione di un sistema di credito sociale possa fungere da incentivo più potente rispetto ai tradizionali meccanismi di controllo, promuovendo comportamenti virtuosi e socialmente responsabili[43].

5. Il quadro normativo

L'attuale quadro normativo europeo sull'intelligenza artificiale mira a creare un contesto giuridico che possa bilanciare lo sviluppo tecnologico con la tutela dei diritti fondamentali. Il pilastro principale di questa disciplina è il già citato Regolamento sull'Intelligenza Artificiale, proposto dalla Commissione Europea nell'aprile 2021, denominato anche *AI Act*.

L'AI Act è una normativa progettata per stabilire un quadro di regolamentazione e *governance* dettagliato per l'utilizzo dell'intelligenza artificiale all'interno dell'Unione Europea. Questa legge rappresenta un avanzamento significativo verso una gestione

[42] L'unico esempio di un sistema di credito sociale che raccoglie dati e influenza vari aspetti della vita è quello annunciato dalla Cina nel 2014. Il governo cinese ha delineato un piano per implementare un sistema di credito sociale a livello nazionale, sebbene il progetto non sia stato completamente realizzato nei tempi previsti. Attualmente, il sistema di credito sociale è stato attivato in modo frammentario, coinvolgendo solo una parte della popolazione e basandosi sull'inserimento in *blacklist* per determinati comportamenti, piuttosto che sull'assegnazione di un punteggio numerico costantemente aggiornato. Nonostante il modello cinese sia l'unico esempio concreto di un sistema di credito sociale, seppur ancora limitato, altri Paesi hanno manifestato l'intenzione di sviluppare forme simili di cittadinanza digitale. Inoltre, analogie con questi sistemi sono sempre più evidenti nei meccanismi di *credit scoring* utilizzati da entità private, che stanno diventando sempre più sofisticati e diffusi anche in diverse democrazie consolidate. Per un approfondimento si veda L. GUERRA, *Il Sistema di credito sociale cinese tra mistificazioni e realtà*, in *Treccani online*, 13 maggio 2024.

[43] Questo sistema si distingue dalle strategie di *nudging* digitale, poiché non si limita a influenzare determinate scelte, ma mira a spingere le persone a comportarsi correttamente per evitare conseguenze negative significative. Del *nudging* parleremo nel capitolo 2.

responsabile e sicura delle tecnologie di IA, cercando di equilibrare le esigenze e gli interessi dei cittadini, delle imprese e dell'intera società. Il processo di elaborazione dell'AI Act ha coinvolto le istituzioni europee, con una partecipazione attiva di una vasta gamma di *stakeholder*, tra cui rappresentanti dell'industria, esperti tecnici e organizzazioni della società civile. L'obiettivo principale della normativa è affrontare le preoccupazioni chiave relative all'IA, come la trasparenza, la responsabilità, la sicurezza e la tutela dei diritti fondamentali.

5.1. Il percorso verso l'adozione dell'IA act.

Nell'aprile 2021 la Commissione europea ha presentato una proposta per un quadro normativo UE sull'intelligenza artificiale finalizzato a regolare l'utilizzo specifico dei sistemi di IA e i rischi associati[44].

Inizialmente è stato adottato un approccio *soft-law*, con la pubblicazione di alcune linee guida di natura etica, non vincolanti per gli Stati membri. Successivamente, a seguito dei veloci progressi dal punto di vista tecnologico, l'attenzione della Commissione si è orientata verso un approccio legislativo, finalizzato all'adozione di norme armonizzate per lo sviluppo, l'immissione sul mercato e l'uso di sistemi di IA. Il processo di legiferazione su queste tematiche è andato di pari passo con il rapido sviluppo delle relative tecnologie, che negli ultimi anni ha reso la regolamentazione dell'IA una questione politica centrale nell'Unione europea.

Già con il Libro bianco sull'intelligenza artificiale del 2020[45], la Commissione Europea si era impegnata a promuovere la diffusione dell'IA e ad affrontare i rischi associati a determinati usi di questa nuova tecnologia.

Ancor prima, il Parlamento europeo aveva invitato la Commissione a valutare l'impatto delle nuove tecnologie sui diritti fondamentali e a redigere un quadro UE

---

[44] C. MINELLI, *La responsabilità "penale" tra persona fisica e corporation alla luce della Proposta di Regolamento sull'Intelligenza Artificiale*, in *Dir. pen. cont.*, 2/2022, p. 50 ss.

[45] Il «*Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*» è stato pubblicato dalla Commissione europea il 19 febbraio 2020 [COM(2020) 65 final].

per l'IA nelle sue raccomandazioni del 2017 relative alle norme di diritto civile in materia di robotica[46]. Più di recente, il Parlamento europeo ha adottato una serie di risoluzioni che chiedono un'azione più decisa da parte dell'UE. Tra tutte, si può citare quella del 6 ottobre 2021, che ha affrontato il tema dell'utilizzo dell'intelligenza artificiale nel diritto penale e, più nel dettaglio, del suo utilizzo da parte delle autorità di polizia e giudiziarie[47], attraverso l'adozione di una serie di raccomandazioni al fine di favorire un approccio comune da parte dell'UE rispetto all'uso dell'IA nei settori della proprietà intellettuale, del diritto penale, dell'istruzione e della cultura, non solo in materia di usi civili ma anche militari.

Nell'ambito del Consiglio d'Europa, la Commissione europea per l'efficacia della giustizia (CEPEJ)[48] ha elaborato nel 2018 la «Carta etica europea sull'impiego dell'intelligenza artificiale nei sistemi giudiziari e in ambiti connessi», che rappresenta il più significativo intervento giuridico in Europa sul tema dello sviluppo dell'IA nei sistemi giudiziari[49].

Nell'aprile del 2019 la Commissione Europea ha pubblicato le «Linee guida etiche per un'intelligenza artificiale affidabile»[50], in cui sono delineati una serie di principi per assicurare uno sviluppo affidabile di tale tecnologia. In queste linee guida sono

---

[46] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), consultabile sulla Gazzetta Ufficiale dell'Unione europea.

[47] Il Parlamento, nella Risoluzione, riconosce il contributo positivo di determinati tipi di applicazioni di IA al lavoro delle autorità di contrasto e giudiziarie in tutta l'Unione; tuttavia, rileva pure che lo sviluppo dell'IA può comportare rischi enormi per i diritti fondamentali. Elenca, quindi, una serie di requisiti che questi sistemi debbono possedere perché possano essere lecitamente utilizzati. La risoluzione è consultabile sul sito *web* del Parlamento europeo.

[48] La Commissione europea per l'efficienza della giustizia (CEPEJ) è stata istituita il 18 settembre 2002 con la risoluzione Res(2002)12 del Comitato dei ministri del Consiglio d'Europa. L'obiettivo della CEPEJ è il miglioramento dell'efficienza e del funzionamento della giustizia negli Stati membri e lo sviluppo dell'attuazione degli strumenti adottati a tal fine dal Consiglio d'Europa. La commissione predispone ogni due anni una relazione sullo stato dei sistemi di giustizia nazionale, stimandone la qualità, i tempi, la composizione di genere, sulla base di parametri come il *budget*, il personale, l'organizzazione, il numero delle decisioni.

[49] S. QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *Leg. pen.*, 18 dicembre 2018.

[50] Le linee guida sono state formulate dal Gruppo di esperti di alto livello sull'intelligenza artificiale, e sono consultabili sul sito *web* della Commissione europea.

stati elaborati sette principi etici non vincolanti, finalizzati a garantire che l'IA sia sicura ed eticamente valida. I sette principi comprendono: intervento e sorveglianza umani, robustezza tecnica e sicurezza, vita privata e *governance* dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale, responsabilità. È anche precisato che i sistemi di IA sono sviluppati e utilizzati come strumenti al servizio delle persone, nel rispetto della dignità umana e dell'autonomia personale, e funzionano in modo da poter essere adeguatamente controllati e sorvegliati dagli individui.

È proprio a tali principi che si è ispirato il Parlamento europeo per stilare la Proposta di Regolamento[51]. L'obiettivo generale della proposta di legge sull'IA, presentata nell'aprile 2021, era quello di garantire il corretto funzionamento del mercato unico creando le condizioni per lo sviluppo e l'uso di sistemi di IA affidabili nell'Unione. Il progetto stabiliva un quadro giuridico armonizzato per lo sviluppo, l'immissione sul mercato e l'uso di prodotti e servizi di IA. Inoltre, la proposta di legge mirava a conseguire una serie di obiettivi specifici: (i) garantire che i sistemi di IA immessi sul mercato dell'UE siano sicuri e rispettino il diritto comunitario esistente, (ii) assicurare la certezza del diritto per facilitare gli investimenti e l'innovazione nell'IA, (iii) migliorare la *governance* e l'effettiva applicazione del diritto comunitario in materia di diritti fondamentali e requisiti di sicurezza applicabili ai sistemi di IA, oltre a facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili e prevenire la frammentazione del mercato. Il punto di partenza doveva essere quello di introdurre nel diritto comunitario una definizione dei sistemi di IA neutra dal punto di vista tecnologico e di stabilirne una classificazione con requisiti e obblighi diversi, adattati in funzione di un approccio «*risk-based*».

Il Consiglio ha approvato la posizione generale degli Stati membri dell'UE nel dicembre 2021 e il Parlamento ha votato sulla sua posizione nel giugno 2023. I legislatori dell'UE hanno infine approvato il testo definitivo in data 14 marzo 2024, con alcune modifiche alla proposta della Commissione, tra cui la revisione della

[51] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, *Il regolamento europeo sull'IA*, in *i-lex – Riv. di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale*, 2/2021; A. GIANNINI, *Intelligenza artificiale, human oversight e responsabilità penale: prove d'impatto a livello europeo*, in *Criminalia*, 2021, p. 249 ss.

definizione dei sistemi di IA e l'ampliamento dell'elenco di quelli ad alto rischio e vietati, un sistema di *governance* a livello europeo, l'introduzione di una valutazione d'impatto sui diritti fondamentali, la limitazione dei modelli di IA generativa come *ChatGPT*[52].

Il nuovo quadro normativo, basato sull'articolo 114 e sull'articolo 16 del trattato sul funzionamento dell'Unione europea (TFUE), conferma quella che è una definizione di sistemi di IA neutrale dal punto di vista tecnologico e adotta il già citato approccio *risk-based*, che stabilisce diversi requisiti e obblighi per il loro sviluppo, l'immissione sul mercato e l'uso nell'UE[53]. In pratica, la legge definisce requisiti obbligatori comuni applicabili alla progettazione e allo sviluppo dei predetti sistemi prima della loro immissione sul mercato e armonizza le modalità di esecuzione dei controlli *ex post*.

Le nuove norme si applicherebbero principalmente a coloro che forniscono o utilizzano sistemi di IA all'interno del mercato europeo, o li mettono in servizio nei Paesi dell'UE. Allo scopo di evitare l'elusione delle nuove norme, esse si

[52] Si tratta di un sistema di intelligenza artificiale cosiddetta generativa. GPT sta per *Generative Pre-trained Transformer*. Il sistema lavora attraverso una rete neurale progettata per l'elaborazione del linguaggio su un *set* di dati di oltre 45 *terabyte* di testo proveniente da *internet* (libri, articoli, siti *web* e altri contenuti testuali). Il modello di base, GPT-3, rilasciato nel novembre 2022, viene perfezionato costantemente e la nuova versione, GPT-4, è stata rilasciata nel marzo 2023. Mentre quest'ultimo rappresenta una versione *premium* a pagamento, il primo è generalmente accessibile attraverso un sito web facile da usare: https://chat.openai.com/chat. Sul punto si veda L. ROMANÒ, *La responsabilità penale al tempo di ChatGPT: prospettive de iure condendo in tema di gestione del rischio da intelligenza artificiale generativa*, in *Sist. Pen.*, 1/2023, p. 70 ss.; EUROPOL INNOVATION LAB, *The criminal use of ChatGPT – a cautionary tale about large language models*, 2023; GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori*, comunicato stampa del 31 marzo 2023, consultabile sul sito *web* www.garanteprivacy.it, nella sezione Stampa e comunicazione; G. FIORINELLI, *Il concorrente virtuale: la prevenzione dell'uso di ChatGPT per finalità criminali tra etero- e auto-regolazione*, in *Riv. it. med. leg.*, 2/2023, p. 361 ss.; L. CALIFANO, *Chat GPT e Meta EDI: spunti problematici su profili regolatori e ruolo delle autorità di controllo di protezione dati*, in *federalismi.it*, 10/2023; L. MEGALE, *Il Garante della "privacy" contro "ChatGPT": quale ruolo per le autorità pubbliche nel bilanciare sostegno all'innovazione e tutela dei diritti?*, in *Giornale di diritto amministrativo*, 3/2023, p. 403 ss.; G. DE MINICO, *Too many rules or zero rules for the ChatGPT?*, in *BioLaw Journal*, 2/2023, p. 491 ss..

[53] A tal proposito si vedano i punti 26 e 27 del testo approvato.

applicherebbero anche ai fornitori e agli utenti di sistemi di IA situati in un paese terzo, la cui produzione sia utilizzata anche nell'UE[54].

5.2. Documenti e normative italiane

Anche l'Italia ha iniziato a sviluppare una propria strategia per lo sviluppo dell'intelligenza artificiale e ha messo in atto una serie di misure e iniziative per regolare e incentivare l'uso etico e sicuro dell'IA. Merita menzione il documento intitolato Strategia italiana per l'intelligenza artificiale, approvato per la prima volta nel novembre 2021 e da ultimo aggiornato a luglio 2024[55]. L'ultima versione del testo è indirizzata a regolamentare il biennio successivo alla sua pubblicazione, con l'obiettivo di garantire che l'Italia sia all'avanguardia nello sviluppo etico, sicuro e innovativo dell'IA.

La strategia si pone come obiettivo principale quello di promuovere l'adozione di tale tecnologia nei settori pubblico e privato per migliorare la competitività dell'Italia, favorendo l'innovazione industriale e rispondendo a esigenze di modernizzazione e digitalizzazione in vari settori.

La sanità, ad esempio, è vista come un campo in cui l'intelligenza artificiale potrebbe rivoluzionare diagnosi e trattamenti, portando a una medicina più precisa e personalizzata. Allo stesso modo, nell'industria, il ricorso all'intelligenza artificiale può ottimizzare i processi produttivi, ridurre i costi e migliorare la qualità del prodotto

---

[54] S. BECK, *Google Cars, Software Agents, Autonomous Weapons Systems. New Challenges for Criminal Law*, in E. Hilgendorf E U. Seidel (eds.), *Robotics, Autonomics and the Law: Legal issues arising from the AUTONOMICS for Industry 4.0 Technology Programme of the German Federal Ministry for Economic Affairs and Energy,* Nomos, Baden-Baden, 2017, p. 227 ss.; M. B. MAGRO, *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, in *Leg. pen.*, 10 maggio 2020; V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. RUFFOLO, *Intelligenza artificiale - Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020, p. 547 ss.; B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'automa artificiale*, in *Dir. inform.*, 2/2021, p. 317 ss.; I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Riv. it. dir. e proc. pen.*, 1/2021, p. 83 ss.

[55] Il documento completo della Strategia Italiana per l'Intelligenza Artificiale 2024-2026 è consultabile sul sito *web* del Dipartimento per la trasformazione digitale, www.innovazione.gov.it.

finale, mentre nell'agricoltura, le tecnologie intelligenti possono contribuire a una gestione più efficiente delle risorse naturali e alla riduzione degli sprechi.

Un altro aspetto fondamentale è quello della formazione e delle competenze[56]. La strategia sottolinea la necessità di investire nell'istruzione e nella formazione professionale, affinché le nuove generazioni siano in grado di lavorare con l'IA e contribuire alla sua evoluzione. Viene posto un forte accento anche sull'aggiornamento dei lavoratori già attivi, affinché possano adattarsi ai cambiamenti tecnologici che stanno trasformando il mondo del lavoro. La strategia punta a rafforzare la collaborazione tra istituti di ricerca, università e aziende, incentivando lo sviluppo di nuovi progetti e tecnologie. Vengono promossi investimenti nella ricerca e nella sperimentazione di soluzioni innovative, attraverso progetti pilota che permettono di testare concretamente le applicazioni dell'IA in vari ambiti.

Un tema centrale della strategia riguarda poi l'uso etico e regolamentato dell'IA[57]. Il suo sviluppo deve avvenire nel rispetto dei diritti fondamentali, della *privacy* e della sicurezza, garantendo trasparenza e responsabilità. In questo contesto, il

---

[56] Si veda il paragrafo «strategia per la formazione» del citato documento, p. 29 ss. Sul punto la strategia pone due obiettivi: «Promuovere una formazione universitaria capillare sull'IA, in risposta alle sempre più pressanti richieste di nuove competenze nella società e nel mondo del lavoro, in un'ottica trasversale e interdisciplinare; consolidare la formazione specialistica sull'IA nei percorsi orientati verso profili tecnici e di ricercatori, quali il Dottorato Nazionale sull'Intelligenza Artificiale; Realizzare percorsi educativi sull'IA nelle scuole, per preparare le nuove generazioni a un uso attento e consapevole delle nuove tecnologie; sviluppare iniziative di divulgazione mirate a sensibilizzare e coinvolgere la società italiana nella rivoluzione dell'IA; finanziare e sostenere iniziative di *reskilling* e *upskilling* in tutti i contesti produttivi».

[57] A pagina 29 del documento si legge che «Affinché le applicazioni derivanti dall'IA producano effetti positivi su tutta la società, riducendo i rischi, sarà necessario allargare ancora di più il concetto di "formazione", puntando in Italia a implementare un processo di alfabetizzazione sull'IA che coinvolga la scuola, i lavoratori e i cittadini tutti, con attenzione alle categorie più deboli. L'obiettivo è quello di evitare che, in una strategia di crescita e di investimenti sull'IA, si alimentino processi di *digital divide* di conoscenze che, sul lungo periodo, minerebbero la coesione sociale ed economica del Paese. Educare alla cittadinanza digitale al tempo dell'IA è essenziale, peraltro, per colmare il divario di conoscenza e affrontare le preoccupazioni etiche e sociali che può produrre questa tecnologia. Creare percorsi formativi di alfabetizzazione sull'IA nelle scuole, diffondere informazioni attraverso campagne pubblicitarie e promuovere la comprensione delle implicazioni etiche dell'IA rappresentano gli "*step*" fondamentali che possono consentire il corretto orientamento del tessuto socio-economico, nel suo complesso, sulla comprensione del giusto utilizzo dell'IA, cogliendone appieno i vantaggi e valutandone criticamente le limitazioni e i rischi».

piano richiama normative come il GDPR[58] per assicurare una gestione corretta dei dati personali, che sono alla base dell'efficacia dell'IA. È cruciale che l'intelligenza artificiale venga utilizzata in modo sicuro e che i dati siano protetti da eventuali abusi.

Un altro punto centrale della strategia riguarda l'accesso alle informazioni, essenziale per il funzionamento dell'IA. Il documento promuove la creazione di infrastrutture che consentano una condivisione sicura ed efficiente dei dati tra attori pubblici e privati, incentivando lo sviluppo di piattaforme che permettano di sfruttare le informazioni in modo etico e responsabile[59]. Infine, viene previsto un sistema di monitoraggio per valutare i risultati concreti dell'implementazione della strategia[60].

In Italia non esiste ancora una legge specifica dedicata esclusivamente all'IA, ma diverse normative già in vigore regolano alcuni degli aspetti chiave che riguardano questa tecnologia, in particolare in tema di protezione dei dati, sicurezza e responsabilità.

Innanzitutto, l'utilizzo di sistemi di IA, in particolare quelli che coinvolgono dati biometrici o sensibili, è soggetto alle stringenti regole stabilite dal GDPR e dalla normativa italiana sulla protezione dei dati personali (D.lgs. 196/2003 e successive modifiche). Il Garante per la protezione dei dati personali svolge un ruolo cruciale al fine

---

[58] Regolamento 2016/679/UE del Parlamento Europeo e del Consiglio del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati», che abroga la direttiva 95/46/CE («regolamento generale sulla protezione dei dati»).

[59] A pagina 15 del documento si legge: «Per mettere a sistema la conoscenza acquisita in specifiche progettualità e consentire il riuso di artefatti di IA, si realizzerà un programma mirato alla definizione di un registro di *dataset* e modelli, che siano costruiti secondo principi di trasparenza e *fairness*, che siano eticamente affidabili *by design* e che siano riusabili per accelerare le soluzioni delle aziende italiane. La definizione del progetto si articolerà secondo tre macro direzioni: (i) metodologica, al fine definire un protocollo nazionale per garantire che i dataset siano *trustworthy-by-design* e *trusthworthy-by-default* sia legalmente sia ingegneristicamente, definendo approcci per la mitigazione di rischi (in termini etici e di *cyber* sicurezza); (ii) realizzativa, al fine di implementare e rendere disponibile una piattaforma che integri moderni approcci *MLops* e di preparazione dei dati; (iii) applicativa, in cui la piattaforma sarà verticalizzata su specifici ambiti applicativi di interesse nazionale. Tutti i progetti finanziati nell'ambito della strategia nazionale o comunque che riceveranno finanziamenti pubblici saranno tenuti a riportare i *dataset* utilizzati e i modelli prodotti nel registro, in accordo a linee guida che definiranno i livelli di accesso e le modalità di riuso».

[60] Si veda il paragrafo «monitoraggio della strategia» a pagina 36 del documento.

di assicurare che, nell'utilizzo delle tecnologie intelligenti, venga rispettato e protetto al meglio il diritto alla *privacy* dei cittadini.

Il Ministero dello Sviluppo Economico (MiSE) ha avviato diverse iniziative per promuovere lo sviluppo dell'IA in Italia, tra cui la creazione di un Fondo Nazionale Innovazione, volto a finanziare progetti innovativi, comprese le tecnologie legate all'intelligenza artificiale[61]. Inoltre, il MiSE ha supportato la creazione di *sandbox* normative, ambienti regolamentari controllati dove le imprese possono sperimentare l'utilizzo di nuove tecnologie, come l'IA, in un quadro regolamentare flessibile.

[61] Le informazioni riguardanti il Fondo Nazionale Innovazione sono rinvenibili sul sito *web* www.incentivi.gov.it.

Capitolo 2
Intelligenza artificiale, giustizia e diritti fondamentali

1. Approccio precauzionale: l'*AI Act*

L'uso dell'IA, con le sue caratteristiche specifiche, può influire negativamente su una serie di diritti fondamentali e sulla sicurezza degli utenti[1]. Per affrontare queste preoccupazioni, il legislatore ha adottato un approccio basato sul rischio, in base al quale l'intervento giuridico viene calibrato in relazione al livello specifico di pericolo associato all'uso del sistema di intelligenza artificiale.

Il *risk-based approach* proposto dall'UE è una strategia razionale che prevede un'analisi approfondita dei rischi, basata su evidenze scientifiche e dati concreti, al fine di raggiungere un bilanciamento dei benefici, e introdurre un insieme di regole vincolanti che siano proporzionate ed efficaci. Queste norme saranno adattate all'intensità e all'estensione dei pericoli che le attività comportano. Di conseguenza, alcune applicazioni dell'IA, classificate come ad alto rischio, saranno soggette a obblighi stringenti per gli operatori, mentre altre pratiche saranno completamente vietate, poiché i pericoli ad esse associati sono considerati inaccettabili.[2].

L'AI Act classifica i rischi legati all'uso dei sistemi di intelligenza artificiale in quattro categorie: inaccettabile, elevato, limitato e basso o minimo. È quindi essenziale identificare correttamente in quale di queste categorie rientra una specifica attività, al

[1] A. ALAIMO, *Il Regolamento sull'Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico*?, in *federalismi.it*, 25/2023, p. 133 ss.; E. PIETROCARLO, *"Predictive Policing": criticità e prospettive dei sistemi di identificazione dei potenziali criminali*, in *Sistema Penale*, 28 settembre 2023; E. C. RAFFIOTTA, *Dalla "self-regulation" alla "over-regulation" in ambito digitale: come (e perché) di un necessario cambio di prospettiva*, in *Osservatorio sulle fonti*, 2/2023, p. 245 ss.; M. DI FLORIO, *Istigazione all'odio razziale e algoritmi di pericolosità*, in *Giur. it.*, 6/2022, p. 1477 ss.; G. SUFFIA, A. LAVORGNA, S. ICARDI, *Polizia "smart" tra paure e realtà: un'analisi esplorativa sulla rappresentazione mediatica dello "smart policing" in Italia*, in *Studi sulla questione criminale*, 3/2022, p. 95 ss.

[2] Si veda il punto 26 del testo approvato.

fine di applicare la normativa appropriata. Per determinare quali sistemi siano da considerarsi ad alto rischio, si tiene conto dell'impatto negativo potenziale che tali sistemi possono avere sui diritti tutelati dalla Carta dei diritti fondamentali dell'Unione Europea[3].

L'AI Act specifica inoltre che i minori godono di una tutela particolare, come stabilito dall'articolo 24 della Carta dei diritti fondamentali dell'Unione Europea e dalla Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza. Questi documenti sottolineano l'importanza di considerare le vulnerabilità dei minori e di assicurare loro la protezione e l'assistenza necessarie per il loro benessere. I sistemi classificati come ad alto rischio dovranno rispettare una serie di requisiti stringenti, tra cui la *governance* dei dati, la documentazione tecnica e la sicurezza informatica. Inoltre, sono previste misure di trasparenza, come l'adozione di istruzioni d'uso, e meccanismi per garantire la supervisione umana degli algoritmi.

L'*AI Act* elenca, poi, una serie di pratiche vietate, tra cui le tecniche di manipolazione cognitivo comportamentale[4], utilizzate per influenzare e modificare pensieri, emozioni e comportamenti delle persone, basate su principi psicologici che mirano a indirizzare decisioni e atteggiamenti, spesso senza che il soggetto ne sia consapevole; il riconoscimento delle emozioni nei luoghi di lavoro o a scuola[5], che analizza le

[3] Tra questi la legge stessa ricorda, al punto 48, «il diritto alla dignità umana, il rispetto della vita privata e della vita familiare, la protezione dei dati personali, la libertà di espressione e di informazione, la libertà di riunione e di associazione e la non discriminazione, il diritto all'istruzione, la protezione dei consumatori, i diritti dei lavoratori, i diritti delle persone con disabilità, l'uguaglianza di genere, i diritti di proprietà intellettuale, il diritto a un ricorso effettivo e a un giudice imparziale, i diritti della difesa e la presunzione di innocenza e il diritto a una buona amministrazione».

[4] Il punto 29 del testo approvato spiega che «le tecniche di manipolazione basate sull'IA possono essere utilizzate per persuadere le persone ad adottare comportamenti indesiderati o per indurle con l'inganno a prendere decisioni in modo da sovvertirne e pregiudicarne l'autonomia, il processo decisionale e la scelta […] con il rischio di causare danni significativi, in particolare aventi effetti negativi sufficientemente importanti sulla salute fisica, psicologica o sugli interessi finanziari. […] Tali sistemi di IA impiegano componenti subliminali quali stimoli audio, grafici e video che le persone non sono in grado di percepire poiché tali stimoli vanno al di là della percezione umana o altre tecniche manipolative o ingannevoli che sovvertono o pregiudicano l'autonomia, il processo decisionale o la libera scelta di una persona senza che ne sia consapevole o, se ne è consapevole, senza che sia in grado di controllarle o resistervi o possa evitare l'inganno».

[5] Punto 44 del testo approvato: «Sussistono serie preoccupazioni in merito alla base scientifica dei sistemi di IA volti a identificare o inferire emozioni. […] Tra le principali carenze di tali sistemi

espressioni facciali, la voce e i gesti al fine di identificare e monitorare lo stato emotivo di studenti o lavoratori, con l'obiettivo di migliorare il benessere o la produttività; il *social scoring*[6], che valuta il comportamento degli individui assegnando loro un punteggio basato su dati raccolti da attività sociali e finanziarie e online, al fine di misurare l'affidabilità o la conformità a determinati *standard*; e infine la polizia predittiva[7], che verrà analizzata nel capitolo 2.

Si è discusso in sede di approvazione del testo definitivo circa l'uso di sistemi di IA di identificazione biometrica remota «in tempo reale» delle persone fisiche in spazi accessibili al pubblico. Il legislatore europeo ha ritenuto che questa pratica andasse vietata in quanto particolarmente invasiva dei diritti e delle libertà delle persone interessate «nella misura in cui potrebbe avere ripercussioni sulla vita privata di un'ampia fetta della popolazione, farla sentire costantemente sotto sorveglianza e scoraggiare

figurano la limitata affidabilità, la mancanza di specificità e la limitata generalizzabilità. Pertanto, i sistemi di IA che identificano o inferiscono emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici possono portare a risultati discriminatori e possono essere invasivi dei diritti e delle libertà delle persone interessate. Considerando lo squilibrio di potere nel contesto del lavoro o dell'istruzione, combinato con la natura invasiva di tali sistemi, questi ultimi potrebbero determinare un trattamento pregiudizievole o sfavorevole di talune persone fisiche o di interi gruppi di persone fisiche. È pertanto opportuno vietare l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA destinati a essere utilizzati per rilevare lo stato emotivo delle persone in situazioni relative al luogo di lavoro e all'istruzione».

[6] Punto 31 del testo approvato: «I sistemi di IA che permettono ad attori pubblici o privati di attribuire un punteggio sociale alle persone fisiche possono portare a risultati discriminatori e all'esclusione di determinati gruppi. Possono inoltre ledere il diritto alla dignità e alla non discriminazione e i valori di uguaglianza e giustizia. Tali sistemi di IA valutano o classificano le persone fisiche o i gruppi di persone fisiche sulla base di vari punti di dati riguardanti il loro comportamento sociale in molteplici contesti o di caratteristiche personali o della personalità note, inferite o previste nell'arco di determinati periodi di tempo».

[7] Punto 42 del testo approvato: «In linea con la presunzione di innocenza, le persone fisiche nell'Unione dovrebbero sempre essere giudicate in base al loro comportamento effettivo. Le persone fisiche non dovrebbero mai essere giudicate sulla base di un comportamento previsto dall'IA basato unicamente sulla profilazione, sui tratti della personalità o su caratteristiche quali la cittadinanza, il luogo di nascita, il luogo di residenza, il numero di figli, il livello di indebitamento o il tipo di automobile, senza che vi sia un ragionevole sospetto che la persona sia coinvolta in un'attività criminosa sulla base di fatti oggettivi verificabili e senza una valutazione umana al riguardo. Pertanto, dovrebbero essere vietate le valutazioni del rischio effettuate in relazione a persone fisiche intese a determinare il rischio che queste ultime commettano un reato o volte a prevedere il verificarsi di un reato effettivo o potenziale unicamente sulla base della loro profilazione o della valutazione dei loro tratti della personalità e delle loro caratteristiche».

in maniera indiretta l'esercizio della libertà di riunione e di altri diritti fondamentali»[8]. Il divieto è giustificato anche dall'impossibilità di eseguire controlli ulteriori o apportare correzioni in tempo reale, in relazione all'uso di tali sistemi, i quali operano in maniera istantanea e possono quindi incrementare significativamente i pericoli per i diritti e le libertà delle persone coinvolte.

Tuttavia, il legislatore ha previsto un'area di rischio consentito, circoscritta a una serie tassativa di situazioni in cui l'uso dei sistemi di IA è considerato strettamente necessario per perseguire un interesse pubblico rilevante, ritenuto di importanza superiore rispetto ai rischi associati[9].

In questo contesto, si è effettuato un bilanciamento con i benefici, considerando anche le evidenze scientifiche disponibili. Il Parlamento europeo ha ritenuto che, in determinati casi, i vantaggi derivanti dall'uso di tali sistemi possano essere sufficientemente rilevanti da giustificare l'accettazione dei rischi connessi.

Come noto, l'ordinamento giuridico spesso consente lo svolgimento di attività intrinsecamente pericolose, in cui gli eventi dannosi sono in buona parte prevedibili e non sempre evitabili, a causa della loro elevata utilità sociale[10]. In tali ipotesi viene in rilievo una logica precauzionale: se un'attività può causare danni gravi, anche in

---

[8] Punto 32 del testo approvato.

[9] Tali situazioni comprendono la ricerca di vittime di reato, comprese le persone scomparse, di determinate minacce per la vita o l'incolumità fisica delle persone o un attacco terroristico nonché la localizzazione o l'identificazione degli autori o dei sospettati di reati elencati nell'allegato del regolamento. Inoltre, si prevede che questa misura possa essere utilizzata solo per quei reati punibili con una pena o una misura di sicurezza privativa della libertà personale della durata massima di almeno quattro anni, così garantendo che il reato sia sufficientemente grave da giustificare l'uso di questo tipo di identificazione biometrica. Sul punto si veda il punto 33 del testo approvato.

[10] C. BRUSCO, *Rischio e pericolo, rischio consentito e principio di precauzione, La c.d. "flessibilizzazione delle categorie del reato"*, in *Criminalia*, 2012, p. 391; C. PERINI, *Il concetto di rischio nel diritto penale moderno*, Giuffrè, Milano, 2010; C. PERINI, *Adattamento e Differenziazione della Risposta Punitiva nella Società Del Rischio*, in G. Morgante, *Il diritto penale di fronte alle sfide della «Società del rischio». Un difficile rapporto tra nuove esigenze di tutela e classici equilibri di sistema*, Giappichelli, Torino, 2017, p. 455 ss.; D. CASTRONUOVO, *Principio di precauzione e diritto penale: paradigmi dell'incertezza nella struttura del reato*, Aracne, Roma, 2012; A. ORSINA, *Rischio da incertezza scientifica e modelli di tutela penale*, Giappichelli, Torino, 2015; E. CORN, *Il principio di precauzione nel diritto penale. Studio sui limiti all'anticipazione della tutela penale*, Giappichelli, Torino, 2013.

assenza di prove definitive, occorre valutare se tale attività debba essere intrapresa con cautela o evitata del tutto.

Tale logica è nota al diritto penale, che ha elaborato e sviluppato il c.d. principio di precauzione, il quale viene in rilievo quando il legislatore deve intervenire penalmente in contesti di incertezza scientifica. Il legislatore può, infatti, decidere di sottoporre a pena un'attività o un comportamento pericoloso in via precauzionale, anche se non è certo che quel rischio si tradurrà in un'offesa ad un bene giuridico.

1.2. I concetti di rischio e pericolo e il principio di precauzione

Le nozioni di rischio e pericolo possono essere considerate come entrambe indicanti, genericamente, una situazione o una circostanza da cui può derivare un danno[11].

Sul punto si sono sviluppate differenti teorie. Alcuni ritengono che il rischio si identifichi con tutte quelle situazioni in cui le conseguenze possibili di una azione e la loro probabilità di verificarsi sono conosciute in anticipo[12].

Altra parte della dottrina ritiene che tra i due concetti vi sia una differenza di tipo qualitativo[13], per cui il rischio afferisce alla condotta e il pericolo all'evento; altri invece sostengono che la differenza sia di tipo esclusivamente quantitativo, ritenendo che vi sarebbe pericolo in casi di probabilità del verificarsi dell'evento dannoso, mentre rischio quando l'evento sia solamente possibile[14]. In altre parole, il concetto di

---

[11] C. BRUSCO, *Rischio e pericolo, rischio consentito e principio di precauzione*, cit., p. 384.

[12] F. CONSORTE, *Tutela penale e principio di precauzione. Profili attuali, problematicità, possibili sviluppi*, Giappichelli, Torino, 2013, p. 20 ss. L'autrice cita l'Agenzia Europea per l'Ambiente e il d.lgs. n. 334/1999, che definisce il rischio quale «probabilità che un determinato evento si verifichi in un dato periodo o in circostanze specifiche», mentre il pericolo viene inteso quale «proprietà intrinseca di una sostanza pericolosa o della situazione fisica esistente in uno stabilimento di provocare danni per la salute umana o per l'ambiente».

[13] V. MILITELLO, *Rischio e responsabilità penale*, Giuffrè, Milano, 1988, p. 17 ss.

[14] C. BRUSCO, *Rischio e pericolo, rischio consentito e principio di precauzione*, cit., 383; G. MARINI, *"Rischio consentito" e tipicità della condotta. Riflessioni*, in *Scritti in memoria di Renato Dell'Andro*, Cacucci Editore, Bari, 1994, vol. II, p. 542 ss. L'autore afferma che «il "pericolo" null'altro è se non un "rischio" caratterizzato da un'alta possibilità di verificazione del danno all'interesse considerato».

rischio ricorrerebbe nelle ipotesi in cui la pericolosità di una condotta o la sua attitudine a provocare danni sono dubbie, e cioè non si hanno certezze circa la probabilità del verificarsi di una lesione.

Sembrerebbe, pertanto, che la distinzione tra pericolo e rischio si basi su due concetti chiave. Il pericolo farebbe riferimento all'esistenza di una «potenzialità di danno» intrinseca in una determinata situazione, tecnologia o evento. In altre parole rappresenterebbe la presenza di una fonte di danno, a prescindere dalle probabilità che questo si concretizzi. Il rischio, invece, riguarderebbe la «probabilità» che tale potenzialità di danno si verifichi effettivamente. Mentre il pericolo descrive una situazione che può essere dannosa, il rischio valuta la possibilità concreta che questa situazione porti a conseguenze negative. Nel primo caso il danno è probabile, nel secondo caso ancora no.

A conferma di questa seconda tesi, l'art. 2 lett. r del d. lgs. 9 aprile 2008 n. 81 – seppur nell'ambito specifico della tutela della salute e sicurezza nei luoghi di lavoro – offre una definizione dei due concetti, precisando che si parla di pericolo in caso di «proprietà o qualità intrinseca di un determinato fattore avente il potenziale di causare danni»; al contrario il rischio si configura come «probabilità di raggiungimento del livello potenziale di danno nelle condizioni di impiego o di esposizione ad un determinato fattore o agente oppure alla loro combinazione».

Da questa analisi pare potersi affermare che perché vi sia pericolo ci si deve trovare in presenza di uno stabile sostegno scientifico, incompatibile con il principio di precauzione che invece, come già precisato, si basa su una situazione diversa, quella dell'incertezza scientifica, in cui vi è un'anticipazione della tutela penale ancor più marcata, anche in assenza di prove. Per tale ragione una attività può essere vietata o limitata compatibilmente col principio di precauzione solo in quanto riconducibile al concetto di rischio, senza dovere (né potere) fornire una prova sulla reale probabilità del danno ipotizzato[15].

[15] Per un ulteriore approfondimento si veda, fra tutti, M. DONINI, *Il volto attuale dell'illecito penale. La democrazia penale tra differenziazione e sussidiarietà*, Giuffrè, Milano, 2004, p. 120 ss.; C. PIERGALLINI, *Danno da prodotto e responsabilità penale. Profili dommatici e politico-criminali*, Giuffrè, Milano, 2004, p. 449 ss.; A. GARGANI, *Il danno qualificato dal pericolo. Profili sistematici e politico-criminali dei delitti contro l'incolumità*

Il principio di precauzione in materia penale, quindi, agisce in primo luogo come «criterio metodologico», orientando l'intervento legislativo nella regolamentazione di attività rischiose[16].

Qualora a fronte di rischi elevati, tuttavia, vi sia un livello di conoscenza scientifica limitata o incompleta, tanto da non poter correttamente gestire la situazione o poterne prevedere le conseguenze, occorrerà astenersi dall'agire, dal momento che non sarebbe possibile assicurare un idoneo controllo dei pericoli[17].

Questa scelta è anzitutto di natura politica, e quindi extrapenale[18]. Consiste infatti nel decidere quale grado di rischio si è disposti a tollerare nell'utilizzo di una certa tecnologia.

La Comunicazione della Commissione sul Principio di Precauzione, COM (2000) 1° febbraio 2002[19] precisa che, in una situazione di incertezza scientifica e a fronte di richieste più o meno pressanti da parte dell'opinione pubblica, la positiva adozione di misure non è l'unica via possibile, visto che «anche la decisione di non agire può costituire una risposta»[20].

Maggiori problemi nascono, invece, qualora si decida che i benefici siano tali da dover consentire l'attività, o qualora si ritenga di poter controllare i rischi da essa nascenti. In questa ipotesi, il legislatore dovrà apprestare tutte le misure idonee a gestire preventivamente i problemi inerenti alla tecnologia in esame, ritagliando appunto

---

pubblica, Giappichelli, Torino, 2005, p. 96 ss.; L. FOFFANI, *Responsabilità per il prodotto e diritto comunitario: verso un nuovo diritto penale del rischio? Note comparatistiche sugli ordinamenti italiano e spagnolo*, in Donini – Castronuovo (a cura di) *La riforma dei reati contro la salute pubblica*, CEDAM, Padova, 2007, p. 152 ss.

[16] D. PULITANÒ, *Gestione del rischio da esposizioni professionali*, in *Cass. pen.*, 2/2006, p. 787; F. GIUNTA, *Il diritto penale e le suggestioni del principio di precauzione*, in *Criminalia*, 2006, p. 227 ss.

[17] G. FORTI, *Colpa ed evento nel diritto penale*, Giuffrè, Milano, 1990, p. 465.

[18] L. ROMANÒ, *La responsabilità penale al tempo di ChatGPT*, cit., p. 9; L. STORTONI, *Angoscia tecnologica ed esorcismo penale*, in *Riv. it. dir. e proc. pen.*, 1/2004, p. 71 ss.

[19] La Comunicazione è consultabile tramite il sito *web* della dell'Unione europea, www.eur-lex.europa.eu.

[20] Vedi paragrafo 5.2.1. della Comunicazione della Commissione.

aree di rischio consentito[21], presidiate da un apparato di sanzioni adeguato e funzionale alla tutela degli interessi coinvolti[22].

La crescita costante delle situazioni di incertezza come conseguenza dell'evoluzione scientifica e tecnologica ha portato alla creazione della cosiddetta società del rischio, nell'ambito della quale si afferma il principio di precauzione, strettamente legato al mutamento dei rischi e della percezione degli stessi[23].

Il principio di precauzione opera proprio in situazioni di incertezza scientifica e quindi anticipa la soglia al di là della quale scattano le misure preventive, mentre quello di prevenzione riguarda danni solamente potenziali.

Il principio in esame serve ad evitare che una situazione di rischio si possa tramutare in situazione di emergenza. Solo attraverso un corretto approccio precauzionale e una approfondita valutazione dei pericoli connessi all'esercizio di determinate attività si può evitare l'insorgenza di danni gravi e irreparabili.

Fondamentale è, dunque, una corretta strategia di gestione del rischio che solo come *ultima ratio* deve portare al divieto dell'attività[24].

Con la formula «incertezza scientifica» si intende descrivere una situazione in cui la pericolosità di una condotta, un prodotto o una sostanza non sia corroborata da consolidate evidenze scientifiche, i dati accertati al riguardo siano discordanti o non pienamente dimostrati, ma si ipotizza l'eventualità di una minaccia nei confronti di beni giuridici tutelati dall'ordinamento[25].

---

[21] C. PERINI, *Il concetto di rischio nel diritto penale moderno*, cit.

[22] Così D. PIVA, *Machina discere, (deinde) delinquere et puniri potest*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, cit., p. 681 ss.

[23] R. TITOMANLIO, *Il principio di precauzione fra ordinamento europeo e ordinamento italiano*, 2018, Giappichelli, Torino, pag. XIII. Si veda anche G. MANFREDI, *Note sull'attuazione del principio di precauzione in diritto pubblico*, in *Riv. trim. dir. pubbl.*, 3/2004, p. 1075 ss.

[24] R. TITOMANLIO, *Il principio di precauzione fra ordinamento europeo e ordinamento italiano*, cit., p. 44.

[25] C. RUGA RIVA, *Principio di precauzione e diritto penale. Genesi e contenuto della colpa in contesti di incertezza scientifica*, in E. Dolcini; C.E. Paliero (a cura di), S*tudi in onore di Giorgio Marinucci*, Giuffrè, Milano, 2006, p. 1743 ss.; D. CASTRONUOVO, *Principio di precauzione e diritto penale: paradigmi dell'incertezza nella struttura del reato*, cit.; C. E. PALIERO, *La Società punita: del come, del perché e del per cosa*, in *Riv. it. dir. e proc. pen.*, 4/2008, p. 1516 ss.; F. CONSULICH, *Flash Offenders. Le prospettive di accountability penale nel contrasto alle intelligenze artificiali devianti*, in *Riv. it. dir. e proc. pen.*, 3/2022, p. 1015 ss.

Data la situazione di incertezza si ritiene che lo svolgimento di un'attività comporti dei rischi, i quali tuttavia non possono essere interamente dimostrati. In tale contesto il principio di precauzione impone di adottare tutte le misure necessarie per garantire la sicurezza, anche giungendo eventualmente a vietare lo svolgimento dell'attività stessa[26].

In dottrina ci si è chiesti se il principio in esame costituisca solamente un criterio interpretativo di fattispecie di reato già presenti nell'ordinamento, oppure se possa essere considerato come un criterio di imputazione e, pertanto, ispirare un intervento legislativo.

Normalmente il dubbio mal si concilia con l'accertamento della responsabilità penale, che deve basarsi su fatti scientificamente valutabili, giuridicamente accertabili in termini di certezza o, perlomeno, di elevata credibilità razionale[27]. Il fatto di disciplinare una determinata situazione, dal punto di vista penale, in via precauzionale si

---

[26] A. MASSARO, *Principio di precauzione e diritto penale: nihil novi sub sole?*, in *Dir. pen. cont.*, 9 maggio 2011.

[27] C. RUGA RIVA, *Principio di precauzione e diritto penale*, cit., p. 1749. Può essere svolto un ulteriore approfondimento sul ruolo del dubbio nella condanna penale, dal momento che l'art. 533 c.p.p. prevede che «il giudice pronuncia sentenza di condanna se l'imputato risulta colpevole del reato contestatogli al di là di ogni ragionevole dubbio». Sul punto si veda V. GAROFOLI, *Dalla non considerazione di colpevolezza alla regola dell'oltre il ragionevole dubbio*, in *Dir. pen. e proc.*, 9/2010, p. 1029 ss.; F. CAPRIOLI, *L'accertamento della responsabilità penale "oltre ogni ragionevole dubbio"*, in *Riv. it. dir. e proc. pen.*, 1/2009, p. 51 ss.; C. PIERGALLINI, *La regola dell'"oltre ragionevole dubbio" al banco di prova in un ordinamento di civil law*, in *Riv. it. dir. e proc. pen.*, 2/2007, p. 593 ss.; G. CARLIZZI, *La regola del ragionevole dubbio nel processo penale, con particolare riguardo al giudizio di cassazione (Nota a Cass. 9 gennaio - 16 giugno 2020, n. 18313, Curca)*, in *Foro it.*, 3/2021, p. 209 ss.; F. J. GAROFOLI, *"Le regole del kaos" tra verità scientifica e ragionevole dubbio*, in *Ind. pen.*, 2/2019, p. 195 ss.; L. SAPONARO, *Il dubbio ragionevole alla ricerca di una definizione*, in *Giur. it.*, 2/2018, p. 469 ss.; O. MAZZA, *Il ragionevole dubbio nella teoria della decisione*, in *Criminalia*, 2012, p. 357 ss.; A. MACCHIA, *Libero convincimento del giudice, dalle prove legali al ragionevole dubbio. Le regole europee*, in *Cass. pen.*, 6/2022, p. 2043 ss.; F. MUNARI, *Il «dubbio ragionevole» nel rinvio pregiudiziale*, in *federalismi.it*, 18/2022, p. 162 ss.; P. MARRA, *La sostenibile certezza nel dubbio. A proposito di un libro di Antonio Incampo e Adolfo Scalfati su "Giudizio penale e ragionevole dubbio"*, in *Diritto & questioni pubbliche*, 1/2020, p. 16 ss.; G, TUZET, *Libero convincimento e ragionevole dubbio secondo Gaetano Carlizzi*, in *Diritto & questioni pubbliche*, 2/2019, p. 13 ss.; G. CARLIZZI, *I due principi costituzionali del giudizio probatorio penale. Repliche a G. Tuzet, "Libero convincimento e ragionevole dubbio secondo Gaetano Carlizzi"*, in *Diritto & questioni pubbliche*, 2/2019, p. 14 ss.; P. DELL'ANNO, *Obbligo di motivazione e "ragionevole dubbio"*, in *Proc. pen. e giust.*, 3/2017, p. 16 ss.; A. FALLONE, *Appello dell'assoluzione, motivazione rafforzata, principio dell'oltre ogni ragionevole dubbio, rinnovazione dibattimentale: la giurisprudenza italiana e della Corte di Strasburgo*, in *Cass. pen.*, 2/2015, p. 820 ss.; E. SOMMA, *"Oltre ogni ragionevole dubbio". Una formula enfatica da contestualizzare: meglio, da evitare*, in *Riv. it. dir. e proc. pen.*, 1/2014, p. 366 ss.

potrebbe giustificare solo con l'esigenza di proteggere degli interessi sospettati di correre un pericolo, anche se questa prudenza dovesse significare una limitazione all'agire o una astensione da determinate condotte.

Occorre precisare che l'applicazione del principio di precauzione non implica necessariamente vietare una certa attività[28]: bisogna decidere se agire o meno e, nel primo caso, in che termini.

Qualora la precauzione lasci spazio per una azione, occorrerà una valutazione dei vari interessi coinvolti anche attraverso il principio di proporzionalità, per cui i limiti imposti dovranno essere commisurati al fine perseguito con l'attività rischiosa.

Nonostante manchi, in dottrina, una precisa definizione del principio di precauzione, esso viene citato più volte sia a livello nazionale che sovranazionale[29].

Per individuare quelli che dovrebbero essere i presupposti per l'applicabilità del principio in esame anche in campo penale si può fare riferimento alla già citata Comunicazione della Commissione sul principio di precauzione[30]. Il documento, con particolare riferimento alla portata del principio in ambito comunitario, chiarisce che lo stesso «comprende quelle specifiche circostanze in cui le prove scientifiche sono insufficienti, non conclusive o incerte e vi sono indicazioni, ricavate da una preliminare valutazione obiettiva, oltre a ragionevoli motivi di temere che gli effetti potenzialmente pericolosi sull'ambiente e sulla salute umana, animale o vegetale possono essere incompatibili con il livello di protezione prescelto»[31].

La stessa Comunicazione, all'art. 5.1.3., afferma che fondamentale per l'applicabilità del principio di precauzione è il contesto di incertezza scientifica finalizzato

---

[28] E. CORN, *Il principio di precauzione nel diritto penale. Studio sui limiti all'anticipazione della tutela penale*, cit., p. 22.

[29] Nell'ordinamento italiano il principio ha ottenuto espliciti riconoscimenti normativi, specie per ciò che attiene alla tutela dell'ambiente, nel d.lgs. n. 152 del 2006 (c.d. codice dell'ambiente) in particolare, agli artt. 3-*ter*, 178, 179, comma 3 e 301. Inoltre, a livello europeo, all'art. 191 del TFUE (ex art. 174 TCE), secondo comma prevede che: «La politica dell'Unione in materia ambientale mira a un elevato livello di tutela, tenendo conto della diversità delle situazioni nelle varie regioni della Comunità. Essa è fondata sui principi della precauzione e dell'azione preventiva, sul principio della correzione, in via prioritaria alla fonte, dei danni causati all'ambiente, nonché sul principio "chi inquina paga"».

[30] Si veda paragrafo 1.2 del presente capitolo.

[31] Si veda l'articolo 3 della Comunicazione di cui alla nota precedente.

proprio a giustificare un'azione in via precauzionale. Tale incertezza deve essere duplice[32], dal momento che deve riguardare sia la plausibilità di una determinata congettura scientifica, e quindi il fatto stesso che una data condotta possa o meno causare un evento dannoso, sia il concreto verificarsi dell'evento stesso, e quindi a quali condizioni esso sia prevedibile.

Le misure adottate in base al principio di precauzione, inoltre, devono essere provvisorie e adattate ai cambiamenti provocati dallo sviluppo scientifico, dal momento che il contesto di incertezza è essenzialmente mutevole grazie ai continui interventi della comunità scientifica che cerca di porvi rimedio attraverso lo studio e l'evoluzione.

Inoltre, la Comunicazione prevede che le misure basate sul principio di precauzione dovrebbero essere non discriminatorie nella loro applicazione, coerenti con misure analoghe già adottate, soggette a revisione alla luce dei nuovi dati scientifici, e in grado di attribuire la responsabilità in caso di danni. Infine, richiede anche che le misure adottate secondo il principio di precauzione siano proporzionate rispetto al livello prescelto di protezione[33].

Il principio di proporzionalità è noto al diritto penale. In forza di questo principio, in sede di scelte di criminalizzazione la pena edittale deve essere commisurata al grado di offesa che la condotta astratta realizza, mentre in sede applicativa il giudice deve irrogare la pena più consona per la condotta concreta[34].

---

[32] C. RUGA RIVA, *Principio di precauzione e diritto penale*, cit., p. 1761.

[33] Si veda pag. 18 della Comunicazione, par. 6.3.1.

[34] Sul punto si veda in dottrina A.S. AGRÒ, *L'eguaglianza in transizione, in Il principio di ragionevolezza nella giurisprudenza della Corte costituzionale – Riferimenti comparatistici*, Giuffrè, Milano, 1994, p. 199 ss.; I. GRIMALDI, *Il principio di proporzionalità della pena nel disegno della Corte Costituzionale*, in *Giurisprudenza Penale Web*, 5/2020, p. 2 ss.; C. LAVAGNA, *Ragionevolezza e legittimità costituzionale*, in *Ricerche sul sistema normativo*, Milano, 1984, p. 650 ss.; S. LEONE, *Sindacato di ragionevolezza e quantum della pena nella giurisprudenza costituzionale*, in *Riv. A.I.C.*, 4/2017, p. 11 ss.; A. MERLO, *Considerazioni sul principio di proporzionalità nella giurisprudenza costituzionale in materia penale*, in *Riv. it. dir. e proc. pen*, 3/2016, p. 1427 ss.; G. SCACCIA, *Gli "strumenti" della ragionevolezza nel giudizio costituzionale*, Giuffrè, Milano, 2000, p. 107 ss.; F. VIGANÒ, *Un'importante pronuncia della Consulta sulla proporzionalità della pena*, in *Dir. pen. cont.*, 14 novembre 2016; N. RECCHIA, *Il principio di proporzionalità nel diritto penale. Scelte di criminalizzazione e ingerenza nei diritti fondamentali*, Giappichelli, Torino, 2020, p. 122 ss.; F. VIGANÒ, *La proporzionalità della pena. Profili di diritto penale e costituzionale*, Giappichelli, Torino, 2021.

Pertanto, a parere della Commissione da una parte le condotte penalmente rilevanti devono essere proporzionate alla pena inflitta e, dall'altra, le misure basate sul principio di precauzione dovrebbero essere proporzionate rispetto al livello di protezione ricercato. Non sarà necessario vietare un'attività per neutralizzarne i rischi, ma potranno essere predisposte misure meno restrittive che consentano di raggiungere un livello di protezione equivalente come, ad esempio, un potenziamento dei controlli, la decisione di introdurre limiti provvisori, raccomandazioni rivolte alle popolazioni a rischio, ecc.

In alcuni casi, invece, un divieto totale potrà essere ritenuto proporzionale ad un rischio eccessivamente alto. Conseguentemente, anche la violazione di un tale divieto dovrà avere una sanzione proporzionata alla gravità del divieto stesso, in ragione del pericolo che si è venuto a creare.

Non è priva di critiche la scelta di chi, in dottrina, arriva a sostenere che il principio di precauzione possa assurgere a criterio di imputazione in materia penale. Questo, infatti, si tradurrebbe nella possibilità di ricollegare una sanzione penale al mancato rispetto delle misure imposte per l'impiego dei sistemi di IA, anche attraverso la creazione di apposite figure di reato. Date le caratteristiche della materia, pare logico fare riferimento alla categoria dei reati di pericolo[35].

Quest'ultima negli ultimi anni è stata notevolmente incrementata con l'introduzione di nuove fattispecie, soprattutto nel campo della circolazione stradale, della sicurezza sui luoghi di lavoro, della sicurezza ambientale e alimentare. Ciò anche a

[35] C. PERINI, *La legislazione penale tra "diritto penale dell'evento" e "diritto penale del rischio"*, in *Leg. pen.*, 1/2012, p. 117 ss.; M. ZINCANI, *Reati di pericolo*, in F. Giunta (a cura di), *Diritto penale*, Giuffrè, Milano, 2008, p. 202 ss.; G. MARINUCCI, E. DOLCINI, G. L. GATTA, *Manuale di diritto penale. Parte generale*, Giuffrè, Milano, 2021, p. 207 ss.; F. PALAZZO, *Corso di diritto penale. Parte generale*, Giappichelli, Torino, 2011, p. 77 ss.; G. FIANDACA, E. MUSCO, *Diritto penale. Parte generale*, Zanichelli, Bologna, 2010; T. PADOVANI, *Diritto penale*, Giuffrè, Milano, 2008, p. 134 ss.; F. GIUNTA, *Il diritto penale e le suggestioni del principio di precauzione*, cit., p. 246; G. FORTI, *"Accesso" alle informazioni sul rischio e responsabilità: una lettura del principio di precauzione*, in *Criminalia*, 2006, p. 155 ss.; V. MANES, *Il principio di offensività. Canone di politica criminale, criterio ermenuetico, parametro di ragionevolezza*, Giappichelli, Torino, 2005, p. 297 ss.; L. STORTONI, *Angoscia tecnologica ed esorcismo penale*, cit., p. 83 ss.; C. PONGILUPPI, *Principio di precauzione e reati alimentari. Riflessioni sul rapporto «a distanza» tra disvalore d'azione e disvalore d'evento*, in *Riv. trim. dir. pen. econ.*, 2010, p. 255 ss.; D. PULITANÒ, *Colpa ed evoluzione del sapere scientifico*, in *Dir. pen. e proc.*, 5/2008, p. 652.

seguito di un rilevante sviluppo delle tecnologie che stanno alla base di questi settori, con un conseguente aumento delle situazioni potenzialmente pericolose per le persone.

Quando si è in presenza di un reato riconducibile alla categoria reati di pericolo c.d. concreto, il giudice dovrà accertare se il bene giuridicamente protetto abbia o meno subito un'effettiva minaccia: si vedano le ipotesi del delitto di strage o di disastro. Perché si configuri il reato, il bene protetto dalla norma incriminatrice deve aver concretamente corso un pericolo[36].

Al contrario, quando si è in presenza di un reato di pericolo c.d. astratto non è necessario che il bene protetto sia stato concretamente minacciato, ma è sufficiente che si realizzi la fattispecie tipica, così come descritta nella norma. È il caso dei delitti di incendio, inondazione, frana o valanga, disastro ferroviario[37].

I reati di pericolo, e in particolare quelli di pericolo astratto, pongono seri problemi di compatibilità con i principi generali del diritto penale, in particolare con quello di offensività, dal momento che il fatto viene punito anche se non si è verificato un danno al bene giuridico tutelato, ma quest'ultimo è stato solo posto in pericolo[38].

---

[36] C. BRUSCO, *Rischio e pericolo, rischio consentito e principio di precauzione*, cit., p. 386. Per un approfondimento sulla categoria dei reati di pericolo concreto si veda L. SIRACUSA, *Leggi scientifiche e ragionevolezza nei reati di pericolo astratto*, in L. de Cataldo Neuburger (a cura di), *La prova scientifica nel processo penale*, CEDAM, Padova, 2007, p. 209 ss.; A. MANNA, *La regola dell'oltre il ragionevole dubbio nel pericolo astratto come pericolo reale*, in *Cass. pen.*, 2/2005, p. 640 ss.; A. NATALINI, *De minimis non curat praetor: diritto penale giurisprudenziale e reati di pericolo astratto, tra tipicità apparente, esiguità del fatto e necessaria offensività*, in *Cass. pen.*, 11/2003, p. 3532 ss.; A. GARGANI, *Il rischio nella dinamica dei reati contro l'incolumità pubblica e nei reati di pericolo astratto*, in *Cass. pen.*, 11/2017, p. 3879 ss.

[37] Parte della dottrina critica il concetto di «pericolo astratto», sul rilievo che se il pericolo è probabilità di un evento temuto, non si può concepire una *species* in cui questa probabilità manchi. Ne deriva che nei casi in cui si ravvisa un pericolo astratto, in realtà non si ha una forma speciale di pericolo, ma una presunzione di pericolo, la quale non ammette prova contraria. Sul punto si veda F. ANTOLISEI, *Manuale di diritto penale. Parte generale*, Giuffrè, Milano, 2017, p. 268 ss.

[38] V. in particolare G. FIANDACA, *La tipizzazione del pericolo*, in *Beni e tecniche di tutela penale,* Franco Angeli, Milano, 1984, p. 67 ss.; Per un approfondimento sul principio di offensività v. G. FIANDACA, *L'offensività è un principio codificabile?*, in *Foro it.*, 124/2001, p. 1 ss.; V. MANES, *Il principio di offensività nel diritto penale*, cit.; G. NEPPI MODONA, *Il lungo cammino del principio di offensività*, in *Studi in onore di Marcello Gallo*, Giappichelli, Torino, 2004, p. 89 ss.; F. PALAZZO, *Offensività e ragionevolezza nel controllo di costituzionalità del contenuto delle leggi penali*, cit., p. 350 ss.

A ben vedere, questo problema si manifesterebbe ancor più ampiamente nel caso di introduzione di un reato di rischio astratto, finalizzato a punire le attività illecite legate all'intelligenza artificiale, le quali – come abbiamo detto – sono connesse al concetto di incertezza dell'esistenza del rischio, con una ancor maggiore anticipazione della tutela penale.

Con riferimento ai reati di pericolo astratto, la dottrina al fine di dare una giustificazione alla loro introduzione, ha ritenuto necessario che gli stessi si basino su un giudizio di pericolosità empiricamente fondato, il quale attesti, nella normalità dei casi (*id quod plerumque accidit*), l'attitudine della condotta penalmente rilevante a ledere il bene oggetto di tutela. Di fronte ad un rischio come sopra definito, invece, si porrebbe quale presupposto del reato proprio la mancata o parziale conoscenza degli effetti dell'attività presa in considerazione[39].

Tuttavia, occorre precisare che l'incertezza scientifica così come sopra definita non comporta necessariamente che non si possa accertare la pericolosità dell'attività stessa. Anche se la scienza non è in grado di dimostrare con sufficiente certezza che tutti i sistemi di intelligenza artificiale siano pericolosi, risulta invero scientificamente verificabile che, ad esempio, un veicolo a guida autonoma che circola su strade pubbliche possa mettere a rischio la vita dei pedoni[40].

---

[39] A. MASSARO, *Principio di precauzione e diritto penale: nihil novi sub sole?*, cit., p. 12; F. ANGIONI, *Il pericolo concreto come elemento della fattispecie penale*, Giuffrè, Milano, 1994, p. 19 ss.; V. MANES, *Il principio di offensività*, cit., p. 293 ss..

[40] Sul punto cfr. L. PICOTTI, *Profili di responsabilità penale per la circolazione di veicoli a guida autonoma*, in *Studi in onore di Antonio Fiorella*, Roma Tre-Press, Roma, 2021; G. CALABRESI, E. AL MUREDEN, *Driveless cars, Intelligenza artificiale e futuro della mobilità*, Il Mulino, Bologna, 2021; A. BERTOLINI, *Robots as Products: The Case for a Realistic Analysis of Robotic Application and Liability Rules*, in *Law, Innovation and Technology*, 2013, p. 214 ss.; E. AL MUREDEN, *Sicurezza "ragionevole" degli autoveicoli e responsabilità del produttore nell'ordinamento giuridico italiano e negli Stati Uniti*, in *Contr. impr.*, 6/2012, p. 1505 ss.; K. VAN WEES, K. BROOKHUIS, *Product Liability for ADAS: legal and human factors perspectives*, in *EJTIR – European Journal of Transport and Infrastructure Research*, 4/2005, p. 357 ss.; A. BERTOLINI, E. PALMERINI, *Regulating robotics: A challenge for Europe,* in *EU Parliament, Workshop on Upcoming issues of EU law for the IURI Committee*, in *Upcoming issues of EU law. Compilation of in-depth analyses*, Publications Office of the EU Parliament, Bruxelles, 2014, p. 169 ss.; J. MANIKA, *Big Data: the next frontier for innovation, competition and productivity, Technical report*, McKinsey Global Institute, 7/2011, sul sito *web* www.mckinsey.com; S. STEFANIZZI, *Riflessioni metodologiche sul concetto e sull'uso dei Big Data*, in S. Gozzo, C. Pennisi, V. Asero, R. Sampugnaro (a cura di), *Big Data e processi decisionali*, Egea, Milano, 2020, p. 17 ss.; C. SEVERONI, *Prime considerazioni su un possibile inquadramento giuridico e sul regime di responsabilità nella conduzione dei veicoli*

Si potrebbe quindi proporre una soluzione a questi dubbi optando per l'introduzione non di fattispecie di pericolo astratto ma, piuttosto, concreto. In questo modo si supererebbe il problema legato all'incertezza scientifica, in quanto si punirebbe la condotta non quando il rischio è ancora incerto, ma solo quando questo si è effettivamente realizzato. Sarebbe salvaguardato anche il principio di offensività, in quanto si punirebbero solo le attività dalle quali sia derivato concretamente un danno (o anche un rischio di danno) per uno dei beni o dei diritti tutelati dall'ordinamento.

Quanto poi, agli elementi soggettivi del reato, il principio di precauzione influenza in larga misura l'interpretazione del criterio da utilizzare in contesti di incertezza scientifica, legittimando l'obbligo di anticipare le cautele[41]. Secondo una logica di rischio, infatti, la precauzione richiede che si adottino delle cautele anche qualora sia dubbio che il loro utilizzo sia idoneo a evitare eventi dannosi, e la mancata adozione delle opportune precauzioni sarebbe fonte di responsabilità penale[42]. Ne consegue che l'agente risponde di tutte le conseguenze causalmente collegate alla mancata adozione delle cautele necessarie, anche se al momento della condotta non era possibile prevedere gli esiti dannosi derivanti dal mancato compimento dell'azione doverosa[43].

---

a guida autonoma, in *Dir. trasp.*, 2018, p. 331 ss. Infine, in D. CERINI, *Dal Decreto Smart Roads in avanti ridisegnare responsabilità e soluzioni assicurative*, in *Danno resp.*, 2018, p. 401, si legge che in futuro dovrà essere valutato, soprattutto da un punto di vista normativo, se mantenere il proprietario del veicolo al «centro di assegnazione del rischio», o identificare altre persone responsabili, richiedendo a queste ultime di adottare nuove forme di assicurazione obbligatoria.

[41] A. CAPPELLINI, *Reati colposi e tecnologie dell'Intelligenza artificiale*, in G. Balbi, A. Esposito, S. Manacorda, F. De Simone (a cura di), *Diritto penale e intelligenza artificiale. Nuovi Scenari*, Giappichelli, Torino, 2023, p. 19 ss.; C. RUGA RIVA, *Principio di precauzione e diritto penale*, cit., p. 1753 ss.

[42] Tale assunto è stato affermato dalla Corte di cassazione in relazione al tema delle esposizioni dei lavoratori a sostanze tossiche, con il caso «Porto Marghera», v. Cass. pen., Sez. IV, 17 maggio 2006, n. 4675, in *Foro it.*, 10/2007, con nota di R. GUARINIELLO, *Tumori professionali a Porto Marghera.*

[43] C. PIERGALLINI, *Il paradigma della colpa nell'età del rischio: prove di resistenza del tipo*, in *Riv. it. dir. e proc. pen.*, 4/2005, p. 1684 ss.; C. PIERGALLINI, *Attività produttive decisioni in stato di incertezza e diritto penale*, in M. Donini, M. Pavarini (a cura di), *Sicurezza e diritto penale*, Bologna University Press, Bologna, 2011, p. 345 ss.; F. GIUNTA, *Il diritto penale e le suggestioni del principio di precauzione*, cit., p. 241 ss.; L. STORTONI, *Angoscia tecnologica*, cit., p. 80; G. FORTI, *"Accesso" alle informazioni sul rischio*, cit., p. 182 ss. e in particolare p. 192; D. PULITANÒ, *Colpa ed evoluzione del sapere scientifico*, cit., p. 651 ss.; A. REGINA, *Colpa ed evento. Note a margine di Cass., Sez. IV, 17 maggio 2006 (caso Marghera)*, in S. Vinciguerra, F. Dassano (a cura di), *Scritti in memoria di Giuliano Marini*, Edizioni Scientifiche Italiane, Napoli, 2010,

Qualora queste cautele siano codificate in precise regole di condotta si parla di colpa specifica, che potrà configurarsi in caso di violazione di regole precauzionali tipizzate dal legislatore al fine di scongiurare determinati rischi, in relazione ad eventi dannosi o pericolosi che ne costituiscano la concretizzazione[44].

Normalmente più l'evento dannoso è prevedibile meno sarà possibile prevenirlo. Si pensi al caso di un'operazione chirurgica in cui è quasi certa la morte del paziente. In questi casi, l'osservanza delle regole cautelari è funzionale ad una riduzione del rischio, il quale tuttavia non può essere eliminato. In queste ipotesi si parla di «rischi inaccettabili o certi» in considerazione del fatto che il nesso di causalità tra il fatto e le possibili conseguenze è scientificamente provato, anche se permangono dubbi sul momento in cui si concretizzerà il rischio stesso[45].

Quando il legislatore decide di ritagliare delle aree di rischio consentito, dispone anche un rafforzamento delle regole di cautela, dal momento che solo una rigorosa osservanza di tali regole potrà fare in modo che il rischio non si realizzi. Inoltre, colui che abbia osservato le regole cautelari non potrà essere ritenuto responsabile, anche

---

p. 728 ss.; F. MARTINI, *Incertezza scientifica, rischio e prevenzione. Le declinazioni penalistiche del principio di precauzione*, in *Responsabilità penale e rischio nelle attività mediche e d'impresa (un dialogo con la giurisprudenza)*, Firenze University Press, Firenze, 2010, p. 587 ss.; G. MINNITI, *Finalità cautelari della norma, sua evoluzione nel tempo e accertamento della colpa*, in *Riv. trim. dir. pen. econ*., 2006, p. 303 ss.

[44] Per un approfondimento sulla nozione di colpa specifica v. M. GROTTO, *Principio di colpevolezza, rimproverabilità soggettiva e colpa specifica*, Giappichelli, Torino, 2012, p. 259 ss.; E. PENCO, *Limiti-soglia e responsabilità colposa. Il ruolo incerto delle soglie quantitative, dalla colpa specifica al rischio consentito*, in *Riv. it. dir. e proc. pen*., 1/2019, p. 195 ss.; G. AMATO, *Un impianto diretto a considerare solo la colpa specifica*, in *Guida dir*., 16/2016, p. 55 ss.; A. M, BONANNO, *Protocolli, linee guida e colpa specifica*, in *Ind. pen*., 1/2006, p. 441 ss.; S. PUGNO, *Accertamento del nesso di causalità e colpa specifica nella circolazione stradale*, in *Giur. it*., 12/2003, p. 2254 ss. G. MARINUCCI, *La responsabilità colposa: teoria e prassi*, in *Riv. it. dir. e proc. pen*., 1/2012, p. 3 ss.; D. CASTRONUOVO, *La colpa penale*, Giuffrè, Milano 2009, pp. 345 e 535; T. PADOVANI, *Il grado della colpa*, in *Riv. it. dir. e proc. pen*., 1969, p. 818 ss.; F. GIUNTA, *Illiceità e colpevolezza nella responsabilità colposa*, CEDAM, Padova, 1993, p. 334 ss.; D. CASTRONUOVO, *L'evoluzione teorica della colpa penale tra dottrina e giurisprudenza*, in *Riv. it. dir. e proc. pen*., 4/2011, p. 1594 ss.; N. MAZZACUVA, *L'apparente prossimità della colpa penale a garantismo e ultima ratio*, in M. Donini, R. Orlandi (a cura di), *Reato colposo e modelli di responsabilità*, Bologna University Press, Bologna, 2013, p. 41 ss.; S. THOBANI, *Percorsi giurisprudenziali in tema di accertamento dell'elemento soggettivo della P.A.: colpa generica e colpa specifica*, in *Giur. it*., 1/2013, p. 189 ss.

[45] P. VENEZIANI, *Regole cautelari "proprie" ed "improprie" nella prospettiva delle fattispecie colpose causalmente orientate*, CEDAM, Padova, 2003, p. 1235 ss. L'autore afferma che in queste ipotesi le relative regole cautelari sono regole cautelari «improprie», che mirano ad una riduzione del rischio di eventi dannosi, mentre «proprie» sono quelle che consentono di eliminare il rischio.

qualora non sia stato possibile evitare il verificarsi dell'evento[46].

Tuttavia, il fatto che il rischio non sia eliminabile non comporta un'attenuazione degli obblighi di garanzia, ma anzi verrà richiesto un maggior livello di diligenza, prudenza e perizia al fine di ridurre il rischio consentito nei limiti del possibile. Per fare un esempio, si pensi alle corse automobilistiche, in cui è possibile superare i limiti di velocità normalmente previsti nelle strade pubbliche. Questo certamente aumenta la probabilità di incidenti – anche mortali – ma è consentito in presenza di tutta una serie di precise e stringenti regole imposte al circuito e a colui che conduce il veicolo[47].

Da qui l'importanza della tipizzazione di regole precauzionali, dal momento che è più difficile riscontrare, a fronte della violazione di un generale obbligo di precauzione, un'ipotesi di colpa generica[48].

In questo senso, il principio di precauzione richiederebbe al legislatore la creazione di regole cautelari positive per l'uso dei sistemi di intelligenza artificiale, che possano di conseguenza configurare ipotesi di responsabilità penale per colpa (specifica) in caso di mancato rispetto delle stesse.

L'*AI Act,* pur senza prevedere tali tipologie di regole, sembra fornire un primo quadro orientativo di misure cautelari e obblighi specificamente concernenti la messa in commercio e l'uso di sistemi IA (artt. 8-15). Come già precisato nei paragrafi precedenti, l'*AI Act* propone una regolazione dell'AI proporzionata alla probabilità, al tipo e all'intensità del rischio rilasciato dall'applicazione che si intenda regolare (c.d.

---

[46] C. BRUSCO, *Rischio e pericolo, rischio consentito e principio di precauzione*, cit., p. 392; F. LA VATTIATA, *La responsabilità penale per danni da intelligenza artificiale alla prova del processo*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, E M. Proto (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, cit.

[47] C. BRUSCO, *Rischio e pericolo, rischio consentito e principio di precauzione*, cit., p. 394.

[48] Quanto alla nozione di colpa generica v. A. ZACCHIA, *L'individuazione della regola cautelare non scritta in tema di colpa generica*, in *Cass. pen.*, 6/2014, p. 2114 ss.; F. BASILE, *Fisionomia e ruolo dell'agente-modello ai fini dell'accertamento processuale della colpa generica*, in G. A. De Francesco, C. Piemontese, E. Venafro (a cura di), *La prova dei fatti psichici,* Giappichelli, Torino 2010, p. 94 ss.; G. MARINUCCI, *La responsabilità colposa: teoria e prassi*, cit., p. 5; D. CASTRONUOVO, *La colpa penale*, cit., p. 345 ss.; T. PADOVANI, *Il grado della colpa*, cit., p. 818 ss; F. GIUNTA, *Illiceità e colpevolezza nella responsabilità colposa*, cit., p. 334 ss.; D. CASTRONUOVO, *L'evoluzione teorica della colpa penale tra dottrina e giurisprudenza*, cit., p. 1597; N. MAZZACUVA, *L'apparente prossimità della colpa penale a garantismo e ultima ratio*, cit., p. 41 ss.; S. THOBANI, *Percorsi giurisprudenziali in tema di accertamento dell'elemento soggettivo della P.A.: colpa generica e colpa specifica*, cit., p. 189 ss.

approccio *risk-based*)[49], individuando differenti classi di rischio e i rispettivi regimi regolatori, compatibilmente con quello che abbiamo definito essere il principio di precauzione[50].

In particolare, per le IA ad alto rischio, la logica utilizzata dalla proposta è quella di una precauzione cosiddetta moderata: la proposta stabilisce i limiti entro i quali è accettabile che un sistema di IA compia errori o causi danni, statuendo espressamente che le figure soggettive tipizzate (ossia, il produttore, programmatore e l'utilizzatore della macchina, persona fisica o giuridica) siano gravate da obblighi di condotta tipici articolati e complessi[51]. A diversi livelli di rischio corrisponde un proporzionale dovere di intervento umano, anche al fine di individuare un soggetto responsabile qualora tale rischio si concretizzi ed egli risulti inadempiente rispetto ai propri obblighi di sorveglianza.

Per fare un esempio, l'art. 14 dell'*AI Act*, al fine di ridurre al minimo i rischi connessi all'attività, impone al fornitore o utilizzatore della macchina di adottare delle misure tecniche ed organizzative idonee a garantire un livello di controllo e intervento umano adeguato.

L'AI Act, dunque, non detta specifiche regole cautelari per i vari utilizzi dei sistemi di intelligenza artificiale, ma si limita a imporre a determinati soggetti, ritenuti responsabili, di modulare la concreta attuazione dei principi sanciti, in astratto, dalla normativa in materia. In questa prospettiva, è immediatamente evidente la centralità attribuita al principio della supervisione umana nella gestione dei sistemi ad alto rischio[52].

Un tale approccio pone rilevanti problemi, in quanto, in assenza di precise regole cautelari predeterminate (o comunque troppo vaghe), si assisterebbe alla formulazione di vere proprie norme precauzionali «retroattive», individuate solo dopo che

---

[49] G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, *Il regolamento europeo sull'IA*, cit.

[50] L. ROMANÒ, *La responsabilità penale al tempo di ChatGPT*, cit., p. 10.

[51] Per i sistemi ad alto rischio, la proposta prevede obblighi di qualità dei *dataset* che alimentano il sistema (art. 10), documentazione (art. 11), registrazione degli eventi (art. 12) e trasparenza (art. 13), funzionale alla valutazione dei rischi *ex ante* (art. 9) e alla sorveglianza umana (art. 14), oltre che alla prevenzione di discriminazioni, nonché di affidabilità (art. 15).

[52] L. ROMANÒ, *La responsabilità penale al tempo di ChatGPT*, cit., p. 10.

il rischio si è già avverato, le quali risulterebbero necessarie per riuscire ad attribuire la responsabilità a qualcuno[53].

In questo modo il principio di precauzione porterebbe ad una stasi in quanto, a fronte di un rischio così vago e di un comportamento diligente non precisato, la scelta più sicura per l'agente sarebbe proprio quella di non agire[54]. Dal punto di vista processuale, inoltre, il soggetto dovrebbe dimostrare di aver fatto tutto il possibile per evitare il danno, e potrebbe essere condannato solo perché, a parere del giudice, avrebbe dovuto aspettarsi che ci fosse un rischio legato all'attività posta in essere.

Il problema non potrebbe dirsi risolto neanche facendo riferimento alla colpa generica e quindi ad una vaga violazione di regole non codificate di diligenza prudenza e perizia, perché in questa ipotesi bisognerebbe comunque stabilire quale dovrebbe essere il comportamento dell'agente modello. In contesti caratterizzati da un sapere scientifico in evoluzione è più complesso individuare il momento a partire dal quale si può pretendere che l'agente riconosca i rischi connessi ad una certa attività e, quindi, si attivi per impedirne i possibili sviluppi lesivi[55].

1.3. Il principio di precauzione come criterio di imputazione della responsabilità penale dell'IA

A seguito dell'analisi che precede occorre domandarsi se il principio di precauzione possa ergersi ad autonomo criterio di imputazione della responsabilità penale,

---

[53] A. MASSARO, *Principio di precauzione e diritto penale: nihil novi sub sole?*, cit., p. 17.

[54] Sul punto si veda V. ATTILI, *L'agente-modello "nell'era della complessità": tramonto, eclissi o trasfigurazione?*, in *Riv. it. dir. e proc. pen.*, 2006, p. 1289 ss.; C. PIERGALLINI, *Danno da prodotto*, cit., pp. 276 e 415 ss; F. GIUNTA, *Il diritto penale e le suggestioni del principio di precauzione*, cit., p. 231 ss.; C. R. SUNSTEIN, *Il diritto della paura. Oltre il principio di precauzione*, Il Mulino, Bologna, 2010, p. 42 ss.

[55] Sul punto si veda 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 ss.; A. MASSARO, *"Concretizzazione del rischio" e prevedibilità dell'evento nella prospettiva della doppia funzione della colpa*, in *Cass. pen.*, 12/2009, p. 4706 ss.

soprattutto nei contesti caratterizzati da incertezza scientifica che pongono seri dubbi circa la possibilità di costituire il fondamento per l'introduzione di figure di reato[56].

Ciò che bisogna evitare è che una repressione penalistica delle attività legate ai sistemi di intelligenza artificiale possa portare a limitarne eccessivamente lo sviluppo, in una condizione di immobilismo dettata proprio dalla minaccia della sanzione.

Bisogna chiedersi se l'unica soluzione possa essere quella di risolvere – o quantomeno ridurre – la situazione di incertezza. Allo stato attuale, potrebbe certamente essere d'aiuto incrementare i doveri di informazione configurabili in capo a chi svolge le citate attività, sicché una mancata conoscenza approfondita della materia e dei rischi connessi possa essere posta a fondamento di una imputazione di responsabilità penale, la quale sorgerebbe in caso di violazione dell'obbligo di approfondimento e aggiornamento scientifico[57]. A tal proposito, il legislatore dovrebbe più precisamente individuare i soggetti tenuti all'aggiornamento scientifico, e di conseguenza creare delle chiare posizioni di garanzia.

Al fine di evitare, poi, un immobilismo preventivo dell'avanzamento tecnologico, dovrebbe essere anche garantita una maggiore informazione pubblica sulla materia, allo scopo di impedire una illogica paura della collettività cagionata da ciò che non è noto[58].

---

[56] A. MASSARO, *Principio di precauzione e diritto penale*, cit.

[57] Sulla rilevanza assunta dal dovere di aggiornamento scientifico per il controllo dei moderni rischi tecnologici G. FORTI, voce *Colpa (dir. pen.)*, in *Diz. dir. pubbl. Cassese*, Vol. II, Milano, 2006, p. 950-951 e, più diffusamente, G. FORTI, *"Accesso" alle informazioni sul rischio*, cit., p. 192 ss. V. anche C. RUGA RIVA, *Principio di precauzione e diritto penale*, cit., p. 1762; D. PULITANÒ, *Gestione del rischio*, cit., pp. 795-796 e, soprattutto, D. PULITANÒ, *Il diritto penale fra vincoli di realtà e sapere scientifico*, in *Riv. it. dir. e proc. pen.*, 2006, p. 821 ss.

[58] Sul punto G. FORTI, *"Accesso" alle informazioni sul rischio*, cit., p. 211 ss., il quale ritiene che le imprese andrebbero responsabilizzate a diffondere le conoscenze possedute o acquisibili, introducendo così una vera e propria «responsabilità per omessa comunicazione di informazioni rilevanti per la gestione del rischio». Inoltre, F. CENTONZE, *La normalità dei disastri tecnologici. Il problema del congedo dal diritto penale*, Giuffrè, Milano, 2004, p. 400 ss., ritiene auspicabile la creazione di una vera e propria autorità indipendente per il controllo e la gestione dei rischi tecnologici, che avrebbe il compito di mettere ordine tra le opinioni spesso contrastanti in materia e di costituire l'interlocutore privilegiato con i vari operatori del settore. Sul punto si veda anche F. GIUNTA, *Il diritto penale e le suggestioni del principio di precauzione*, cit., p. 244.

Occorre infine tener presente che spesso chi progetta, programma e immette nel mercato un sistema di intelligenza artificiale non è una persona fisica, bensì giuridica. È ad essa che dovranno essere indirizzate e imposte le regole cautelari di cui si è parlato in precedenza, tenendo in considerazione la laboriosità che caratterizza i processi decisionali delle organizzazioni complesse[59].

A tal proposito, occorrerà anche predisporre dei meccanismi sanzionatori efficaci, almeno fino a quando l'evoluzione dell'intelligenza artificiale e del *machine learning* non ci permetterà di rivolgere il rimprovero penale non più al programmatore o al produttore del *software*, ma al sistema stesso[60]. Alcuni studiosi, infatti, hanno ipotizzato la responsabilizzazione diretta della macchina. I sistemi di intelligenza artificiale non sono più meri esecutori dei comandi umani, ma operano con un certo grado di autonomia.

Tuttavia, la responsabilità penale si basa sull'attribuzione del rimprovero a un soggetto consapevole delle sue azioni e delle conseguenze, distinguendo tra giusto e sbagliato. Nel caso dei sistemi di intelligenza artificiale, allo stato attuale, essi non possiedono una coscienza o un'intelligenza morale comparabile a quella umana. Sebbene possano prendere decisioni autonome basate su algoritmi complessi, queste decisioni sono il risultato di regole predefinite da programmatori umani.

La mancanza di coscienza rende impossibile ascrivere una responsabilità penale alle IA, poiché il sistema penale è progettato per orientare il comportamento umano attraverso la minaccia della punizione, un concetto inefficace nei confronti di entità

---

[59] C. PIERGALLINI, *Danno da prodotto*, cit., p. 305 ss. L'autore evidenzia come la moderna realtà delle organizzazioni complesse sia caratterizzata da una frammentazione delle competenze e da una polverizzazione dei centri decisionali: la «procedimentalizzazione della decisione» che ne deriva rende assai difficoltoso l'adattamento del modello «individualistico», basato sul più lineare percorso informazione – scelta – azione – esecuzione. Sul punto si veda anche G. MARINUCCI, *Innovazioni tecnologiche*, cit., p. 56; D. PULITANÒ, *Gestione del rischio da esposizioni professionali*, cit., p. 796.

[60] In tal senso si veda G. GIUFFRIDA, F.M. RINALDI, *Big Data, Intelligenza Artificiale e Machine Learning: tra discriminazione e responsabilità algoritmica*, in S. Gozzo, C. Pennisi, V. Asero, R. Sampugnaro (a cura di), *Big Data e processi decisionali*, cit., p. 35 ss.; C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato?*, in *Riv. it. dir. e proc. pen.*, 4/2020, p. 1746 ss.; I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, cit., p. 90 ss.; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1/2019, p. 69 ss.; D. PIVA, *Machina discere, (deinde) delinquere et puniri potest. Il diritto nell'era digitale,* cit., p. 681.

che non sono in grado di percepire o comprendere un rimprovero. Perciò, le IA non possono essere considerate soggetti penalmente imputabili. La responsabilità, in questi casi, ricade sugli esseri umani che progettano, utilizzano e supervisionano questi sistemi.

In breve, la sanzione penale richiede un soggetto consapevole, capace di comprendere il significato della colpa, e i sistemi IA non raggiungono questo livello di consapevolezza[61].

La responsabilità delle «scelte» operate dal sistema di IA sarà quindi, ancora per il momento, da attribuire ad un agente umano, attraverso una ricostruzione dei diversi contributi causali che hanno portato alla condotta posta in essere dal sistema.

2. Algoritmi, diritti fondamentali e responsabilità penale

2.1. Il principio personalista prima dell'intelligenza artificiale: l'evoluzione dei diritti a protezione della sfera dell'identità

Un primo riconoscimento in Italia di un diritto pieno all'identità personale si ha con la giurisprudenza degli anni '70, che lo concepisce come la corretta rappresentazione della propria persona da parte di terzi, includendo aspetti relazionali, sociali e ideologici, e tutelabile anche in assenza di una specifica normativa[62].

[61] Sul punto si veda L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta cambiando il mondo*, Raffello Cortina editore, Milano, 2017.

[62] Si può far riferimento a un'ordinanza del Pretore di Roma del 6 maggio 1974 relativa all'uso di un'immagine in un manifesto di propaganda antidivorzista che ritraeva un uomo e una donna le cui convinzioni, rispetto al referendum imminente, erano opposte a quelle suggerite dal manifesto e che, per di più, non erano neppure sposati. Il giorno successivo, lo stesso giudice emise un provvedimento simile a favore del *leader* comunista Palmiro Togliatti, la cui dichiarazione era stata manipolata e utilizzata in un diverso manifesto antidivorzista per suggerire erroneamente una sua opposizione al divorzio.

Il riconoscimento definitivo del diritto all'identità personale da parte della Corte di Cassazione giunse nel 1985 con la sentenza nel caso Veronesi[63], in cui i giudici dettero ragione all'oncologo, le cui dichiarazioni contro il fumo erano state distorte a scopi pubblicitari da un marchio di sigarette.

Durante il giudizio di merito, la lesione della posizione giuridica era stata identificata come una violazione del diritto al nome, e quindi ricondotta all'art. 7 del codice civile, sebbene attraverso un'interpretazione estensiva ed evolutiva di tale norma.

Questa sentenza ha quindi radicato la tutela del diritto al nome nell'articolo 2 della Costituzione Italiana, che viene visto come una «clausola aperta» capace di estendere la protezione costituzionale anche a interessi non esplicitamente menzionati nella Carta. Infatti, nonostante questa interpretazione espansiva, la sentenza non ha riconosciuto il diritto all'identità personale come costituzionalmente garantito, affermando che solo i diritti specificamente previsti dalla Costituzione possono essere considerati tali.

Questo ha portato ad un risultato che può apparire incoerente: se l'identità personale è protetta in modo da poter limitare il diritto alla libertà di espressione, garantito dall'art. 21 della Carta, la stessa dovrebbe avere lo stesso rango. In altre parole, se il diritto all'identità personale può interferire con un diritto di rango costituzionale come la libertà di espressione, dovrebbe anch'esso essere riconosciuto come tale. La questione è particolarmente rilevante quando si considerano altri diritti correlati, come la riservatezza e l'onore, che concorrono a definire l'identità personale.

Nella sentenza del 1985, la Cassazione affermò chiaramente l'esistenza di un diritto soggettivo a vedere rispettato, da parte di terzi, il proprio «modo di essere nella realtà sociale» al fine di «svolgere integralmente la propria personalità individuale»[64].

---

[63] Cass. civ., sez. I, 22 giugno 1985, n. 3769, in *Foro it.*, 1/1985, p. 2211; sul punto si veda M. DOGLIOTTI, *Il diritto all'identità personale approda in Cassazione*, in *Giust. civ.*, 1/1985, p. 3049 ss.

[64] Cass. civ., sez. I, 22 giugno 1985, n. 3769 cit., p. 2216. A pagina 2211 si legge anche che «Ciascun soggetto ha interesse, ritenuto generalmente meritevole di tutela giuridica, di essere rappresentato, nella vita di relazione, con la sua vera identità, così come questa nella realtà sociale, generale e particolare, è conosciuta o poteva essere conosciuta con l'applicazione dei criteri della normale diligenza e della buona fede soggettiva; ha, cioè, interesse a non vedersi all'esterno alterato, travisato, offuscato, contestato il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico,

Si sostiene con fermezza che il diritto all'identità personale goda di una solida rilevanza costituzionale, data la sua stretta connessione con la tutela del pieno sviluppo della personalità individuale e con la partecipazione all'organizzazione politica e sociale del Paese, come previsto dagli artt. 2 e 3 della Costituzione. Anche la Cassazione ha affermato che si può «individuare con maggiore risolutezza il correlativo fondamento giuridico, ancorandolo direttamente all'art. 2 Cost. inteso tale precetto nella sua più ampia dimensione e suscettibile di apprestare copertura costituzionale ai nuovi valori emergenti della personalità in correlazione anche all'obiettivo primario di tutela del "pieno sviluppo della persona umana", di cui al successivo art. 3 cpv».[65]

Questa impostazione è stata accolta dalla Corte Costituzionale, nella sentenza n. 13 del 1994, in cui si legge che «è certamente vero che tra i diritti che formano il patrimonio irretrattabile della persona umana l'art. 2 della Costituzione riconosce e garantisce anche il diritto all'identità personale»[66].

Nella successiva sentenza n. 978 del 1996[67], relativa al noto caso Tabocchini - Re Cecconi, la Corte di Cassazione ha chiarito che il diritto a definire e proteggere la

professionale ecc. quale si era estrinsecato od appariva, in base a circostanze concrete ed univoche, destinato ad estrinsecarsi nell'ambiente sociale».

[65] Cass. civ. sez. I, 7 febbraio 1996, n. 978, p. 116, in *DeJure.it*. Si parla in questo caso di «teoria costituzionalmente orientata del bene giuridico», secondo la quale per individuare quali interessi socialmente rilevanti meritino tutela penale, è essenziale fare riferimento alla Costituzione. Ciò implica la necessità di selezionare solo quei beni che possiedono una rilevanza costituzionale, sia esplicita che implicita. I beni impliciti sono quegli interessi che, pur non essendo espressamente menzionati nel testo costituzionale, risultano fondamentali per la protezione di altri beni che, invece, sono direttamente tutelati dalla Costituzione. In questo modo, si assicura che il diritto penale sia applicato solo per la difesa di valori essenziali riconosciuti nell'ordinamento costituzionale.

[66] Corte cost., sent. n. 13 del 3 febbraio 1994 (ud. 24 gennaio 1994); per un commento si veda la nota di A. PACE, *Nome, soggettività giuridica e identità personale*, in *Giur. cost.*, 1/1994, p. 103 ss. In particolare, la Corte ha affermato che «è certamente vero che tra i diritti che formano il patrimonio irretrattabile della persona umana l'art. 2 Cost. riconosce e garantisce anche il diritto all'identità personale. Si tratta – come efficacemente è stato affermato – del diritto ad essere sé stesso, inteso come rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo. L'identità personale costituisce quindi un bene per sé medesima, indipendentemente dalla condizione personale e sociale, dai pregi e dai difetti del soggetto, di guisa che a ciascuno è riconosciuto il diritto a che la sua individualità sia preservata»: v. punto 5.1. del Considerato in diritto.

[67] Cass. civ., sez. I, 7 febbraio 1996, n. 978, in *Dir. inform.,* 1997, p. 116 ss.; per un commento v. la nota di A. D'ADDA, *La Corte di Cassazione riafferma il proprio orientamento in tema di diritto all'identità*

propria identità personale ha rango costituzionale e rappresenta una delle modalità principali per attuare il principio personalista[68]. Secondo i giudici, solo garantendo a ciascun individuo la libertà di essere e svilupparsi senza interferenze indebite da parte di terzi è possibile realizzare pienamente l'obiettivo costituzionale del «pieno sviluppo della persona umana», che è un principio cardine dell'intero ordinamento giuridico.

Questa sentenza, insieme alla dottrina civilistica prevalente, abbraccia la cosiddetta teoria monistica dei diritti della personalità[69]. Tale teoria considera i diritti della personalità come un unico diritto soggettivo volto alla piena realizzazione della propria individualità, che può manifestarsi in forme diverse a seconda del contesto, alcune esplicitamente riconosciute dalla legge e altre derivabili per analogia dai principi generali dell'ordinamento. Questa posizione ha ormai superato le vecchie incertezze sull'estensione di tale categoria di diritti.

Secondo una diversa tesi sarebbe invero preferibile ricondurre la tutela costituzionale del diritto all'identità personale al principio della libertà di manifestazione del pensiero, sancito dall'art. 21 della Costituzione[70]. Questa prospettiva si basa

---

personale, in *Resp. civ. prev.*, 1997, p. 474 ss. Inoltre, si veda G. PINO, *L'identità personale*, in AA.VV., *Gli interessi protetti nella responsabilità civile*, vol. II, Utet, Torino, 2005, p. 367 ss.

[68] La Corte ha infatti affermato: «individuare con maggiore risolutezza il correlativo fondamento giuridico del diritto all'identità, ancorandolo direttamente all'art. 2 Cost. inteso tale precetto nella sua più ampia dimensione e suscettibile, per ciò appunto, di apprestare copertura costituzionale ai nuovi valori emergenti della personalità in correlazione anche all'obiettivo primario di tutela del pieno sviluppo della persona umana, di cui al successivo art. 3 cpv.».

[69] Per un approfondimento sul dibattito tra teoria monista e pluralista si veda G. PINO, *Teorie e dottrine dei diritti della personalità. Uno studio di meta-giurisprudenza analitica*, in *Materiali per una storia della cultura giuridica*, 1/2003, p. 237 ss; G. ALPA, *Alle origini dei diritti della personalità*, in *Riv. trim. dir. proc. civ.*, 3/2021, p. 671 ss.; S. PICCININI, *Appunti sui diritti della personalità e sui c.d. nuovi diritti. Tutela e promozione della identità personale*, in *Dir. fam.*, 1/2021, p. 227 ss.; G. RESTA, *Diritti della personalità: problemi e prospettive*, in *Dir. inf.*, 6/2007, p. 1043 ss.; P. RESCIGNO, *I diritti della personalità e la loro rilevanza costituzionale (a proposito di un recente libro)*, in *Dir. inf.*, 2/1986, p. 333 ss.; A. PROTO PISANI, *La tutela giurisdizionale dei diritti della personalità*, in *Foro it.*, 1/1990, 5, pp. 1-19; A. MANNA, *La tutela penale dei diritti della personalità: aspetti problematici*, in *Indice pen.*, 3/1986, p. 711 ss.; A. GAMBARO, *Diritti della personalità*, in *Riv. dir. civ.*, 6/1981, 2, p. 519 ss.; E. LECALDANO, *Identità: una critica tra storia e teoria*, in *Notizie di Politeia*, 135/2019, p. 8 ss.

[70] Questa tesi è sostenuta da A. PACE, *Problematica delle libertà costituzionali. Parte generale*, CEDAM, Padova, 2003. Sul punto si veda anche G. PINO, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, il Mulino, Bologna, 2003; A. BEVERE, A. CERRI, *Il diritto di informazione e i diritti della persona*, Giuffrè, Milano, 1995; G. PINO, *Teoria e pratica del bilanciamento: tra libertà di manifestazione del pensiero e tutela dell'identità personale*, in *Danno e resp.*, 6/2003, p. 577 ss.; R. CASO, *La*

sull'osservazione che l'attribuzione a un individuo di opinioni mai espresse viola il suo diritto a non manifestare idee non proprie e a essere riconosciuto solo per le opinioni effettivamente professate.

Tale impostazione consentirebbe di distinguere, in termini di rilevanza costituzionale, tra le pretese relative all'identità personale legate all'espressione del pensiero (come opinioni politiche, religiose o culturali) e quelle più strettamente connesse a profili patrimoniali, differenziando anche gli eventuali profili risarcitori che potrebbero emergere in ciascuna situazione. Tuttavia, va riconosciuto che questa distinzione, pur facilmente enunciabile in teoria, potrebbe risultare meno chiara nella pratica.

A partire dagli anni '90, la protezione dell'identità personale ha subito una trasformazione radicale a causa della diffusione massiccia dei *computer*. La capacità dei sistemi informatici di archiviare e analizzare una quantità senza precedenti di informazioni sugli individui ha sollevato nuovi rischi e problematiche riguardanti la sfera della personalità morale[71].

In effetti, qualsiasi diritto collegato all'identità di una persona, come il controllo sull'integrità della sua rappresentazione pubblica o la tutela di aspetti privati della sua vita, ruota attorno al tema del controllo sui dati personali. Anche in Italia, la legislazione in materia ha riconosciuto l'importanza della protezione dell'identità personale, includendo esplicitamente tale tutela tra gli obiettivi delle normative, rappresentando così un primo riconoscimento legislativo indiretto di questo diritto.

2.1.1. La normativa sul trattamento dei dati personali

L'evoluzione tecnologica ha reso necessaria una nuova attenzione alle dinamiche della *privacy* e dell'identità personale, portando alla nascita di leggi e regolamenti specifici volti a tutelare le informazioni personali in un contesto tecnologico in continua evoluzione.

---

società della mercificazione e della sorveglianza: dalla persona ai dati, Ledizioni, Milano, 2021, p. 190 ss; G. ALPA, G. RESTA, *Le persone e la famiglia. 1. Le persone fisiche e i diritti della personalità*, in R. Sacco (diretto da), *Trattato di diritto civile*, Utet Giuridica, Torino, 2019, p. 319 ss.

[71] Sul punto si veda S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna, 1973.

Ogni diritto legato, in senso ampio, all'identità della persona - che si tratti dell'integrità della sua rappresentazione pubblica o della facoltà di mantenere riservati certi aspetti della propria vita - è essenzialmente connesso al controllo sulla comunicazione e diffusione dei dati personali. Questo implica che la tutela dell'identità personale si fonda primariamente sulla gestione e protezione delle informazioni che circolano riguardo a ciascun individuo.

Obiettivo principale di tutte le normative sulla tutela dei dati personali è quello di assicurare che la libertà di manifestazione del pensiero - che si esplica attraverso un trattamento di dati - sia esercitata nel bilanciamento con gli altri diritti fondamentali dell'individuo, primo fra tutti, quello alla sua dignità[72].

Il rapido incremento dei rischi per la *privacy*, conseguente al progresso tecnologico, informatico e telematico degli ultimi anni, ha reso evidente la necessità di una nuova regolamentazione a livello europeo. In risposta a questa esigenza, il 4 maggio 2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio, datato 27 aprile 2016, già citato nei paragrafi precedenti. Tale regolamento, conosciuto come Regolamento Generale sulla Protezione dei Dati (GDPR), riguarda la protezione delle persone fisiche rispetto al trattamento dei dati personali e la libera circolazione di questi ultimi, abrogando la precedente Direttiva 95/46/CE[73].

Il regolamento è entrato in vigore il 24 maggio 2016, stabilendo che gli Stati membri dell'UE dovessero implementare pienamente le sue disposizioni entro il 25 maggio 2018. Il GDPR evidenzia come la quantità di informazioni raccolte e condivise sia cresciuta enormemente, sottolineando la necessità di riaffermare a livello europeo il principio secondo cui «il trattamento dei dati personali dovrebbe essere al servizio dell'uomo»[74].

---

[72] E. ROMANELLI (a cura di), *Web, social ed etica. Dove non arriva la privacy: come creare una cultura della riservatezza*, in PQM Collana di psicologia giuridica (4), Edizioni ETS, Pisa, 2018.

[73] La direttiva del 1995 si limitava a prescrivere agli Stati membri di adottare le misure appropriate per garantire la piena applicazione delle disposizioni ivi contenute e in particolare di stabilire le sanzioni da applicare in caso di violazione delle disposizioni introdotte in ossequio alla direttiva.

[74] V. 4° considerando del citato Regolamento.

Questo riflette una visione in cui la protezione dei dati personali è considerata fondamentale per salvaguardare la dignità e i diritti fondamentali degli individui in un contesto di crescente digitalizzazione.

Il Regolamento introduce una serie di regole in merito all'informativa e al consenso degli interessati, rafforzando la trasparenza del trattamento dei dati personali. Inoltre, definisce rigorosi limiti alla gestione automatizzata degli stessi, garantendo che i processi decisionali basati su algoritmi rispettino i diritti degli individui, specialmente in contesti come la profilazione e le decisioni che producono effetti giuridici.

In Italia, il diritto alla protezione dei dati personali è stato formalmente introdotto nel nostro ordinamento con la legge 31 dicembre 1996, n. 675, insieme alla legge-delega n. 676, le quali recepivano la direttiva comunitaria 95/46/CE[75]. Questi interventi legislativi hanno permesso all'Italia di recuperare un ritardo di quasi vent'anni rispetto ad altri Paesi europei.

Sebbene tale diritto sia stato codificato in tempi relativamente recenti, le sue radici possono essere individuate già nella nostra Costituzione, in particolare nell'art. 2, che riconoscendo e tutelando i «diritti inviolabili» della persona, indirettamente garantisce anche il «diritto alla vita privata».

Le disposizioni comunitarie conferiscono agli Stati membri un significativo margine di autonomia per stabilire le garanzie necessarie a bilanciare il diritto alla protezione dei dati personali con il diritto alla libertà di espressione.

La legislazione italiana ha voluto sottolineare in modo esplicito l'importanza del rispetto della dignità umana nella protezione di tutte le informazioni legate all'individuo. Il Codice della *privacy*, introdotto con il d.lgs. 30 giugno 2003, n. 196 ed entrato in vigore il primo gennaio 2004, prevede, all'art. 2, che «il trattamento dei dati personali deve avvenire nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità

[75] Dalla lettura dell'articolo 1 della citata Direttiva si evince che l'oggetto della tutela è costituito dai diritti e le libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.

personale e al diritto alla protezione dei dati personali»[76]. Nella versione aggiornata dal d.lgs. 10 agosto 2018, n. 101, viene ulteriormente enfatizzata la centralità della dignità della persona, che viene posta in primo piano rispetto agli altri diritti e libertà fondamentali.

Ciò che emerge da una analisi della normativa è che nel nostro sistema penale vi è una tutela incompleta e a tratti inefficiente dei diritti della personalità, e in particolare della riservatezza, della vita privata e intima della persona umana. Questi *deficit* si sono ulteriormente acuiti con la depenalizzazione del delitto di ingiuria.

Nonostante nel nostro ordinamento la scelta sia stata quella di relegare la tutela di questo settore alla normativa civilistica, l'attuale contesto tecnologico con l'avvento dei *social* ha portato certamente a mettere in dubbio questa strategia in ragione della enorme potenzialità offensiva del mezzo informatico.

La Corte di cassazione sul punto ha precisato che «il diritto alla riservatezza o all'intimità della sfera privata dell'individuo, appare, ben più di altri aspetti di tutela della personalità, strettamente collegato alle profonde trasformazioni operate dalla società industriale: accresciuto contatto e ad un tempo maggiore estraneità tra individui, più ampio dinamismo e circolazione dei soggetti che possono inserirsi in ambienti e situazioni tra loro del tutto indipendenti, talora rivestendo ruoli differenziati e mostrando così profili diversi della propria personalità. Ma è soprattutto l'incessante progresso tecnologico, il perfezionamento (e la pericolosità) dei mezzi di comunicazione

---

[76] Art. 2, d.lgs. 30 giugno 2003, n. 196. Per un approfondimento sul Codice v. V. MANES, N. MAZZACUVA, *GDPR e nuove disposizioni penali del Codice "privacy"*, in *Dir. pen. e proc.*, 2/2019, p. 171 ss.; E. ANTONINI, *Il trattamento illecito di dati personali nel codice della privacy: i nuovi confini della tutela penale*, in *Dir. pen. e proc.*, 3/2005, p. 340 ss.; A. MANNA, *Codice della privacy: nuove garanzie per i cittadini nel Testo unico in materia di protezione dei dati personali*, in *Dir. pen. e proc.*, 1/2004, p. 17 ss.; M. LAMANUZZI, *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento 2016/679/UE e nuove responsabilità per gli enti*, in *JusOnline*, 1/2017, p. 218 ss.; G. M. BACCARI, C. CONTI, *La corsa tecnologica tra Costituzione, codice di rito e norme sulla "privacy": uno sguardo d'insieme*, in *Dir. pen. e proc.*, 6/2021, p. 711 ss.; D. PROVOLO, *Il sistema sanzionatorio del novellato Codice della "privacy" e la tutela penale "patchwork" dei dati genetici e dei dati biometrici*, in *Riv. trim. dir. pen. econ.*, 2/2019, p. 242 ss.; E. VARANI, *Diritto alla privacy e trattamento dei dati sensibili in ambito sanitario: dalla Carta dei diritti fondamentali dell'Unione Europea al D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"*, in *Giur. it.*, 4/2005, p. 1769 ss.; S. DEL CORSO, *La Protezione dei dati personali. Commentario sistematico al d.lgs. 30 giugno 2003, n. 196*, Padova 2007, *sub* art. 167.

di massa e degli strumenti di raccolta di dati e notizie che, attraverso inedite, per il passato del tuto impensabili, e talora gravissime, aggressioni agli aspetti più intimi della personalità, richiedono necessariamente l'individuazione di più efficaci ed adeguate difese. Solo in tempi relativamente recenti si è pervenuti ad una disciplina organica della materia, con la L. n. 675 del 1996, variamente modificato, successivamente, con un ancor più incisivo Digs. N. 196/2003»[77].

2.1.2. Identità personale e riservatezza digitale

Questi obiettivi di rispetto dei diritti e libertà fondamentali che la legge si pone sono oggi sempre più difficili da bilanciare con il trattamento dei dati personali per diversi motivi, tra cui certamente il graduale aumento degli strumenti mediante i quali prendono consistenza le varie forme di manifestazione del pensiero. Dalla radio si è passati alla televisione fino ad arrivare a *internet* e ai *social media.* Questi ultimi, in particolare, hanno portato non solo ad un ampliamento della platea dei destinatari, ma hanno anche contribuito ad aumentare il numero, la varietà e l'accessibilità dei dispositivi attraverso cui si può esprimere e diffondere il proprio pensiero. Con un *computer*, un *tablet* o persino un semplice *smartphone*, è ormai possibile competere con i mezzi di comunicazione tradizionali.

Da segnalare, inoltre, una evidente modifica dei contenuti della comunicazione. Dalla diffusione di fatti, notizie e opinioni di interesse generale, come eventi di cronaca, vicende politiche o fatti di costume, si è arrivati alla condivisione di contenuti molto più specifici e personali, come viaggi, cerimonie o episodi quotidiani. Questi eventi, pur avendo una rilevanza limitata, vengono esposti all'attenzione di una platea vasta e indefinita, diventando oggetto di dibattito pubblico.

Inizialmente si riteneva che i procedimenti di trattamento dei dati su *internet* avessero solo finalità economiche e di profitto, e fossero dunque legati alle operazioni commerciali svolte in rete[78].

---

[77] Cass., Sez. I civ., 20 maggio 2016, n. 10510, in *DeJure.*

[78] Il tema del trattamento dei dati identificativi delle persone emerge anche dalla Direttiva 95/46 «*Privacy Directive*», adottato sulla base dell'art. 95 del precedente Trattato della Comunità

Tuttavia, lo sviluppo delle relazioni umane nel *web* e più in generale l'evoluzione culturale ha portato al passaggio dalla nozione dicotomica della *privacy*-trattamento dati, a quella della *privacy*-riservatezza personale[79].

Riformulare la pratica di protezione dei dati in modo da andare oltre le semplici procedure di trattamento e rispondere alle esigenze di tutela della dignità e della riservatezza personale può portare a una moderna interpretazione del concetto di vita intima. Questa, intesa come un diritto inviolabile della persona, si inserisce nel più ampio contesto dei diritti di libertà: la libertà di gestire autonomamente e senza condizionamenti o mortificazioni gli spazi della propria *privacy* e l'insieme delle proprie informazioni e dati identificativi.

La connessione tra la protezione dei dati personali e i diritti della personalità è diventata così profonda che, secondo alcuni studiosi, è ormai impossibile considerare l'una senza l'altra. Di conseguenza, ogni disputa riguardante la tutela dell'identità personale si configura oggi anche come una questione di trattamento dei dati corrispondenti.

Quest'ultima nozione coincide oggi esattamente con quella di riservatezza, che un tempo veniva intesa come «discrezione della propria solitudine»[80].

Anche se non si accoglie pienamente questa posizione, è innegabile che la normativa sui dati personali, sviluppata in risposta alla rivoluzione digitale, rappresenti oggi il quadro normativo più complesso e dettagliato in questo ambito, costituendo il riferimento principale per affrontare le sfide legate all'identità personale, comprese quelle emergenti dallo sviluppo dell'intelligenza artificiale.

La riservatezza informatica rappresenta un concetto specifico all'interno del panorama giuridico legato alle tecnologie dell'informazione e del *cyberspazio*. Viene intesa

---

Europea chiamato a garantire la creazione e il rafforzamento del mercato interno attraverso la certezza giuridica e la garanzia operativa offerta a ogni persona consumatore.

[79] Sul punto si veda P. TRONCONE, *La tutela penale della riservatezza e dei dati personali. Profili dommatici e nuovi approdi normativi*, Edizioni Scientifiche Italiane, Napoli, 2020, p. 51 ss.; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016; S. RODOTÀ, *La "privacy" tra individuo e collettività*, in *Pol. dir.*, 1974, p. 545 ss.

[80] S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Editori Laterza, Bari.

come il diritto di escludere terzi dall'accesso non autorizzato e di essere protetti contro intrusioni indesiderate o interferenze che potrebbero compromettere il proprio spazio informatico, in cui ciascuno gestisce le sue attività e relazioni *online*[81]. Questo diritto si configura come una forma di autonomia e sicurezza personale, garantendo l'integrità delle proprie risorse digitali e dei dati che vi risiedono.

Il concetto di riservatezza informatica si distingue dalla sicurezza informatica, che si focalizza sulla protezione tecnica contro attacchi o minacce digitali. La riservatezza informatica, infatti, ha una portata più ampia, poiché non solo salvaguarda il «domicilio informatico» (cioè lo spazio virtuale e fisico in cui sono conservati i dati personali)[82], ma garantisce anche l'esclusività nell'accesso e gestione di tali dati. Questo diritto mira a proteggere la confidenzialità, la sicurezza e la libertà delle azioni che possono essere svolte nel proprio ambito cibernetico, includendo anche le attività future o potenziali.

L'avanzamento delle tecniche di archiviazione e analisi dei dati negli ultimi decenni, insieme allo sviluppo di tecnologie basate sull'intelligenza artificiale, ha intensificato i rischi legati alla protezione dell'identità personale.

L'uso di algoritmi di ultima generazione consente una profilazione estremamente precisa degli individui, con la possibilità di utilizzare tali informazioni per diverse finalità, tra cui l'influenza sul comportamento delle persone. Questa evoluzione pone nuove sfide per la tutela dei diritti, in particolare quello all'identità, che assume

---

[81] L. PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in L. Picotti (a cura di), *Tutela penale della persona e nuove tecnologie*, CEDAM, Padova, 2013, p. 59 ss.

[82] Anche la Corte di cassazione, con la sentenza n. 42021/2012, ha cercato di chiarire la definizione di domicilio informatico, disciplinato dall'art. 615-*ter* c.p. La questione nasceva dalla denuncia presentata dal legale rappresentante di una società, il cui *server* di posta elettronica era stato violato da un tecnico informatico che si era impossessato di indirizzi *e-mail* riservati. Secondo la Corte, il «domicilio informatico» non è solo uno spazio fisico dove si trovano i *server* o le apparecchiature informatiche, ma include anche uno spazio ideale dove risiedono i dati di pertinenza di una persona. In tal senso, la protezione conferita dall'art. 615-*ter* c.p. estende la tutela della riservatezza della persona anche a tale spazio virtuale, trattandolo come parte della sfera individuale garantita a livello costituzionale. Inoltre, la Corte sottolinea che la protezione offerta dall'art. 615-*ter* c.p. non si limita ai soli dati personalissimi, ma si estende a qualsiasi dato contenuto all'interno di un sistema informatico, purché attinente alla sfera di pensiero o alle attività dell'utente, lavorative o meno. Questa protezione, infine, si applica anche ai dati economico-patrimoniali, sia che il titolare del diritto sia una persona fisica, una persona giuridica, un ente pubblico o privato.

un'importanza centrale non solo come diritto alla libera espressione e corretta rappresentazione di sé, ma anche, in una fase anteriore, come diritto alla libera e autentica definizione della propria identità e alla possibilità di modificarla.

I sistemi di intelligenza artificiale, come descritti in precedenza, si basano sull'elaborazione di quantità sempre maggiori di dati personali, permettendo di identificare analogie e schemi complessi, spesso incomprensibili per un osservatore umano.

Questo tipo di analisi consente di collocare l'utente, i cui dati vengono trattati, all'interno di categorie specifiche di individui con caratteristiche simili (il cosiddetto *clustering*, o profilazione secondo la terminologia della normativa europea sulla protezione dei dati)[83]. Il profilo risultante è continuamente aggiornato e perfezionato tramite l'acquisizione di nuovi dati e può essere impiegato non solo per suggerire prodotti all'utente, ma anche per dedurre le sue inclinazioni politiche, orientamento sessuale, credenze religiose e, in definitiva, per svelare aspetti profondi e nascosti della sua personalità.

Le informazioni così ottenute possono essere utilizzate per vari scopi, che spaziano dal *marketing* mirato alla propaganda politica, fino all'automazione di decisioni che un tempo erano di competenza esclusiva degli esseri umani, basate sulla loro conoscenza, sensibilità ed esperienza. Tuttavia, queste tecnologie stanno dimostrando una capacità crescente non solo di comprendere e prevedere il comportamento umano, ma anche di influenzarlo e modificarlo, come dimostrato da diversi studi condotti negli ultimi dieci anni.

Questo aspetto introduce il concetto di *nudge*, reso popolare dall'economista Richard Thaler e dal giurista Cass Sunstein[84]. La teoria si basa sulle scoperte

---

[83] Per *clustering* o profilazione si intende «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica» cfr. art. 4 comma 1 n. 4 del Reg. UE n. 679 del 2016 (GDPR).

[84] Si veda R. THALER, C. SUNSTEIN, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Penguin Books, Londra, 2008. Per un ulteriore approfondimento dal punto di vista tecnico v. C. SUNSTEIN, *Nudging: a very short guide*, in *Journal of consumer policy*, 37/2014, p. 583 ss; M. VON

dell'economia comportamentale e della psicologia cognitiva, che hanno evidenziato come le decisioni umane siano spesso influenzate da vari *bias* cognitivi, soprattutto in situazioni di *stress*, mancanza di tempo o complessità elevata, contesti nei quali prevalgono decisioni rapide e istintive piuttosto che riflessive e razionali[85].

La teoria del *nudging* suggerisce di analizzare approfonditamente il contesto in cui vengono prese le decisioni, al fine di ridurre gli effetti negativi di questi *bias*. Thaler e Sunstein propongono di intervenire attraverso tecniche di architettura della scelta che rendano più probabile che una decisione – anche se presa in modo rapido e approssimativo – conduca a un risultato desiderato. Un esempio di *nudge* è il posizionamento strategico di frutta e verdura in una mensa *self-service* per promuovere una dieta sana, oppure l'adozione di un sistema di *opt-out* per i piani pensionistici aziendali, che garantisce una sicurezza economica a lungo termine per la maggior parte dei lavoratori.

L'idea di fondo è che l'opzione favorita da queste tecniche rappresenti la scelta che il soggetto farebbe se fosse perfettamente razionale, considerata la migliore per lui o lei e per la società nel suo complesso. Il *nudging* viene considerato preferibile rispetto a interventi coercitivi poiché mantiene intatta la libertà di scelta dell'individuo, pur influenzandone i risultati.

Thaler e Sunstein nel loro lavoro definiscono il *nudge* come un elemento della «architettura della scelta» che può influenzare il comportamento delle persone in modo prevedibile, senza però imporre alcuna restrizione o alterare sostanzialmente gli incentivi economici. Un intervento è considerato un *nudge* solo se può essere evitato

---

ROOKHUIJZEN, E. DE VET, *Nudging healthy eating in Dutch sports canteens: a multi-method case study*, in *Public Health Nutrition*, 2020; C. KAWA, P.M. IANIRO DAHM, J. F. H. NIJHUIS, W.H. GIJSELAERS, *Cafeteria online: nudges for healthier food choices in a university cafeteria – a randomized online experiment,* in *National Insitutes of Health (NIH),* 2021; R. L. CLARK, R. G. HAMMOND, M. SANDLER MORRILL, C. KHALAF, *Nudging retirement savings: a field experiment on supplemental plans*, Working Paper 23679 – National Bureau of Economic Research, Cambridge (USA), 2017; C.KRONCKE, *Nudging towards a stable retirement*, in *Politics and the Life Sciences*, 1/2018, p. 126 ss.

[85] Sul tema dei *bias* si rinvia a D. KAHNEMAN, A. TWERSKY, *Prospect theory: an analysis of decision under risk*, in *Econometrica*, 2/1979, p. 263 ss.; D. KAHNEMAN, A. TWERSKY, P. SLOVIC, *Judgment under uncertainity. Heuristics and biases*, Cambridge, 1982; V. SMITH, *Rationality in economics: constructivist and ecological forms*, Leiden, 2007. La tematica dei *bias* verrà approfondita nel paragrafo 3.4.

dalle persone facilmente e a basso costo. In altre parole, il *nudge* orienta le scelte individuali in una direzione desiderata, mantenendo comunque la libertà di scegliere diversamente[86].

Con l'avvento dell'intelligenza artificiale, si apre un ulteriore scenario: la creazione di *nudges* su misura, personalizzati in base al profilo dell'utente, e quindi ancora più efficaci. Infatti, molti servizi *online*, in particolare le piattaforme *social*, sono strutturati appositamente per mantenere gli utenti connessi il più a lungo possibile, influenzando così le loro scelte.

Questa continua interazione dell'utente con un *nudge* riesce a fornire informazioni preziose sul suo funzionamento, permettendo una continua ottimizzazione della profilazione. Questi *feedback* vengono spesso richiesti direttamente dai gestori delle piattaforme, che invitano gli utenti a esprimere il loro gradimento su determinati contenuti.

Esempi concreti di come queste strategie possano influenzare il comportamento degli utenti includono: la proposta di prodotti su un sito di *e-commerce* basata su acquisti precedenti; l'esposizione a contenuti ideologicamente orientati che rafforzano le convinzioni degli utenti; o la raccomandazione di contenuti multimediali su piattaforme di *streaming*, selezionati in base ai gusti personali.

Un aspetto cruciale delle tecniche di *nudging* basate sull'analisi dei dati è che queste non mirano necessariamente al benessere dell'utente[87]. L'interesse che viene tenuto in considerazione è infatti quello del soggetto privato che gestisce il servizio, il

---

[86] Cfr. R. H. THALER, C. R. SUNSTEIN, *Nudge. The final edition,* cit., p. 11, dove si legge: *«a nudge, as we will use the term, is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting fruit at eye level counts as a nudge. Banning junk food does not».*

[87] Un esempio emblematico è quello di uno studio condotto da *Facebook* nel 2012 (c.d. esperimento di contagio emotivo), secondo cui la manipolazione dei contenuti visualizzati avrebbe portato migliaia di persone a votare in un'elezione, anche se inizialmente non avevano intenzione di farlo. Si veda A. D. I. KRAMER, J. E. GUILLORY, J. T. HANCOCK, *Experimental evidence of massive-scale emotional contagion through social networks*, in *Proceedings of the National Academy of Sciences (PNAS)*, 2 giugno 2014, consultabile sul sito *web* www.pnas.org.

quale utilizza l'analisi delle preferenze degli utenti per creare *nudges* che servano i propri interessi, spesso legati all'aumento dei ricavi pubblicitari.

Questo contrasta con la visione di Thaler e Sunstein, che consideravano il *nudging* come uno strumento per orientare le persone verso decisioni ottimali per loro, sotto la supervisione dei poteri pubblici. Tuttavia, nella realtà digitale, gli attori coinvolti sono privati e guidati da scopi che non sempre coincidono con il benessere degli utenti.

2.1.3. La data retention

Per *data retention* si intende il tempo di conservazione dei dati delle comunicazioni da parte delle compagnie telefoniche o dei *provider*[88]. La normativa che prevede questo meccanismo di conservazione è stata oggetto di innumerevoli critiche. A tal proposito occorre far riferimento all'articolo 24 della legge 20 novembre 2017, n. 167, il quale ha modificato la precedente disciplina contenuta nell'articolo 132 del Codice in materia di protezione dei dati personali[89].

Quest'ultimo prevedeva dei termini di conservazione molto brevi: ventiquattro mesi per i dati relativi al traffico telefonico, dodici mesi per i dati relativi al traffico telematico, trenta giorni per i dati relativi alle chiamate senza risposta.

---

[88] Per un approfondimento sul concetto di *data retention* si veda: M. GIANGRECO, *"Data retention", acquisizione e utilizzabilità dei tabulati telefonici e telematici: una riflessione incrociata*, in *Cass. pen.*, 4/2022, p. 1672 ss.; A. MALACARNE, *"Gravità" dell'ingerenza e "terzietà" dell'organo titolare del potere autorizzatorio: vecchi e nuovi princìpi in materia di "data retention"*, in *Riv. it. dir. e proc. pen.*, 3/2021, p. 1164 ss.; L. SCAFFARDI, *"Data retention" e diritti della persona*, in *Costituzionalismo.it*, 2/2017, 54 ss.; F. IOVENE, *"Data retention" tra passato e futuro. Ma quale presente?*, in *Cass. pen.*, 12/2014, p. 4274 ss.; G. TORALDO, *Un difficile bilanciamento tra la conservazione dei dati per fini di sicurezza e il diritto all'oblio del condannato (riabilitato)*, in *DPCE online*, 1/2024, p. 617 ss.; V. PALLADINI, *"Data retention" e "privacy" in rete: verso una regolazione conforme al diritto UE?*, in *Rivista italiana di informatica e diritto*, 1/2022, p. 103 ss.; G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *MediaLaws*, 2/2018, p. 5 ss.; S. ATERNO, A. CISTERNA, *Il legislatore interviene ancora sul Data retention, ma non è finita - Decreto legislativo 30 maggio 2008, 109*, in *Dir. pen. e proc.*, 3/2009, p. 282 ss.

[89] Per un approfondimento si veda A. STRACUZZI, *Data retention: il faticoso percorso dell'art. 132 Codice Privacy nella disciplina della conservazione dei dati di traffico*, in *Dir. inform.*, 4/2008, p. 585 ss.

La normativa del 2017, invece, ha prolungato i termini di conservazione di tutte e tre le categorie di dati a settantadue mesi.

La modifica è stata introdotta con l'obiettivo di fornire strumenti di indagine più efficaci, tenendo conto delle esigenze straordinarie legate al contrasto del terrorismo, compreso quello di natura internazionale. Prolungando i termini di conservazione dei dati, le autorità possono disporre di una finestra temporale più ampia per analizzare le informazioni rilevanti ai fini delle indagini, garantendo così una maggiore efficacia nelle operazioni di prevenzione e repressione delle attività terroristiche[90].

Il Garante per la protezione dei dati ha ritenuto questa disciplina contraria al principio di minimizzazione dei trattamenti, anche quando effettuati per fini di giustizia.

Anche la Corte di giustizia aveva più volte ricordato la necessità di un rigido principio di proporzionalità nel bilanciare protezione dei dati ed esigenze di pubblica sicurezza, soprattutto quando le misure di conservazione vanno a colpire in maniera indifferenziata tutti cittadini senza prevedere, per di più, garanzie sufficienti per evitare abusi[91].

---

[90] Più precisamente, l'art. 24 recita: «In attuazione dell'articolo 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'articolo 4-*bis*, commi 1 e 2, del decreto-legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, è stabilito in settantadue mesi, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-*bis*, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196».

[91] L'avvio a quest'indirizzo pretorio è stato fornito dalla sentenza *Digital Rights* dell'8 aprile 2014 (cause riunite C-293/12 e C-594/12), con cui Corte di giustizia ha dichiarato l'illegittimità della direttiva 2006/24/Ce per violazione del principio di proporzionalità nel bilanciamento tra protezione dati ed esigenze di pubblica sicurezza. Successivamente, questo orientamento è stato confermato da ulteriori pronunce: 21 dicembre 2016, caso Tele2 Sverige (cause riunite C 203/15 e C 698/15); 2 marzo 2018, causa C-746/18, su rinvio del Riigikohus (Estonia); 2 marzo 2021, causa C-746/18, caso H.K.; 5 aprile 2022 (causa C-140/20). Per un approfondimento si veda G. NADDEO, *Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella "data retention saga" dinanzi alla Corte di giustizia*, in *Freedom, Security & Justice: European Legal Studies*, 2/2022, p. 188 ss.; N. FAIOLA, *"Data retention" ed accesso ai dati per scopi securitari: condizioni e limiti alla luce della giurisprudenza della Corte di giustizia*

A parere della Corte si realizzerebbe una violazione del principio di proporzionalità in varie ipotesi: ogniqualvolta vengano previste misure di conservazione dei dati applicabili in modo generalizzato, in assenza di differenziazione, limitazione o eccezione; o ancora, quando venga omessa l'adozione di criteri oggettivi idonei a limitare l'accesso a tali dati per sole esigenze di accertamento di reati sufficientemente gravi da giustificare una simile ingerenza; quando non siano ipotizzati dei parametri sostanziali e procedurali per l'accesso, da parte delle competenti autorità nazionali, ai dati in esame, in particolare non richiedendo in ogni caso il previo controllo dell'autorità giudiziaria o di un'autorità amministrativa indipendente; infine, quando non siano previsti parametri idonei a differenziare la durata della conservazione dei dati.

Inoltre, la Corte ha sottolineato l'importanza di adottare un approccio selettivo e mirato nella conservazione dei dati, limitandola in base a diversi criteri. Questi includono il tipo di dato raccolto, il mezzo di comunicazione utilizzato, la durata per cui i dati vengono conservati e le persone coinvolte[92].

dell'Unione europea, in *Dir. Un. eur.*, 1/2023, p. 77 ss.; M. NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di "data retention"*, in *Dir. Un. eur.*, 4/2014, p. 803 ss.; G. FORMICI, *Le Conclusioni dell'Avvocato Generale nel rinvio pregiudiziale C-178/22 promosso dal Tribunale di Bolzano: "quo vadis, data retention"?*, in *MediaLaws*, 2/2023, p. 158 ss.; A. MALACARNE, *Corte di giustizia e "data retention": ultimo atto?*, in *Cass. pen.*, 12/2021, p. 4105 ss.; E. COLOMBO, *"Data retention" e Corte di giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della Direttiva 2006/24/CE*, in *Cass. pen.*, 7/2014, p. 2705 ss.; L. TRUCCO, *"Data retention": la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. it.*, 8/2014, p. 1850 ss.; G. FORMICI, *La "data retention saga" al capolinea? Le ultime pronunce della CGUE in materia di conservazione dei metadati per scopi securitari, tra conferme e nuove aperture*, in *DPCE online*, 1/2021, p. 1361 ss.; M. NINO, *La disciplina internazionale ed europea della "data retention" dopo le sentenze "Privacy International" e "La Quadrature du Net" della Corte di giustizia UE*, in *Dir. Un. eur.*, 1/2021, p. 93 ss.; E. ANDOLINA, *La sentenza della Corte di giustizia UE nel caso "H.K. c. Prokuratuur": un punto di non ritorno nella lunga "querelle" in materia di "data retention"?*, in *Proc. pen. e giust.*, 5/2021, p. 1204 ss.; C. GRECO, *Quest'acquisizione non s'ha da fare: ennesimo "no" della Corte di Giustizia alla "data retention" indiscriminata in campo penale*, in *Dir. inform.*, 2/2021, p. 235 ss.; F. GUELLA, *"Data retention" e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali*, in *DPCE online*, 2/2017, p. 19 ss.; G. TIBERI, *Il caso "Tele2 Sverige/Watson": una "iconica" sentenza della Corte di Giustizia nella saga sulla "data retention"*, in *Quad. cost.*, 2/2017, p. 434 ss.

[92] Sul punto si veda G. ZICCARDI, *Diritti digitali. Informatica giuridica per le nuove professioni*, Raffaello Cortina Editore, Milano, 2022.

Tale approccio mira a garantire un equilibrio tra l'efficacia delle indagini e il rispetto dei diritti fondamentali, evitando una conservazione indiscriminata e massiva delle informazioni personali.

Per tali ragioni il Garante ha richiesto un intervento normativo finalizzato a conformare la disciplina nazionale ai principi sanciti dalla Corte di giustizia. A tal fine sarebbe necessario subordinare l'acquisizione dei dati all'autorizzazione del GIP o di un'autorità amministrativa, ossia un soggetto terzo rispetto al Pubblico Ministero che dirige le indagini, nonché differenziare i tipi di dati e prevedere dei più bassi termini di ritenzione degli stessi.

Tuttavia, la Corte di cassazione ha espresso un'opinione contraria rispetto a quella del Garante. Ha infatti affermato in più occasioni[93] che la disciplina interna fosse compatibile con il canone di proporzionalità perché delimita temporalmente la durata della conservazione e demanda al pubblico ministero l'effettivo controllo della stretta necessità dell'acquisizione dei dati. Ad avviso della Corte, l'indicazione della Corte di giustizia relativa alla necessità di un controllo rimesso ad una «autorità giudiziaria» sarebbe da intendere come compatibile con l'attribuzione di tale vaglio al pubblico ministero stesso.

La Cassazione ha, inoltre, affermato che «non può ritenersi che la disciplina italiana di conservazione dei dati di traffico (c.d. *data retention*) sia in contrasto con le pronunce della Corte di giustizia datate 8 aprile 2014 e 21 dicembre 2016 poiché la suddetta normativa prevede la conservazione dei dati per un periodo limitato pari a 24 mesi, subordina la possibilità di acquisizione degli stessi soltanto a finalità di accertamento e repressione dei reati, prevede che l'utilizzazione degli stessi dati sia sottoposta al provvedimento di acquisizione emesso da parte del Pubblico Ministero e cioè di un organo giurisdizionale che procede nell'ambito di una attività di indagine preliminare. Ne deriva quindi che la legislazione italiana non prevede la facoltà delle autorità pubbliche di accesso indiscriminato ai dati sensibili bensì la limita ai soli casi di indagini per fatti di reato svolte entro un determinato arco temporale di 24 mesi

[93] Si fa qui riferimento alle sentenze Cass., Sez. V, 24 aprile 2018, n. 273892; Cass. Sez. III, 23 agosto 2019, n. 36380; Cass. Sez. II, 13 febbraio 2020, n. 5741 in *DeJure.it*.

(elevati a 72 solo per fatti di reato di particolare allarme sociale) e la subordina alla autorizzazione proveniente da un organo giurisdizionale. […] Va pertanto ribadita la legittimità della normativa nazionale di riferimento costituita dall'art. 132 Codice della privacy, poiché la deroga al diritto alla riservatezza delle comunicazioni è prevista per un periodo limitato, ha come esclusivo obiettivo l'accertamento e la repressione dei reati è subordinato alla emissione di un provvedimento da parte di un'autorità giurisdizionale»[94].

Nel 2021 la Corte di giustizia è nuovamente intervenuta per chiarire gli interrogativi scaturiti dalle precedenti sentenze, precisando che l'acquisibilità processuale dei dati di traffico è limitata ai soli procedimenti per gravi reati o per gravi minacce per la sicurezza pubblica e deve essere subordinata all'autorizzazione di un'autorità terza rispetto a quella pubblica richiedente[95]. In questo modo la Corte rimarca l'esigenza di un vaglio da parte di un'autorità non tanto e non solo giudiziaria, quanto piuttosto

[94] Cass. pen., sez. II, 13 febbraio 2020, n. 5741, in *DeJure.it*.

[95] Cfr. Corte di Giustizia, Grande Sezione, 2 marzo 2021, causa C-746/18 avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dal Riigikohus (Corte suprema, Estonia), con decisione del 12 novembre 2018, pervenuta in cancelleria il 29 novembre 2018. Più precisamente, la Corte, al punto 45 della sentenza, precisa che «l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale consenta l'accesso di autorità pubbliche ad un insieme di dati relativi al traffico o di dati relativi all'ubicazione, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali da costui utilizzate e a permettere di trarre precise conclusioni sulla sua vita privata, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati, senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica, e ciò indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo […] la disciplina europea osta ad una normativa nazionale, la quale renda il pubblico ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento, competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale». Per un approfondimento si veda F. TORRE, *"Data retention": una ventata di "ragionevolezza" da Lussemburgo (a margine della sentenza della Corte di giustizia 2 marzo 2021, C-746/18)*, in *Consulta online*, 2/2021, p. 615 ss.; G. CASCONE, *La Corte di Giustizia dell'Unione europea definisce le condizioni per la legittimità delle normative nazionali in materia di acquisizione dei tabulati. Le ripercussioni sull'ordinamento italiano della sentenza del 2 marzo 2021 (C-746/18) nel caso H.P.*, in *Cass. pen.*, 2/2022, p. 419 ss.

terza; dato, quest'ultimo, difficilmente compatibile con la figura del pubblico ministero.

2.1.4. Tecnologie di riconoscimento facciale

Le Tecnologie di riconoscimento facciale (TRF) sono sistemi progettati per identificare o autenticare un individuo basandosi sulle caratteristiche uniche del suo volto[96].

L'*AI Act* offre anche una definizione di identificazione biometrica al Considerando 15: «La nozione di identificazione biometrica di cui al presente regolamento dovrebbe essere definita come il riconoscimento automatico di caratteristiche fisiche, fisiologiche e comportamentali di una persona, quali il volto, il movimento degli occhi, la forma del corpo, la voce, la prosodia, l'andatura, la postura, la frequenza cardiaca, la pressione sanguigna, l'odore, la pressione esercitata sui tasti, allo scopo di determinare l'identità di una persona confrontando i suoi dati biometrici con quelli di altri individui memorizzati in una banca dati di riferimento, indipendentemente dal fatto che la persona abbia fornito il proprio consenso. Sono esclusi i sistemi di IA destinati a essere utilizzati per la verifica biometrica, che include l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso di sicurezza a locali».

---

[96] Per un approfondimento sul tema si veda il lavoro di G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, Napoli, 2021; v. anche M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini,* in F. Basile, M. Caterini, S. Romano (a cura di), *Il sistema penale ai confini delle hard sciences*, cit., p. 122 ss.; J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. e proc. pen.*, 3/2022, p. 1057 ss.; E. SACCHETTO, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *Leg. pen.*, 16 ottobre 2020; E. CRIPPA, *Riconoscimento facciale e vita privata*, in *Riv. it. dir. e proc. pen.*, 4/2023, p. 1660 ss.; F. DI MATTEO, *La riservatezza dei dati biometrici nello Spazio europeo dei diritti fondamentali: sui limiti all'utilizzo delle tecnologie di riconoscimento facciale*, in *Freedom, Security & Justice: European Legal Studies*, 1/2023, p. 74 ss.; S. DEL GATTO, *La "governance" delle nuove tecnologie tra tentativi di regolazione e istanze di "self regulation". Il caso del riconoscimento facciale*, in *Riv. it. dir. pubbl. com.*, 1/2023, p. 37 ss.; F. PAOLUCCI, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *MediaLaws*, 1/2021, p. 204 ss.

Queste tecnologie rientrano pertanto nella categoria della raccolta di dati biometrici, che consentono di distinguere le persone attraverso specifici attributi fisici come le impronte digitali, la conformazione dell'iride o il DNA. Ciò che rende le TRF particolarmente significative è il fatto che i dati da acquisire e analizzare, ossia i tratti del volto, sono altamente visibili e relativamente semplici da raccogliere, sia nel mondo reale che in quello digitale[97].

L'art. 4, n. 14) del Regolamento generale sulla protezione dei dati (GDPR) definisce i dati biometrici come «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici».

L'art. 9, inoltre, afferma che «è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona». Di conseguenza, le tecnologie di TRF rientrano in questa categoria delle particolari tipologie di dati disciplinate dall'art. 9, e il trattamento di tali dati è soggetto a un regime di protezione rafforzato, con la possibilità, prevista dallo stesso art. 9, per ciascuno Stato membro, di imporre ulteriori restrizioni al trattamento dei dati biometrici, specialmente quando si tratta di informazioni così sensibili.

Utilizzando tecniche biometriche, il *software* estrae i tratti distintivi del volto e li trasforma in codici alfanumerici. Questi codici possono essere ulteriormente arricchiti con altri indicatori, creando un profilo digitale dettagliato della persona che può essere utilizzato per scopi di identificazione o autenticazione.

Un primo utilizzo di questo procedimento è quello dell'autenticazione o verifica dell'identità di una persona, attraverso l'abbinamento del volto rilevato dal vivo con la foto presente su un documento di identità. Un altro impiego riguarda la ricerca di

[97] Per un approfondimento si veda F. LA VATTIATA, *Brevi note "a caldo" sulla recente Proposta di Regolamento UE in tema di intelligenza artificiale*, in *Dir. pen. e Uomo*, 30 giugno 2021, p. 9 ss.

una corrispondenza tra una fotografia acquisita e quelle già presenti in un *database*. Questa funzione è particolarmente utile in contesti come la sicurezza pubblica o la gestione dei servizi, dove è essenziale identificare rapidamente e con precisione gli individui sulla base delle immagini archiviate.

Infine, le TRF possono essere utilizzate per la rilevazione dei volti in tempo reale, ad esempio attraverso telecamere a circuito chiuso. In questo caso, il sistema confronta le immagini catturate con quelle contenute nel *database*, alla ricerca di una corrispondenza. Questa funzione permette una sorveglianza efficace e tempestiva in ambienti pubblici o privati, facilitando l'individuazione di persone di interesse.

Per insegnare al sistema a riconoscere dei volti si utilizzano le già citate tecniche di *deep learning*, raccogliendo un vasto campione di immagini, che vengono accuratamente catalogate ed etichettate e in seguito analizzate dalla macchina, che riconosce la frequenza con cui determinati schemi si ripetono all'interno del campione, migliorando progressivamente nel riconoscerli[98].

Le tecnologie così descritte rappresentano uno strumento con ampie possibilità di applicazione. Esse possono essere integrate in sistemi di videosorveglianza diffusi, mirati a catturare il volto delle persone, e possono essere impiegate per una vasta gamma di scopi, che spaziano dalla gestione della sicurezza pubblica a usi di natura commerciale. Questa tecnologia segna un significativo passo evolutivo nella raccolta e gestione dei dati biometrici, rendendoli utilizzabili in molteplici ambiti. Le sue applicazioni variano dall'implementazione di strategie commerciali volte ad aumentare la vendita di prodotti, all'uso da parte delle autorità pubbliche per il controllo e la sorveglianza, anche in contesti bellici[99].

---

[98] M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini,* cit., p. 128.

[99] Ad esempio, nel marzo 2022, durante le prime settimane dell'invasione russa in Ucraina, un'attivista russa venne arrestata a Mosca per aver organizzato tramite Twitter una manifestazione contro la guerra. La donna è stata fermata all'uscita della metropolitana grazie al sistema di riconoscimento facciale Sphere, installato sui mezzi pubblici della capitale russa. Questa vicenda ha sollevato ulteriori preoccupazioni riguardo all'uso delle tecnologie di sorveglianza per reprimere il dissenso politico. Sotto questo profilo, di particolare interesse è anche la sentenza della Corte Edu con riferimento al caso *Glukhin c. Russia,* dove la Corte ha affermato che il trattamento dei dati personali del ricorrente, un cittadino russo autore di una manifestazione solitaria di natura pacifica, effettuato

In Italia, dal 2017 viene utilizzato il sistema SARI (Sistema automatico di riconoscimento immagini) utilizzato esclusivamente nella sua funzione da remoto che permette l'identificazione di un soggetto sconosciuto a partire da un'immagine fotografica[100].

Il Garante per la protezione dei dati personali ha espresso una forte critica riguardo alla modalità in tempo reale adottata da SARI, che «realizza un trattamento automatizzato su larga scala che può riguardare, tra l'altro, anche coloro che siano presenti a manifestazioni politiche e sociali, che non sono oggetto di "attenzione" da parte delle forze di Polizia, potendo determinare una evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui»[101].

---

tramite strumenti di riconoscimento facciale specificatamente utilizzati per identificarlo e procedere al suo arresto, non può essere ritenuto – secondo la Corte – necessario nel contesto di una società democratica. L'uso di detti sofisticati sistemi di riconoscimento facciale, da parte delle autorità della Federazione Russa, a parere dei giudici, risulta lesivo anche del diritto alla libertà di espressione del ricorrente e appare, di conseguenza, del tutto incompatibile con i valori essenziali di una società democratica – governata dai principi basilari dello stato di diritto – per il cui mantenimento e per il cui sviluppo progressivo la Convenzione stessa è stata concepita. Per un approfondimento si veda G. MOBILIO, *La Corte EDU condanna il ricorso alle tecnologie di riconoscimento facciale per reprimere il dissenso politico: osservazioni a partire dal caso "Glukhin c. Russia"*, in *DPCE online*, 1/2024, p. 695 ss.; O. BRUNO, *La condanna per manifestazione pacifica (non preavvisata e) con riconoscimento facciale viola i diritti fondamentali*, in *Proc. pen. e giust.*, 2/2024, p. 433 ss.; C. NARDOCCI, *Il riconoscimento facciale sul "banco" degli imputati. Riflessioni a partire, e oltre, Corte EDU "Glukhin c. Russia"*, in *BioLaw Journal*, 1/2024, p. 279 ss.; G. GALLO, *Tecnologie di riconoscimento facciale e diritti fondamentali a rischio: il caso "Glukhin c. Russia" dinanzi alla Corte europea dei diritti dell'uomo*, in *MediaLaws*, 3/2023, p. 189 ss.

[100] In particolare, sul sito del Ministero dell'Interno si legge che SARI, attraverso «una ricerca computerizzata nella banca dati AFIS, e grazie a due algoritmi di riconoscimento facciale, è in grado di fornire un elenco di immagini ordinato secondo un grado di similarità», cfr. www.interno.gov.it. La banca dati AFIS (*Automated Fingerprint Identification System*) è un sistema automatizzato di acquisizione delle impronte digitali, di cui fa parte SSA (Sotto sistema anagrafico), che contiene, invece, le foto segnaletiche presenti nei *database* della polizia, insieme alle informazioni fisiche delle persone ritratte.

[101] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, provvedimento n. 127 del 25 marzo 2021. Il Garante aveva ritenuto, al contrario, che non destasse preoccupazioni l'utilizzo di SARI in modalità cosiddetta differita, per individuare una corrispondenza tra un fotogramma che ritraeva l'autore di un reato e le immagini presenti nel *database*. In questo frangente il Garante ha ritenuto che si trattasse di «un mero ausilio all'agire umano, avente lo scopo di velocizzare l'identificazione, da parte dell'operatore di polizia, di un soggetto ricercato della cui immagine facciale si disponga, ferma restando l'esigenza dell'intervento dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema automatizzato».

Le TRF richiedono un'attenta analisi dal punto di vista penalistico, poiché sollevano questioni che vanno ben oltre i rischi di violazione della *privacy* e del trattamento corretto dei dati personali. Questi sistemi, infatti, spesso giustificati dalla necessità di tutelare la sicurezza pubblica, utilizzano la raccolta ed elaborazione di dati personali allo scopo di influenzare o controllare coloro ai quali essi appartengono (c.d. sorveglianza di massa) e «valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica» (profilazione)[102].

Tuttavia, tali pratiche rischiano di comprimere severamente i diritti fondamentali e costituzionalmente garantiti, come quelli relativi alla personalità, alla riunione, all'associazione, e alla libera manifestazione del pensiero. Questo scenario pone una sfida significativa per il diritto penale, che deve bilanciare le esigenze di sicurezza con la protezione delle libertà individuali.

Innanzitutto, l'installazione di tecnologie di riconoscimento facciale in spazi pubblici può generare un preoccupante effetto di autocensura tra la popolazione, noto

[102] Così recita l'art. 4 del art. 4 del GPDR. Per un approfondimento circa le tecniche di profilazione si veda A. SPANGARO, *Il concetto di profilazione tra "direttiva madre" e GDPR*, in *Giur. it.*, 7/2022, p. 1579 ss.; F. LAGIOIA, G. SARTOR, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in *federalismi.it*, 11/2020, p. 85 ss.; D. MESSINA, *Online platforms, profiling, and artificial intelligence: new challenges for the GDPR and, in particular, for the informed and unambiguous data subject's consent*, in *MediaLaws*, 2/2019, p. 159 ss.; M. FASAN, *Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico*, in *BioLaw Journal*, 1/2019, p. 6 ss.; R. DE MEO, *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Dir. inform.*, 3/2013, p. 587 ss.; G. MACCABONI, *La profilazione dell'utente telematico tra tecniche pubblicitarie online e tutela della privacy*, in *Dir. inform.*, 3/2001, p. 425 ss.. Con riferimento alla sorveglianza di massa: F. MOLLO, *Sorveglianza di massa, rispetto della vita privata e trattamento di categorie particolari di dati nel quadro multilivello di tutela della persona*, in *federalismi.it*, 19/2023, p. 267 ss.; D. LYON, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano, 2002; G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, Milano, 2015; A. STIANO, *Ancora sul bilanciamento tra la tutela del diritto alla privacy e l'utilizzo di strumenti di sorveglianza di massa: tra garanzie procedurali e sostanziali*, in *Riv. dir. int.*, 3/2021, p. 904 ss.; M. NINO, *La normalizzazione della sorveglianza di massa nella prassi giurisprudenziale delle Corti di Strasburgo e Lussemburgo: verso il cambio di paradigma del rapporto "privacy v. security"*, in *Freedom, Security & Justice: European Legal Studies*, 3/2022, p. 105 ss.; A. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto. La "data retention" al test di legittimità*, in *Dir. pubbl. comp. eur.*, 3/2014, p. 1224 ss.

come *chilling effect*[103]. La consapevolezza di essere costantemente sorvegliati potrebbe dissuadere le persone dall'esercitare i propri diritti fondamentali, come la libertà di espressione, la partecipazione a manifestazioni, e il diritto di associazione, limitando la capacità dei cittadini di esprimere le proprie opinioni e di partecipare attivamente alla vita pubblica.

Inoltre, i sistemi di riconoscimento facciale necessitano di poter attingere a un catalogo quanto più ampio e variegato possibile di immagini, spesso reperite senza il consenso delle persone coinvolte, anche ricorrendo a *database* già esistenti e concepiti per altri utilizzi, come accaduto con le raccolte di foto segnaletiche a disposizione delle autorità di pubblica sicurezza. Ne discendono problematiche connesse al rispetto del diritto alla *privacy* delle persone le cui foto sono state utilizzate per allenare i sistemi di riconoscimento facciale.

In ragione di questi dubbi, l'*AI Act* ha inserito le TRF tra i sistemi di intelligenza artificiale ad alto rischio. A causa delle significative implicazioni per la *privacy* e i diritti fondamentali, l'uso di queste tecnologie dovrebbe essere soggetto a restrizioni rigorose o, in determinate circostanze, persino vietato. Questa classificazione riflette la crescente preoccupazione riguardo ai potenziali abusi e agli effetti negativi che tali sistemi possono avere sulla libertà individuale e sulla protezione dei dati personali.

Gli Stati membri avranno la possibilità di utilizzare le tecnologie di riconoscimento facciale (sia quelle in tempo reale che «differito») per supportare le attività investigative su specifici reati, in particolare quelli di maggiore gravità. Questi strumenti potranno essere impiegati nella lotta contro la criminalità organizzata e il terrorismo, nonché nella ricerca di persone scomparse o vittime di sequestri[104]. La capacità di

---

[103] Il *chilling effect* viene esplicato anche da F. VIGANÒ, *La proporzionalità della pena. Profili di diritto penale e costituzionale*, cit., p. 277 ss. Si veda inoltre, per un profilo più tecnico: A. GULLO, *Diffamazione, pena detentiva e "chilling effect": la Consulta bussa alla porta del legislatore*, in *Dir. pen. e proc.*, 2/2021, p. 217 ss; N. RECCHIA, *Il principio di proporzionalità nel diritto penale. Scelte di criminalizzazione e ingerenza nei diritti fondamentali*, cit., p. 122 ss.

[104] Più precisamente, l'articolo 5 dell'*AI Act*, alla lettera h), dispone quanto segue: «l'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto a meno che, e nella misura in cui, tale uso sia strettamente necessario per uno degli obiettivi seguenti: i) la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse; ii) la prevenzione di

analizzare immagini catturate in tempo reale o di confrontarle con *database* esistenti offre un vantaggio significativo nelle indagini, consentendo interventi più rapidi ed efficaci in situazioni critiche.

Già prima dell'*AI Act* il Parlamento europeo aveva evidenziato l'importanza di una regolamentazione della materia, e con la Risoluzione del 6 ottobre 2021 chiese alla Commissione «una moratoria sulla diffusione dei sistemi di riconoscimento facciale per le attività di contrasto con funzione di identificazione»[105].

2.1.5. Profili penalistici della tutela dell'identità della persona

L'avanzamento dell'intelligenza artificiale ha reso inadeguati gli attuali strumenti giuridici per la protezione dell'identità personale. L'uso di algoritmi di *machine learning* per analizzare dati e l'integrazione di componenti basati sull'IA nelle tecnologie di uso quotidiano hanno ampliato e diversificato i rischi per l'identità personale e i diritti correlati. La memorizzazione e l'elaborazione automatizzata di dati personali da parte di sistemi intelligenti possono produrre esiti imprevedibili per gli individui, spesso al di fuori del loro controllo.

---

una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico; iii) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni».

[105] Così il paragrafo 27 della Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale (2020/2016(INI)). L'Italia ha risposto a questa richiesta con l'introduzione di una moratoria sull'uso dei sistemi biometrici di riconoscimento facciale in luoghi pubblici o aperti al pubblico fino alla fine del 2023, una misura temporanea in attesa dell'approvazione dell'*AI Act*. Tuttavia, questa sospensione non si applicava ai trattamenti effettuati dalle autorità competenti per fini di prevenzione e repressione dei reati o per l'esecuzione di sanzioni penali, come previsto dal d.lgs. n. 51/2018. Questa eccezione consentiva alle autorità di continuare a utilizzare queste tecnologie in ambiti strettamente legati alla sicurezza pubblica e alla giustizia penale. Al successivo paragrafo 28 il Parlamento esprime preoccupazione «per l'utilizzo di *database* privati di riconoscimento facciale da parte delle autorità di contrasto e dei servizi di *intelligence*, come *Clearview AI*, una banca dati di oltre tre miliardi di immagini raccolte illegalmente dai *social network* e da altre fonti *Internet*». Per un approfondimento si veda R. PIROSA, *Tecniche biometriche e trattamento dei dati. Il caso "Clearview AI": l'avamposto di una rivoluzione pacifica*, in *Notizie di Politeia*, 151/2023, p. 95 ss.

Di fronte a queste nuove sfide, il modello del consenso, che spesso funge da base giuridica per il trattamento dei dati personali *online*, si rivela inadeguato. Questo sistema richiede infatti agli utenti di dare il loro assenso a trattamenti di dati le cui conseguenze sono spesso difficili, se non impossibili, da prevedere. Nella pratica, gli utenti sono chiamati a fare una scelta senza avere piena consapevolezza dell'impatto che tale trattamento può avere sulla loro identità e *privacy*, soprattutto in un contesto in cui l'analisi dei dati e le decisioni automatizzate tramite IA possono produrre risultati imprevedibili e complessi da comprendere.[106]

La situazione descritta solleva nuove e complesse questioni legate alla riservatezza, profondamente diverse rispetto a quelle tradizionali. Oggi, infatti, risulta difficile prevedere quali informazioni, diffuse *online*, possano rivelare aspetti personali che preferiremmo rimanessero privati, come gusti, preferenze o dettagli intimi. Non solo è complicato determinare chi avrà accesso a tali dati, ma anche per quali scopi verranno utilizzati.

Le tecniche di profilazione basate sull'analisi dei dati e integrate con l'idea di architettura della scelta già citata nei paragrafi precedenti[107] stanno diventando strumenti centrali nel *marketing* commerciale e nella comunicazione politica. Ogni giorno, milioni di individui sono bersagliati da pubblicità mirate, suggerimenti di prodotti o servizi e contenuti personalizzati, che appaiono su piattaforme digitali come *social network*, motori di ricerca, siti di *e-commerce* e app di messaggistica. Questo flusso costante di raccomandazioni non solo influenza le scelte d'acquisto e i contenuti da fruire, ma

---

[106] Per un approfondimento sul tema del consenso al trattamento dei dati personali si veda I. SALVADORI, *Il trattamento senza consenso di dati personali altrui reperibili su Internet costituisce reato?*, in *Dir. pen. e proc.*, 4/2006, p. 467 ss.; G. ANDREAZZA, *Cronaca giornalistica e trattamento dei dati personali: le condizioni di esonero dal consenso dell'interessato*, in *Cass. pen.*, 12/2009, p. 4864 ss.; S. CAGLI, *La rilevanza del consenso nella disciplina del trattamento dei dati personali*, in *Ind. pen.*, 2/2001, p. 855 ss.; L. AULINO, *Consenso al trattamento dei dati e carenza di consapevolezza: il "legal design" come un rimedio "ex ante"*, in *Dir. inform.*, 2/2020, p. 303 ss.; B. SIRGIOVANNI, *Informed Consent to Processing of Genetic Data*, in *The Italian Law Journal*, 2/2022, p. 955 ss.; S. THOBANI, *Richieste preventive di consenso al trattamento dei dati: quando la cautela rischia di essere eccessiva*, in *Dir. inform.*, 3/2020, p. 499 ss.; P. IAMICELI, *Il consenso al trattamento dei dati personali e la giurisprudenza europea tra tutela dei diritti fondamentali e giustizia contrattuale*, in *Persona e Mercato*, 1/2024, p. 27 ss.

[107] Cfr. R. H. THALER, C. R. SUNSTEIN, *Nudge. The final edition,* cit., p. 11.

orienta anche le opinioni politiche e i comportamenti sociali, rendendo le persone sempre più vulnerabili alle manipolazioni di tali sistemi.

Il Codice della privacy dedica agli illeciti penali in materia di trattamento dei dati personali il Capo II del Titolo III[108].

In particolare, l'art. 167 co. 1 prevede il reato di trattamento illecito di dati, punito con la reclusione da sei mesi a un anno e sei mesi[109]. Ai fini della sussistenza del reato è necessario che sussista il dolo specifico, ovvero che l'autore del reato agisca con l'intenzione di ottenere un profitto per sé o per altri, oppure con l'obiettivo di arrecare un danno al soggetto interessato.

Il nocumento previsto dall'art. 167 deve essere subito dal soggetto titolare dei dati personali o anche da terzi, come conseguenza diretta di un trattamento illecito dei dati e si riferisce a un danno giuridicamente rilevante, che può essere di natura sia patrimoniale che non patrimoniale. In altre parole, il nocumento può manifestarsi non solo come una perdita economica, ma anche come una lesione di diritti personali o

---

[108] Tra le disposizioni più rilevanti ai nostri fini occorre citare l'art. 167 che disciplina la fattispecie di trattamento illecito di dati; l'art. 168, rubricato «falsità nelle dichiarazioni e notificazioni al Garante»; l'art. 170 che disciplina il delitto di inosservanza di provvedimenti del Garante, punito con la reclusione da tre mesi a due anni e integrato da chi, essendo tenuto a rispettarli, violi i provvedimenti adottati dal Garante in materia di dati meritevoli di particolare tutela; l'art. 172 che prevede, in caso di condanna per uno dei delitti previsti dal Codice, la pena accessoria della pubblicazione della sentenza. Sul punto si veda L. PALAMARA, *Note in tema di rilevanza penale del trattamento illecito di dati personali*, in *Cass. pen.*, 6/2005, p. 1898 ss.; M. CHIAROLLA, *Trattamento dei dati personali su Internet ed illecito penale (nota a Cass. 17 nov. 2004)*, in *Foro it.*, 1/2006, p. 46 ss.; I. SALVADORI, *Il trattamento senza consenso di dati personali altrui reperibili su Internet costituisce reato?*, cit., p. 467 ss.; V. MANES, N. MAZZACUVA, *GDPR e nuove disposizioni penali del Codice "privacy"*, cit., p. 171 ss.; P. TRONCONE, *Profili penali del codice della privacy*, in *Riv. pen.*, 12/2004, p. 1147 ss.; E. ANTONINI, *Il trattamento illecito di dati personali nel codice della privacy: i nuovi confini della tutela penale*, cit., p. 340 ss.; M. LAMANUZZI, *Diritto penale e trattamento dei dati personali,* cit., p. 227 ss.; D. PROVOLO, *Il sistema sanzionatorio del novellato Codice della "privacy" e la tutela penale "patchwork" dei dati genetici e dei dati biometrici*, cit., p. 242 ss.; G. CORRIAS LUCENTE, *La nuova normativa penale a tutela dei dati personali*, in F. Cardarelli, S. Sica, V. Zeno Zencovich, *Il codice dei dati personali. Temi e problemi*, Giuffrè, Milano 2004; M. LUBERTO, *I reati informatici contro il diritto alla privacy. La tutela fornita dal d.lgs. n. 196 del 2003 e dal codice penale*, in *Giur. mer.*, 2008, p. 898 ss.; A. MANNA, *Il quadro sanzionatorio penale e amministrativo del codice sul trattamento dei dati personali*, in *Dir. inform.*, 2003, p. 727 ss.; V. PLANTAMURA, *La tutela penale dei dati personali*, in *Dir. inform.*, 2007, p. 649 ss.

[109] Il testo dell'art. 167, comma 1, recita: «Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi».

della dignità della persona, ad esempio legata alla violazione della riservatezza o della reputazione[110].

Un altro elemento della fattispecie prevista dall'art. 167 è rappresentato dalla mancanza del consenso dell'interessato. La norma richiama espressamente gli artt. 23 e 26, che stabiliscono come condizione di liceità del trattamento dei dati il consenso esplicito dell'interessato. Questo consenso deve essere fornito in forma scritta nel caso di trattamento di dati sensibili, a meno che non si applichino alcune eccezioni tassativamente previste[111].

Il consenso, in questo contesto, agisce come un elemento negativo della fattispecie: qualora il consenso sia presente e regolarmente fornito, il trattamento non costituirà un fatto tipico penalmente rilevante.

Il bene giuridico protetto è il diritto alla protezione dei dati personali, un interesse che, secondo la teoria costituzionalmente orientata del bene giuridico di cui si è detto nei paragrafi precedenti, possiede una rilevanza costituzionale indiretta. Questo perché è funzionale e strumentale alla tutela dell'identità, considerata una manifestazione della personalità che merita protezione ai sensi dell'art. 2 della Costituzione. A supporto di questa interpretazione, la dottrina sostiene che il bene tutelato dalla norma non sia soltanto la riservatezza, ma, in maniera preminente, la protezione dei dati personali.

In dottrina si è osservato che, se l'oggetto della norma fosse solo la riservatezza, bene giuridico personale e disponibile, la procedibilità del reato dovrebbe essere subordinata alla querela di parte, coerentemente con una politica criminale basata sul principio di *extrema ratio*. Tuttavia, il fatto che la procedibilità sia d'ufficio suggerisce un approccio diverso: la vita privata dell'individuo non sarebbe considerata il bene primario tutelato, ma piuttosto quello finale a cui il soggetto ambisce. Il bene protetto dalla norma sarebbe invece l'interesse alla sicurezza dei dati e l'efficienza del sistema

[110] Cfr. *ex multis* Cass. pen., sez. III, 19 giugno 2018, n. 52135 e Cass. pen., sez. III, 23 novembre 2016, n. 15221, in *DeJure.it*.

[111] Si fa riferimento alle eccezioni indicate nell'art. 24 e in specifiche norme della Parte II del Codice, relative a trattamenti effettuati da forze di polizia, per fini di ordine pubblico o per la difesa sociale.

di regolamentazione in materia, che fa capo al Garante per la protezione dei dati personali. Questa lettura implica che la norma non si limiti a tutelare la riservatezza individuale, ma si preoccupi anche di preservare la fiducia e il corretto funzionamento del sistema di gestione e trattamento dei dati personali nell'interesse della collettività[112].

Sul punto la Corte di cassazione ha affrontato il tema del c.d. *spamming*, ovvero l'invio massivo di messaggi pubblicitari senza il consenso degli utenti. Questa pratica costituisce una violazione dei diritti alla riservatezza e al trattamento corretto dei dati personali, oltre a porre in evidenza la necessità di garantire una maggiore tutela per gli individui. Tuttavia, la Corte precisa che «affinché tale condotta assuma rilievo penale, occorre che si verifichi per ciascun destinatario un effettivo "nocumento", che non può certo esaurirsi nel semplice fastidio di dover cancellare di volta in volta le *mail* indesiderate, ma deve tradursi in un pregiudizio concreto, anche non patrimoniale, ma comunque suscettibile di essere giuridicamente apprezzato»[113]. Pertanto, si rende necessaria un'accurata verifica per determinare se l'utente abbia chiaramente manifestato al mittente la volontà di non ricevere ulteriori messaggi e se, nonostante tale richiesta, il soggetto agente, ossia il titolare o il responsabile del trattamento[114] dei dati, abbia continuato, in modo non sporadico, ad inviare comunicazioni indesiderate.

L'elemento chiave è la valutazione della condotta ripetuta e intenzionale del mittente, che, ignorando la volontà esplicita dell'utente, potrebbe aggravare la situazione al punto da costituire un illecito trattamento dei dati personali. Di conseguenza, l'accertamento di tali comportamenti assume un ruolo centrale nel determinare la

---

[112] Di questo parere è A. MANNA, *Prime osservazioni sul Testo Unico in materia di protezione dei dati personali: profili penalistici*, in *privacy.it*, 2003; si veda anche M. LAMANUZZI, *Diritto penale e trattamento dei dati personali,* cit., p. 227; D. PROVOLO, *Il sistema sanzionatorio del novellato Codice della "privacy" e la tutela penale "patchwork" dei dati genetici e dei dati biometrici*, cit., p. 232 ss.

[113] Cass. pen., Sez. III, 10 ottobre 2019, n. 41604, in *Dejure.it*.

[114] Ai sensi dell'art. 4 del Codice della *privacy*, è il titolare del trattamento «la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza»; è invece responsabile del trattamento «la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali».

responsabilità giuridica e le eventuali sanzioni applicabili al titolare o al responsabile del trattamento.

La giurisprudenza della Cassazione si è chiesta, inoltre, se tale reato possa essere classificato come un proprio o improprio.

Inizialmente si riteneva che i reati previsti e disciplinati dal Codice della *privacy* dovessero considerarsi propri, potendo essere integrati solo dal titolare o dal responsabile del trattamento.

La sentenza della Cassazione n. 13102, depositata il 29 marzo 2023, ha invece ritenuto che si trattasse di un reato comune, che può essere commesso da chiunque e non richiede, per la sua configurazione, una qualifica soggettiva specifica da parte del reo.

Questa interpretazione deriva dall'analisi del testo normativo, che non impone particolari requisiti di qualifica o *status* per il soggetto attivo del reato. In altre parole, il reato di trattamento illecito di dati personali non è limitato a soggetti che abbiano ruoli specifici, come il titolare o il responsabile del trattamento, ma può essere commesso da qualunque persona che, in violazione della normativa, tratti dati personali con dolo specifico (ovvero per trarre profitto o arrecare danno all'interessato). Il reato può configurarsi anche nel caso in cui, ad esempio, un privato cittadino diffonda un dato sensibile altrui di cui sia entrato in possesso solo occasionalmente.

Più precisamente, la citata sentenza della Cassazione, al punto 1 del Considerato in diritto, afferma che «Ad una semplice lettura della norma punitiva, l'*incipit* "chiunque" già esclude in radice una interpretazione in senso restrittivo riferita ai destinatari: è evidente che, laddove si parla di persona fisica, ci si intende riferire al soggetto privato in sé considerato, e non solo a quello che svolga un compito, per così dire, istituzionale, di depositario della tenuta dei dati sensibili e delle loro modalità di utilizzazione all'esterno: una interpretazione siffatta finirebbe con l'esonerare in modo irragionevole dall'area penale tutti i soggetti privati, così permettendo quella massiccia diffusione di dati personali che il Legislatore, invece, tende ad evitare. Può quindi affermarsi senza tema di smentita che l'assoggettamento alla norma in tema di divieto di diffusione di dati sensibili riguardi tutti indistintamente i soggetti entrati in possesso

di dati, i quali saranno tenuti a rispettare sacralmente la *privacy* di altri soggetti con i primi entrati in contatto, al fine di assicurare un corretto trattamento di quei dati senza arbitri o pericolose intrusioni».

I giudici sottolineano dunque l'ampia portata della norma, valorizzando il contenuto testuale che conferisce a questa fattispecie un carattere di generalità.

In queste ipotesi occorrerà chiedersi chi sia il soggetto ritenuto responsabile del trattamento illecito, soprattutto quando il reato è stato commesso mediante l'utilizzo di sistemi automatizzati di intelligenza artificiale. Fino a quando non sarà possibile muovere un rimprovero al software stesso, la responsabilità andrà ricercata in capo a chi ha programmato l'algoritmo al fine di ottenere un risultato conforme a quello richiesto dalla fattispecie incriminatrice, oppure in capo a colui che ha richiesto una tale programmazione.

2.2. Intelligenza artificiale e libera manifestazione del pensiero: i social media

La diffusione dei servizi di *internet* interattivo non ha solo generato lacune nella protezione giuridica dell'identità personale, ma ha anche avuto un impatto diretto sul campo di applicazione, sui limiti e sull'ambito di tutela del diritto alla libera manifestazione del pensiero[115]. *Internet*, come spazio interattivo e globale, ha ampliato le

[115] Per una disamina sulla libertà di manifestazione del pensiero, per ciò che rileva ai fini del presente lavoro, si veda A. PACE, M. MANETTI, *La libertà di manifestazione del pensiero. Art. 21*, in G. Branca, A. Pizzorusso (a cura di), *Commentario della Costituzione*, XI, Zanichelli, Bologna, 2006; C. ESPOSITO, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Giuffrè, Milano, 1958; P. BARILE, *Libertà di manifestazione del pensiero*, Giuffrè, Milano, 1975; F. GUELLA, C. PICIOCCHI, *Libera manifestazione del pensiero tra fatti di sentimento e fatti di conoscenza*, in *Quad. cost.*, 4/2013, p. 849 ss.; C. R. CALDERONE, *Libertà di manifestazione del pensiero e limiti*, in *Cass. pen.*, 1/1985, p. 54 ss.; V. ANGIOLINI, *Manifestazione del pensiero e "libertà altrui"*, in *Giur. cost.*, 6/1995, p. 4585 ss.; A. CERRI, *Libertà di pensiero: manifestazione, diffusione, mezzi*, in *Giur. cost.*, 5/1972, p. 2877 ss.; E. SELVAGGI, *Sulla libertà di espressione*, in *Cass. pen.*, 1/2013, p. 342 ss.; G. VECCHIO, *Riflessioni sullo stato della libertà di espressione nell'attuale contesto informativo*, in *dirittifondamentali.it*, 3/2023, p. 14 ss.; A. CAVALIERE, *La discussione intorno alla punibilità del negazionismo, i principi di offensività e libera manifestazione del pensiero e la funzione della pena*, in *Riv. it. dir. e proc. pen.*, 2/2016, p. 999 ss.; P. STANCATI, *Il diritto fondamentale comunitario alla libera*

possibilità di espressione, ma al contempo ha reso più complessa la definizione dei confini tra la libertà di espressione e la necessità di garantire la tutela della *privacy* e dell'identità personale. Tale evoluzione impone una riflessione sui limiti giuridici e sui meccanismi di bilanciamento tra questi diritti fondamentali[116].

Tra i vari servizi di internet interattivo, i *social media* assumono un rilievo particolare per questa analisi, in quanto basano gran parte del loro funzionamento sulla

manifestazione del pensiero: profili critici e ricostruttivi, in *Politica del diritto*, 2/2005, p. 171 ss.; G. M. LABRIOLA, *La libertà di espressione fra ragione e storia. Nota breve su un tema vasto*, in *Notizie di Politeia*, 138/2020, p. 95 ss.; A. AMBROSI, *Libertà di pensiero e manifestazione di opinioni razziste e xenofobe*, in *Quad. cost.*, 3/2008, p. 519 ss.; P. STANCATI, *Lineamenti evolutivi della libertà di manifestazione del pensiero e della informazione: rivoluzione mediatica, "buona" e "cattiva" televisione, multiculturalismo, fenomenologia terroristica*, in *Dir. soc.*, 3/2005, p. 313 ss.; L. ROSSI, *Dall'uso all'abuso: quando la libertà di espressione sconfina nel negazionismo*, in *Riv. it. dir. e proc. pen.*, 1/2020, p. 369 ss.; P. COSTANZO, *Libertà di manifestazione del pensiero e pubblicazione in internet*, in *Dir. inform.*, 2/1998, p. 372 ss.; M. BETZU, *Comunicazione, manifestazione del pensiero e tecnologie polifunzionali*, in *Quad. cost.*, 3/2006, p. 511 ss.; G. CORRIAS LUCENTE, *Internet e libertà di manifestazione del pensiero*, in *Dir. inform.*, 4/2000, p. 597 ss.; T. CASADEI, *La libertà d'espressione e i suoi dilemmi*, in *Notizie di Politeia*, 138/2020, p. 90 ss.; A. NICITA, *Libertà d'espressione e pluralismo 2.0: i nuovi dilemmi*, in *MediaLaws*, 1/2019, p. 314 ss.; O. POLLICINO, *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, in *MediaLaws*, 1/2018, p. 3 ss.

[116] Per un quadro generale sul tema, da diverse prospettive, si veda U. RUFFOLO, *Piattaforme, A.I. generativa e libertà di (formazione e) manifestazione del pensiero. Il caso ChatGPT*, in *Giur. it.*, 2/2024, p. 472 ss.; C. MAGNANI, *Nuovi media, libertà di espressione e costituzionalismo*, in *dirittifondamentali.it*, 2/2023, p. 795 ss.; C. M. REALE, M. TOMASI, *Libertà d'espressione, nuovi media e intelligenza artificiale: la ricerca di un nuovo equilibrio nell'ecosistema costituzionale*, in *DPCE online*, 1/2022, p. 325 ss.; C. MELZI D'ERIL, *La complessa individuazione dei limiti alla manifestazione del pensiero in internet*, in *Dir. inform.*, 4/2011, p. 571 ss.; C. EQUIZI, *Libertà di manifestazione del pensiero e piattaforme online*, in *dirittifondamentali.it*, 3/2021, p. 550 ss.; D. MORANA, *La libertà di manifestazione del pensiero sulla rete tra vecchi e nuovi limiti. Introduzione*, in *MediaLaws*, 1/2020, p. 132 ss.; C. PINELLI, *Poteri e diritti nelle piattaforme. Problemi di una prospettiva costituzionale*, in *Giur. it.*, 2/2024, p. 452 ss.; F. BASILE, *I delitti contro il sentimento religioso: tra incriminazione dell'opinione e tutela della libertà di manifestazione del pensiero*, in *MediaLaws*, 2/2018, p. 12 ss.; M. E. BUCALO, *La libertà di espressione nell'era dei "social network" fra "content moderation" e necessità di una regolazione flessibile*, in *Dir. pubbl. comp. eur.*, 1/2023, p. 143 ss.; V. CAVANNA, *Nuovi poteri, vecchi problemi. Il costituzionalismo alla prova del digitale*, in *Dir. pubbl. comp. eur.*, 1/2023, p. 223 ss.; L. CALIFANO, *La libertà di manifestazione del pensiero... in rete; nuove frontiere di esercizio di un diritto antico. "Fake news", "hate speech" e profili di responsabilità dei "social network"*, in *federalismi.it*, 26/2021, p. 1 ss.; C. COLAPIETRO, *Libera manifestazione del pensiero, fake news e privacy, oggi*, in *dirittifondamentali.it*, 2/2022, p. 422 ss.; M. TOMASI, *La Corte EDU torna sui caratteri del discorso politico online: una diluizione della libera manifestazione del pensiero?*, in *DPCE online*, 1/2024, p. 741 ss.; F. FERREIRA, *La questione della compatibilità dei sistemi automatizzati di filtraggio con la libertà di manifestazione del pensiero alla luce della sentenza CGUE, C-401/2019*, in *dirittifondamentali.it*, 3/2023, p. 383 ss.; C. PAGELLA, *Responsabilità penale di un aspirante deputato per i commenti islamofobi pubblicati da terzi sulla sua pagina Facebook: la Corte EDU [Corte europea dei diritti dell'uomo] sui limiti alla libertà di manifestazione del pensiero*, in *Riv. it. dir. e proc. pen.*, 3/2023, p. 1243 ss.

generazione di contenuti da parte degli utenti stessi. Sebbene sia difficile individuare una data precisa che segni l'inizio del fenomeno, si può affermare che i primi tentativi di creare piattaforme simili agli attuali *social network* risalgano alla fine degli anni '90. Le multinazionali che oggi dominano questo settore sono nate principalmente nel primo decennio del XXI secolo, consolidando la loro posizione nel decennio successivo[117].

Nonostante la diversità nel loro funzionamento, ciascuno di questi strumenti ha come elemento centrale la possibilità per gli utenti di condividere contenuti, che siano testi, immagini, audio o video. A ciò si aggiunge la capacità di costruire relazioni virtuali di vario genere, permettendo agli utenti di certificare rapporti di «amicizia» tra diversi profili, usare servizi di messaggistica, esprimere apprezzamenti. Questo modello interattivo ha trasformato il modo di comunicare e ha implicazioni dirette sulla tutela dell'identità e della *privacy*, oltre a influenzare in misura profonda la libertà di manifestazione del pensiero.

Sul punto la giurisprudenza europea ha chiarito che il diritto alla libera manifestazione del pensiero, garantito dall'art. 10 della Convenzione Europea dei Diritti dell'Uomo, non è assoluto, ma comporta anche doveri e responsabilità, specialmente quando si tratta di comunicazioni sui *social network*, che possono amplificare il messaggio diffuso, rendendo i contenuti virali e capaci di raggiungere un vasto pubblico in poco tempo[118].

---

[117] Sul punto si veda A. MANGANELLI, *Piattaforme digitali e "social network", fra pluralità degli ordinamenti, pluralismo informativo e potere di mercato*, in *Giur. cost.*, 2/2023, p. 883 ss.; S. GAZZELLA, *Consumatore digitale e "social network" nel diritto dell'Unione europea*, in *Rivista della Cooperazione Giuridica Internazionale*, 59/2018, p. 128 ss.; M. MONTI, *Regolazione, Internet e tecnica: le implicazioni di motori di ricerca e "social networks" sulla libertà di informazione*, in *federalismi.it*, 24/2017, p. 9 ss.; S. BRASCHI, *Il ruolo delle reti sociali nel contrasto ai reati commessi all'interno del web. Tendenze evolutive e prospettive di sviluppo*, in *MediaLaws*, 2/2021, p. 100 ss.; P. BONINI, *L'autoregolamentazione dei principali "Social Network". Una prima ricognizione delle regole sui contenuti politici*, in *federalismi.it*, 11/2020, p. 265 ss.; P. FALLETTA, *Controlli e responsabilità dei "social network" sui discorsi d'odio "online"*, in *MediaLaws*, 1/2020, p. 146 ss.; F. BALLAGUER CALLEJON, *"Social network", società tecnologiche e democrazia*, in *Nomos*, 3/2019, p. 4 ss.

[118] In particolare, l'art. 10 della CEDU afferma: «Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza considerazione di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, di cinema o di televisione. L'esercizio di queste libertà, poiché comporta

La Corte EDU ha più volte evidenziato che tale diffusione potenzialmente illimitata e immediata richiede una maggiore attenzione rispetto all'uso di mezzi tradizionali di comunicazione[119]. I social network permettono una trasmissione rapida di informazioni, ma anche di disinformazione, odio o diffamazione. Per questo motivo, gli utenti devono essere consapevoli dell'impatto che possono avere i contenuti diffusi in rete, e del conseguente aumento delle loro responsabilità. Questo equilibrio è fondamentale per garantire che la libertà di espressione non si trasformi in abuso, danneggiando il diritto e la reputazione altrui, o la sicurezza pubblica.

A parere della Corte, pertanto, è legittimo per gli Stati imporre delle restrizioni all'uso delle piattaforme *social*, se tali restrizioni servono a proteggere altri diritti fondamentali o interessi collettivi come l'ordine pubblico o la dignità delle persone. Queste limitazioni, tuttavia, devono essere proporzionate e necessarie in una società democratica.

Le piattaforme *social* hanno acquisito in pochi anni un ruolo centrale nel mercato dell'informazione, diventando strumenti potenti per la diffusione di notizie e opinioni. Un contenuto diffuso da un singolo utente su un *social media* può raggiungere milioni di persone in poche ore, grazie alla rapida condivisione tra utenti, trasformandosi così in un fenomeno virale. Nessun altro mezzo offre la stessa capacità di raggiungere un pubblico così vasto e diversificato, soprattutto tra le fasce di popolazione meno legate ai *media* tradizionali come la televisione o la stampa. Questo ha modificato profondamente il modo in cui le persone accedono e condividono informazioni, ampliando il potenziale di influenza dei contenuti *online*.

---

doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, per la sicurezza nazionale, per l'integrità territoriale o per la pubblica sicurezza, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, per la protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario».

[119] Un caso significativo è Delfi AS v. Estonia (2015, ric. n. 64569/09), in cui la CEDU ha stabilito che le piattaforme possono essere ritenute responsabili per i commenti di terzi se non vengono adottate misure adeguate a prevenire contenuti dannosi. Questo caso sottolinea la responsabilità dei *provider* di siti *web*, compresi i *social network*, nel moderare i contenuti, bilanciando la libertà di espressione con la protezione contro la diffamazione e il discorso dell'odio.

In questo contesto occorre analizzare il ruolo delle tecnologie basate sull'intelligenza artificiale nell'automazione delle attività sui *social media*, soprattutto considerando la mole di dati generata quotidianamente da milioni di utenti. Il ricorso all'intelligenza artificiale potrebbe essere finalizzato alla gestione di tali dati, per monitorare e filtrare i contenuti, ma un tale utilizzo può comportare rischi significativi.

Questi sistemi, infatti, potrebbero non essere in grado di comprendere appieno il contesto o le sfumature di un messaggio, portando a decisioni di moderazione inappropriate o ingiustificate, come la rimozione di contenuti che non violano effettivamente le regole della piattaforma o, viceversa, la mancata rimozione di contenuti offensivi o pericolosi. Questo processo di moderazione automatica può risultare eccessivamente rigido, sacrificando la complessità e la libertà del discorso umano per esigenze di efficienza e velocità.

Si pone quindi il problema di bilanciare la necessità di mantenere un ambiente sicuro e privo di abusi con la salvaguardia dei diritti fondamentali degli utenti. L'intelligenza artificiale, pur offrendo strumenti potenti per affrontare l'enorme mole di dati, rischia di limitare il diritto alla libera manifestazione del pensiero, introducendo nuovi dilemmi etici e giuridici.

2.2.1. I filtri sui social media e la responsabilità dei provider

Il filtro dei contenuti su una piattaforma di *social media* si fonda su due processi principali: il *matching*, che consiste nel cercare copie esatte o leggermente modificate di materiali già noti, particolarmente rilevante quando si cerca di bloccare la diffusione di immagini o video già considerati illeciti, e la *classification*, ovvero l'analisi di contenuti nuovi o sconosciuti per determinarne l'eventuale appartenenza a categorie vietate[120].

Le piattaforme utilizzano spesso la tecnica dell'*hashing* crittografico per eseguire il *matching*[121]. Questa tecnica assegna un valore numerico unico, detto *hash*, a un

[120] Le nozioni di *matching* e *classification* sono efficacemente spiegate da R. GORWA, R. BINNS, C. KATZENBACH, *Algorithmic content moderation: Technical and political challenges in the automation of platform governance*, in *Big Data & Society*, 7/2020, p. 4 ss.

[121] Per un approfondimento sull'*hashing* si veda S. LUCKS, *Design Principles for Iterated Hash Functions*, in *Cryptology ePrint Archive*, 253/2004; J. KELSEY, B. SCHNEIER, *Second Preimages on n-bit Hash*

contenuto specifico. Ogni copia dello stesso contenuto riceverà lo stesso *hash*, consentendo al sistema di identificarla e filtrarla rapidamente. L'efficacia dell'*hashing* risiede nel fatto che ogni *hash* è teoricamente unico per il contenuto associato, con una probabilità molto bassa di coincidenza tra *hash* di contenuti differenti.

Tuttavia, l'*hashing* crittografico presenta delle limitazioni, in particolare la sua estrema sensibilità anche a piccole modifiche nel contenuto, che possono impedire al sistema di riconoscerlo. Per affrontare questo problema, sono state sviluppate tecniche più avanzate che si concentrano sull'identificazione di contenuti simili piuttosto che identici. Questi sistemi rinunciano al concetto di unicità dell'*hash*, confrontando i contenuti in base a caratteristiche fondamentali e assegnando valori simili a materiali analoghi. In questo modo, i sistemi di moderazione riescono a riconoscere e bloccare contenuti che, pur non essendo esattamente identici, condividono elementi significativi con materiali già segnalati come illeciti. Queste tecnologie rappresentano un passo importante nell'efficacia della moderazione automatizzata dei contenuti, permettendo una maggiore flessibilità e accuratezza nel filtraggio[122].

Le reti sociali impiegano l'intelligenza artificiale anche nei sistemi di *computer vision*, che svolgono un ruolo centrale nella moderazione automatizzata dei contenuti

Functions for Much Less than 2^n Work, in *Cryptology ePrint Archive*, 304/2004; E. BIHAM O. DUNKELMAN, *A Framework for Iterative Hash Functions - HAIFA*, in *Cryptology ePrint Archive*, 278/2007; M. NANDI, P. SOURADYUTI, *Speeding Up The Widepipe: Secure and Fast Hashing*, in *Cryptology ePrint Archive*, 193/2010; A. JOUX, *Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions*, in M. Franklin (a cura di), *Advances in Cryptology – CRYPTO 2004. Lecture Notes in Computer Science*, vol 3152, Springer, Berlin, 2004; J. HOCH, A. SHAMIR, *On the Strength of the Concatenated Hash Combiner when All the Hash Functions Are Weak*, in L. Aceto, I. Damgård, L. A. Goldberg, M. M. Halldórsson, A. Ingólfsdóttir, I. Walukiewicz, (a cura di), *Automata, Languages and Programming. ICALP 2008. Lecture Notes in Computer Science*, Springer, Berlino, 2008.

[122] Un esempio di *hashing* è il *Global Internet Forum to Counter Terrorism (GIFCT),* una ONG progettata per impedire ai terroristi e agli estremisti violenti di sfruttare le piattaforme digitali. Fondato da *Meta* (*ex Facebook*), *Microsoft*, *YouTube* e *X* (*ex Twitter*) nel 2017, il *GIFCT* è stato istituito per promuovere la collaborazione tecnica tra queste imprese, far progredire la ricerca pertinente e condividere le conoscenze. Dal 2017, i membri del *GIFCT* si sono ampliati oltre le società fondatrici per includere oltre trenta diverse piattaforme impegnate in sforzi intersettoriali per contrastare la diffusione di contenuti *online* terroristi e violenti. Il *GIFCT* ha creato e aggiorna periodicamente un *database* di *hashing-sharing* che consente di identificare rapidamente e condividere segnali di attività terroristiche ed estremiste violente in modo sicuro, efficiente e rispettoso della *privacy* degli utenti. Per un approfondimento sul lavoro svolto dal *GIFCT* si veda il sito *web* www.gifct.org.

visivi, come immagini e video. Questi sistemi si basano su algoritmi avanzati capaci di analizzare, riconoscere e classificare i contenuti in base a criteri predefiniti, come il rilevamento di materiale inappropriato o illegale.

Le tecnologie descritte hanno oramai raggiunto un notevole grado di accuratezza, ma sono ancora soggette a margini di errore. Questo apre il campo a dibattiti accesi, poiché l'imprecisione residua può comportare la rimozione di contenuti in misura eccessiva o non necessaria, limitando così la libertà di espressione degli utenti. Il rischio è che, nell'intento di garantire la sicurezza e il rispetto delle regole della piattaforma, si possa giungere a una forma di moderazione eccessiva, in cui anche contenuti legittimi vengano censurati per errore.

Questo delicato equilibrio tra efficacia e precisione dei sistemi di moderazione automatizzati solleva importanti questioni etiche e giuridiche, soprattutto per quanto riguarda il diritto alla libera manifestazione del pensiero e la trasparenza nei processi decisionali automatizzati.

Alcuni ritengono, inoltre, che le tecnologie di moderazione possano produrre effetti negativi su gruppi sociali già marginalizzati, aggravando discriminazioni già esistenti. Qui si fa riferimento alla minor efficacia di questi sistemi nell'interpretare contenuti espressi in versioni non *standard* della lingua di riferimento, che può portare a risultati meno accurati e colpire determinati segmenti della popolazione. È stato dimostrato, ad esempio, che la capacità di molti sistemi di moderazione di analizzare il *African American Vernacular English* (AAVE)[123], una variante dell'inglese parlata principalmente da comunità afroamericane negli Stati Uniti, è estremamente limitata, generando una comprensione meno precisa per questi contenuti.

[123] L'*African American Vernacular English* (*AAVE*) è un dialetto con proprie regole grammaticali, lessicali e fonetiche, che lo differenziano dall'inglese *standard*. L'*AAVE* ha radici storiche nelle lingue e nei dialetti delle popolazioni africane portati in America durante il periodo della schiavitù, e si è evoluto nel tempo, incorporando elementi della cultura afroamericana e della lingua inglese. Si tratta di un sistema linguistico completo con regole ben definite. Tuttavia, è spesso stato stigmatizzato, in particolare perché associato a stereotipi razziali e discriminazione sociale. Per un approfondimento si veda G. BAILEY, *The relationship between African American Vernacular English and White Vernaculars in the American South: A sociocultural history and some phonological evidence*, in S. Lanehart (a cura di), *Sociocultural and Historical Contexts of African American English*, *Varieties of English Around the World*, John Benjamins Publishing Company, Amsterdam, p. 53 ss.

Un ulteriore problema sorge nei contesti in cui i sistemi automatizzati possono interpretare in modo errato contenuti che utilizzano termini comunemente associati all'*hate speech*. Spesso questi termini vengono riutilizzati da membri delle stesse comunità bersaglio di tali insulti, nel contesto di una riappropriazione linguistica all'interno di movimenti sociali o di attivismo, come quelli del movimento LGBTQI+. In queste situazioni, le tecnologie di moderazione possono erroneamente censurare contenuti che, anziché promuovere odio, sono espressione di resistenza o critica. Di conseguenza, l'effetto finale può essere l'oscuramento di messaggi che, invece di diffondere discriminazione, cercano di contrastarla, come è già accaduto in numerosi casi.

Per questi motivi le piattaforme *social* hanno adottato diverse strategie per integrare l'intervento umano nel processo di moderazione dei contenuti. Un esempio significativo è la creazione dell'*Oversight Board* di *Meta*, un organo indipendente composto da esperti esterni, incaricato di supervisionare le decisioni più controverse[124]. Tuttavia, nonostante l'introduzione di controlli umani, la massiccia quantità di contenuti che vengono generati e condivisi quotidianamente sulle piattaforme rende inevitabile il ricorso a sistemi automatizzati, alimentati dall'intelligenza artificiale.

La velocità con cui i contenuti vengono pubblicati impone infatti che la maggior parte del lavoro di moderazione venga svolto da algoritmi, poiché non è pensabile che gli esseri umani possano gestirlo interamente da soli. L'intervento umano avviene principalmente in un secondo momento, spesso come revisione delle decisioni già prese dai sistemi automatizzati, o in risposta a segnalazioni degli utenti quando un contenuto non viene filtrato.

---

[124] Si veda il sito *web* www.oversightboard.com. Sul punto si veda anche l'intervento di Ginevra Cerrina Feroni, Vicepresidente del Garante per la protezione dei dati personali, dal titolo *L'Oversight Board di Facebook: il controllo dei contenuti tra procedure private e norme pubbliche*, pubblicato in data 16 febbraio 2021 sul sito *web* del Garante della *privacy*. Per un approfondimento: C. ASPRELLA, *L'"Oversight Board", la "Corte d'appello" di Facebook, e i nuovi "confini" della giurisdizione*, in *Judicium*, 3/2023, p. 241 ss.; A. GOLIA, *Pluralità degli ordinamenti giuridici e costituzionalizzazione degli spazi digitali. Osservazioni sulla giurisprudenza dell'"Oversight Board"*, in *Quad. cost.*, 3/2023, p. 595 ss.; A. BURATTI, *Framing the Facebook Oversight Board: Rough Justice in the Wild Web?*, in *MediaLaws*, 2/2022, p. 31 ss.; A. IANNOTTI DELLA VALLE, *La giurisdizione privata nel mondo digitale al tempo della crisi della sovranità: il "modello" dell'"Oversight Board" di Facebook*, in *federalismi.it*, 26/2021, p. 144 ss.

Una delle maggiori criticità di questi sistemi è legata al fatto che la moderazione dei contenuti è oggi affidata quasi interamente a società private, che finiscono per avere una forte influenza sul flusso delle informazioni, senza le stesse garanzie procedurali e trasparenza che caratterizzavano i media tradizionali[125].

Questi cambiamenti sollevano preoccupazioni riguardo al potere crescente delle piattaforme *social* nel determinare quali contenuti debbano essere visibili o oscurati, e al rischio che tale controllo possa compromettere il libero dibattito pubblico senza le adeguate tutele democratiche.

I sistemi di moderazione finora descritti sono principalmente usati dagli *Internet Service Provider (ISP)* per garantire una piacevole fruizione dei loro *social network*, non anche per evitare situazioni di responsabilità, anche penale, per gli illeciti commessi dagli utenti. La responsabilità dei *provider*, infatti, è già a priori limitata dal principio della c.d. *liability exemption*, sancito dagli articoli da 12-15 della Direttiva UE 2000/31/CE, nota anche come direttiva *e-commerce*. Ai sensi di queste norme le piattaforme *online* non sono responsabili in maniera generalizzata per i contenuti pubblicati dagli utenti. Questo significa che la loro posizione non è equiparabile a quella di un editore, che invece ha una responsabilità diretta sui contenuti che pubblica sul suo giornale[126].

---

[125] Per un approfondimento sul tema della privatizzazione dei controlli si veda M. MONTI, *Privatizzazione della censura e internet platforms: la libertà di espressione e i nuovi censori dell'agorà digitale*, in *Inf. dir.*, 1/2019, p. 35 ss. Più in generale si veda anche U. RUFFOLO, *Piattaforme e "content moderation" negoziale*, in *Giur. it.*, 2/2024, p. 442 ss.; M. E. BUCALO, *La libertà di espressione nell'era dei "social network" fra "content moderation" e necessità di una regolazione flessibile*, cit.

[126] Sul ruolo del *provider* si veda G. FIORINELLI, *L'attuale ruolo del provider nella società digitale: modelli di responsabilità penale*, in *Leg. pen.*, 4/2022, p. 258 ss.; A. INGRASSIA, *Responsabilità penale degli "internet service provider": attualità e prospettive*, in *Dir. pen. e proc.*, 12/2017, p. 1621 ss.; O. POLLICINO, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in *Percorsi costituzionali*, 1/2014, p. 45 ss.; R. BARTOLI, *Brevi considerazioni sulla responsabilità penale dell'"Internet Service Provider"*, in *Dir. pen. e proc*, 5/2013, p. 600 ss.; A. P. SEMINARA, *"Marketing" d'influenza e pubblicità non trasparente: la responsabilità dell'inserzionista, degli "influencer" e dell'"internet service provider"*, in *Persona e Mercato*, 3/2023, p. 548 ss.; G. CASSANO, B. TASSONE, *Responsabilità dell'Internet "service provider", diritti di proprietà intellettuale e danni punitivi*, in *Foro it.*, 9/2022, p. 2840 ss.; M. R. ALLEGRI, *Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, in *Inf. dir.*, 2/2021, p. 7 ss.; G. D'ALFONSO, *Verso una maggiore responsabilizzazione dell' "hosting provider" tra interpretazione evolutiva della disciplina vigente, innovazioni legislative e prospettive "de jure condendo"*, in *federalismi.it*, 2/2020, p. 108 ss.; E. GARZONIO, *Responsabilità degli ISP ["Internet Service Provider" - Fornitore di servizi Internet] rispetto al trattamento*

Tuttavia, la direttiva introduce un importante obbligo per le piattaforme: una volta che vengono a conoscenza, in qualsiasi modo, dell'illiceità di un contenuto specifico, sono tenute a rimuoverlo rapidamente. Se non adempiono a questo obbligo e rimangono inerti, possono essere considerate responsabili per i contenuti in questione. Questo principio mira a bilanciare la libertà di espressione e l'autonomia delle piattaforme con la necessità di tutelare i diritti degli individui e prevenire abusi.

L'esenzione di responsabilità per gli ISP nacque principalmente per evitare che questi ultimi optassero per una moderazione eccessiva dei contenuti, bloccando preventivamente una vasta gamma di espressioni lecite per evitare eventuali sanzioni. Si pensava infatti che la paura di conseguenze legali potesse favorire forme di autocensura non solo da parte delle piattaforme ma anche degli utenti stessi, preoccupati che le loro opinioni o contenuti potessero essere rimossi. La *liability exemption* è stata quindi introdotta per proteggere la libertà di espressione *online* e per evitare che le piattaforme si trasformassero in arbitri incontestabili della moderazione dei contenuti[127].

Il Regolamento sui servizi digitali (*Digital Services Act, DSA*), entrato in vigore a novembre 2022, introduce nuove disposizioni riguardanti la responsabilità degli *Internet Service Provider*[128]. Il DSA mantiene alcune basi della direttiva *e-commerce* del 2000, ma apporta aggiornamenti significativi per rispondere all'evoluzione del mondo digitale e al crescente ruolo dei social network.

---

automatizzato dei dati personali con finalità di comunicazione politica: applicabilità del GDPR alle piattaforme "social", in *MediaLaws*, 2/2019, p. 190 ss.; G. MICELI, *Profili evolutivi della responsabilità in rete: il ruolo degli "Internet Service Provider" tra prevenzione e repressione*, in *MediaLaws*, 1/2017, p. 10 ss.

[127] Sul punto si veda il documento dal titolo *Providers Liability: From the eCommerce Directive to the future*, pubblicato dalla Direzione generale delle Politiche interne dell'Unione (IPOL) nel 2017, consultabile sul sito *web* del Parlamento europeo.

[128] V. Regolamento UE 2022/2065. Il *Digital Services Act (DSA)* è un regolamento dell'Unione europea per modernizzare e ampliare la Direttiva sul commercio elettronico 2000/31/CE in relazione ai contenuti illegali, alla pubblicità trasparente e alla disinformazione. Per un approfondimento v. S. BRASCHI, *Il nuovo Regolamento sui servizi digitali: quale futuro per la responsabilità degli "Internet Service Provider"?*, in *Dir. pen. e proc.*, 3/2023, p. 367 ss.; A. PALUMBO, J. PIEMONTE, *Delega di funzioni regolamentari e lotta ai rischi sistemici causati dalla disinformazione nel "Digital Services Act": quali rischi per la libertà di espressione?*, in *MediaLaws*, 3/2023, p. 114 ss.; S. TOMMASI, *"Digital services act" e "artificial intelligence act": tentativi di futuro da armonizzare*, in *Persona e Mercato*, 2/2023, p. 279 ss.

Similmente alla direttiva *e-commerce*, il DSA esclude che i fornitori di servizi *internet* abbiano una responsabilità generale per i contenuti trasmessi dai loro utenti. Questo significa che gli ISP non sono obbligati a monitorare attivamente tutti i contenuti che circolano sulle loro piattaforme o a cercare attività illecite. Sono però tenuti a rimuovere o disabilitare l'accesso ai contenuti illeciti non appena ne vengono a conoscenza, attraverso una notifica da parte di autorità o privati.

Sul punto anche la Cassazione ha sostenuto che i *provider* potessero essere ritenuti responsabili per l'omesso impedimento della protrazione del reato altrui[129]. Secondo i giudici la responsabilità penale del gestore del sito non deriva semplicemente dal suo ruolo apicale (cioè dall'essere il titolare o amministratore del sito stesso): se così fosse, si creerebbe una forma di responsabilità cosiddetta da posizione, che produrrebbe fondati dubbi di incostituzionalità. Appare, invece, più sostenibile che la responsabilità del gestore sia legata alla sua condotta omissiva: egli risponde penalmente per non aver rimosso i contenuti offensivi una volta venuto a conoscenza del loro carattere denigratorio. In questo caso, l'obbligo del gestore sorge nel momento in cui è informato del contenuto illecito. La sua inazione dopo aver acquisito consapevolezza dell'illegittimità del materiale pubblicato, infatti, costituisce la base della responsabilità, poiché omettere la rimozione si traduce in una forma di complicità indiretta nel mantenimento della condotta illecita.

Il DSA introduce obblighi più severi per le piattaforme *online* di grandi dimensioni[130], che devono adottare misure per limitare i rischi sistemici, inclusa la diffusione di contenuti illegali o dannosi. Questi fornitori sono obbligati a effettuare valutazioni periodiche dei rischi connessi al loro servizio, in particolare per quanto riguarda i contenuti illeciti e l'uso improprio dei loro servizi.

Il Regolamento considera l'apporto fondamentale dei sistemi avanzati di intelligenza artificiale per gestire l'enorme volume di contenuti che circolano sulle piattaforme *online*. Riconosce l'efficacia e l'efficienza dell'IA nell'identificare e moderare contenuti potenzialmente dannosi o illegali, ma evidenzia anche i rischi connessi a un

[129] Così Cass., sez. V, 14 luglio 2016, n. 54946; Cass., sez. V, 8 novembre 2018, n. 12546 in *DeJure.it*.

[130] Il regolamento a tal proposito parla di *Very Large Online Platforms – VLOPs*.

uso esclusivo o eccessivo di sistemi automatizzati. Pertanto, adotta un approccio bilanciato che punta a regolare l'uso di questi sistemi in modo da garantire una maggiore trasparenza e un controllo più accurato delle loro attività, che dovranno sempre essere affiancate e supervisionate da soggetti umani. Questo permetterà di correggere gli eventuali errori dei sistemi automatizzati, specialmente nei casi in cui il contesto o l'intento dei contenuti pubblicati siano ambigui o richiedano una valutazione più approfondita[131].

Tuttavia, il ruolo dei *provider* potrebbe assumere un'importanza sempre maggiore nel contrasto agli illeciti *online*, soprattutto in un contesto normativo che sempre più li riconosce come attori chiave nella rimozione e gestione dei contenuti illegali in rete. Un esempio significativo di questo approccio è rappresentato dalla Legge 71/2017[132] sul cyberbullismo, che introduce un quadro normativo su misura per affrontare questo fenomeno specifico. Tale norma ha previsto strumenti di tutela e prevenzione che pongono al centro il *provider*, rendendolo parte attiva nella rimozione dei contenuti lesivi su richiesta della vittima che, attraverso una procedura diretta, può richiederne la cancellazione al *provider*, senza dover passare esclusivamente per le autorità.

---

[131] A tal proposito, il Considerando 25 del Regolamento afferma: «Al fine di garantire la certezza del diritto e non scoraggiare le attività volte a individuare, identificare e contrastare i contenuti illegali che i prestatori di tutte le categorie di servizi intermediari intraprendano su base volontaria, è opportuno chiarire che il semplice fatto che i prestatori intraprendano tali attività non comporta il venir meno delle esenzioni dalla responsabilità stabilite nel presente regolamento, purché tali attività siano svolte in buona fede e in modo diligente. La condizione di agire in buona fede e in modo diligente dovrebbe includere l'agire in modo obiettivo, non discriminatorio e proporzionato, tenendo debitamente conto dei diritti e degli interessi legittimi di tutte le parti coinvolte e fornendo le necessarie garanzie contro la rimozione ingiustificata di contenuti legali, conformemente agli obiettivi e alle prescrizioni del presente regolamento. A tal fine, i prestatori interessati dovrebbero, ad esempio, adottare misure ragionevoli per garantire che, in caso di utilizzo di strumenti automatizzati per svolgere tali attività, l'apposita tecnologia sia sufficientemente affidabile da limitare al massimo il tasso di errore».

[132] Legge 29 maggio 2017, n. 71, Disposizioni a tutela dei minori per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo. Per un approfondimento si veda M. LAMANUZZI, *Il cyberbullismo. Prospettive criminologiche e giuridico-penali a partire dalla l. 71/2017*, in *JusOnline*, 6/2020, p. 166 ss.; M. MANTOVANI, *Profili penali del "cyberbullismo": la l. 71 del 2017*, in *Ind. pen.*, 2/2018, p. 475 ss.; M. A. SENOR, *Un primo commento alla legge sul cyberbullismo*, in *MediaLaws*, 1/2017, p. 23 ss.; C. PANICALI, *Il "cyberbullismo": i nuovi strumenti (extrapenali) predisposti dalla legge n. 71/2017 e la tutela penale*, in *Resp. civ. prev.*, 6/2017, p. 2081 ss.

In particolare, l'art. 2 della legge prevede la possibilità per chiunque (inclusi i minori o i loro genitori) di inviare un'istanza ai gestori di siti *web* o *social media* per richiedere l'oscuramento, la rimozione o il blocco di contenuti illeciti diffusi in rete[133]. Il coinvolgimento attivo dei *provider* in queste procedure è centrale per garantire l'effettività di tali misure, poiché essi possiedono la capacità tecnica per intervenire rapidamente sulla diffusione dei contenuti.

L'efficacia di tale approccio si rivela cruciale soprattutto a fronte della natura pervasiva, de-territorializzata e anonima della rete, che rende difficile intervenire sui contenuti illeciti senza la collaborazione di chi gestisce le piattaforme digitali[134].

Questa norma rappresenta un passo avanti rispetto agli approcci tradizionali che si limitano a delegare la gestione dei contenuti illeciti alla auto-organizzazione dei fornitori di servizi digitali. Al contrario, con la Legge 71/2017, viene riconosciuta la responsabilità concreta e diretta dei *provider*, contribuendo a rendere il contrasto al cyberbullismo più rapido ed efficace.

La validità di questo intervento legislativo risiede nella sua capacità di affrontare in modo mirato il problema, evitando soluzioni generalizzate e valorizzando il ruolo attivo dei fornitori di servizi. Questo modello potrebbe servire come riferimento per altre forme di gestione di contenuti illeciti nella società dell'informazione,

---

[133] Più precisamente l'art. 2, comma 1, afferma che: «Ciascun minore ultraquattordicenne, nonché ciascun genitore o soggetto esercente la responsabilità del minore che abbia subito taluno degli atti di cui all'articolo 1, comma 2, della presente legge, può inoltrare al titolare del trattamento o al gestore del sito *internet* o del *social media* un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, diffuso nella rete *internet*, previa conservazione dei dati originali, anche qualora le condotte di cui all'articolo 1, comma 2, della presente legge, da identificare espressamente tramite relativo *URL* (*Uniform resource locator*), non integrino le fattispecie previste dall'articolo 167 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, ovvero da altre norme incriminatrici».

[134] Per un approfondimento sul tema del cyberbullismo si veda C. COLOMBO, *Il cyberbullismo. Una particolare tipologia di devianza*, in *Ind. pen.*, 3/2019, p. 441 ss.; A. STRINGI, G. DIOGUARDI, V. CARETTI, *"Problematic internet use" (piu) e cyberbullismo in adolescenza. Vittimizzazione, condotte a rischio e percezione del fenomeno tra pari: una ricerca*, in *Rass. it. crim.*, 4/2022, p. 290 ss.; G. FIORINELLI, *L'attuale ruolo del provider nella società digitale: modelli di responsabilità penale*, in *Leg. pen.*, 27 dicembre 2022; M. LAMANUZZI, *Il cyberbullismo. Prospettive criminologiche e giuridico-penali a partire dalla l. 71/2017*, cit.; M. MANTOVANI, *Profili penali del "cyberbullismo": la l. 71 del 2017*, cit.; C. PANICALI, *Il "cyberbullismo": i nuovi strumenti (extrapenali) predisposti dalla legge n. 71/2017 e la tutela penale*, cit.

rappresentando un passo avanti nella costruzione di un quadro normativo più maturo e consapevole in materia di diritto penale online.

2.2.2. Fake news e Hate speech

Dalla precedente analisi sono emerse la necessità e l'urgenza di garantire che la libertà di pensiero e di parola, diritti fondamentali sanciti dalle costituzioni democratiche e dai trattati internazionali, siano pienamente riconosciuti e tutelati anche sui *social network*. L'insorgere, inoltre, di fenomeni di disinformazione sistematica e contenuti dannosi ha evidenziato ulteriormente il bisogno di strumenti regolatori, che tutelino gli utenti delle piattaforme. Il tema delle *fake news* e dell'*hate speech* pone un delicato dilemma tra la difesa della libertà di espressione e la necessità di tutelare la società dai danni che possono essere provocati dalla disinformazione e dai discorsi d'odio.

Quanto alle *fake news*, si tratta di informazioni false, ingannevoli o distorte, presentate come notizie verificate e diffusesi in modo intenzionale o non intenzionale attraverso diversi canali, soprattutto i *social media*[135]. Questi contenuti sono spesso progettati per manipolare l'opinione pubblica o promuovere disinformazione per scopi economici, politici o ideologici.

Il termine *hate speech* si riferisce a qualsiasi forma di espressione che inciti all'odio, alla violenza, o alla discriminazione contro individui o gruppi basata su aspetti come

[135] Si parla di *misinformation* quando la diffusione di informazioni false non è intenzionale, e di *disinformation* quando vi è un intento consapevole di ingannare. Per un approfondimento sul tema delle *fake news* v. A. VISCONTI, *Alcune considerazioni criminologiche e politico-criminali sulle c.d. "Fake News"*, in *Jus*, 1/2020, p. 43 ss.; C. MELZI D'ERIL, *"Fake news" e responsabilità: paradigmi classici e tendenze incriminatrici*, in *MediaLaws*, 1/2017, p. 6 ss.; T. GUERINI, *Fake news e diritto penale*, Giappichelli, Torino, 2020; B. GRAZZINI, *"Fake news" e disinformazione*, in *Giur. it.*, 2/2024, p. 491 ss.; G. MARCHETTI, *Le "fake news" e il ruolo degli algoritmi*, in *MediaLaws*, 1/2020, p. 29 ss.; M. BASSINI, G. E. VIGEVANI, *Primi appunti su "fake news" e dintorni*, in *MediaLaws*, 1/2017, p. 11 ss.; F. DONATI, *"Fake news" e libertà di informazione*, in *MediaLaws*, 2/2018, p. 36 ss.; S. FLAMINIO, *Lotta alle "fake news": dallo stato dell'arte a una prospettiva di regolamentazione per il vivere digitale a margine del "Digital Services Act"*, in *Inf. dir.*, 2/2022, p. 75 ss.; C. VALDITARA, *"Private" e "public enforcement" nel contrasto alle "fake news"*, in *Dir. inform.*, 3/2021, p. 493 ss.; A. SCIORTINO, *"Fake news" e "post"-verità nella società dell'algoritmo*, in *dirittifondamentali.it*, 2/2021, p. 422 ss.

razza, religione, origine etnica, orientamento sessuale, genere, disabilità o altre caratteristiche identitarie[136]. La definizione di *hate speech* può variare a seconda delle giurisdizioni legali e del contesto culturale. In molti Paesi, specialmente in Europa, esistono leggi che vietano e puniscono l'incitamento all'odio, mentre in altri contesti, come negli Stati Uniti, la libertà di espressione garantita dal primo emendamento può offrire maggiore protezione, con limitazioni più ristrette all'azione legale contro l'*hate speech*[137].

Il dibattito su *fake news* e *hate speech* ci riporta al tema affrontato nel paragrafo precedente, ovvero alla possibilità di attribuire responsabilità ai titolari dei siti *web*, compresi i gestori delle piattaforme *social*, per i contenuti generati dagli utenti. Il nodo cruciale riguarda se e in quale misura sia possibile imputare loro un obbligo di vigilanza su ciò che gli utenti pubblicano tramite i propri profili personali e, nel caso, quali sarebbero le fattispecie cui fare riferimento.

Non è agevole trovare un giusto bilanciamento tra la lotta alle *fake news* e all'*hate speech* e la tutela della libertà di espressione. La rilevanza costituzionale di quest'ultima impone di evitare qualunque sua impropria limitazione. Una regolamentazione troppo restrittiva potrebbe disincentivare gli utenti dall'esprimere le proprie opinioni per paura di sanzioni o rimozioni ingiustificate dei contenuti. In quest'ottica, diventa cruciale trovare un equilibrio che permetta di contrastare la diffusione di contenuti

---

136 La Convenzione del Consiglio d'Europa del 1997 definisce l'*hate speech* come: «qualsiasi espressione che diffonda, inciti, promuova o giustifichi l'odio razziale, la xenofobia, l'antisemitismo o altre forme di odio basato sull'intolleranza». Per un approfondimento v. I. ANRÒ, *"Online hate speech": la prospettiva dell'Unione europea tra regolamentazione della condotta dei prestatori di servizi intermediari e ricorso al diritto penale*, in *Osservatorio sulle fonti*, 1/2023, p. 13 ss.; M. NINO, *The freedom of expression and hate speech in cyberspace*, in *Comun. intern.*, 1/2023, p. 33 ss.; P. FALLETTA, *Controlli e responsabilità dei "social network" sui discorsi d'odio "online"*, in *MediaLaws*, 1/2020, p. 146 ss.; M. LUGATO, *Il «discorso di odio»: le coordinate giuridiche del ragionamento internazionalistico*, in *Riv. dir. int.*, 4/2022, p. 959 ss.; P. DUNN, *Moderazione automatizzata e discriminazione algoritmica: il caso dell'"hate speech"*, in *Inf. dir.*, 1/2022 p. 133 ss.; I. GASPARINI, *L'odio ai tempi della rete: le politiche europee di contrasto all'"online hate speech",* in *Jus*, 3/2017, p. 505 ss.; A. MADEO, *Diffamazione e "hate speech": quando il giudizio non è meramente critico ma discriminatorio in ragione dell'orientamento sessuale*, in *GenIUS*, 2/2022, p. 205 ss.

137 Sul punto v. F. RATTO TRABUCCO, *L'"hate speech" nell'esperienza dei "social networks" e della giurisprudenza americana*, in *Rivista della Cooperazione Giuridica Internazionale*, 3/2017, p. 85 ss.

dannosi senza soffocare il dibattito pubblico, proteggendo al contempo il diritto dei cittadini di accedere a informazioni affidabili e verificate.

Quando le *fake news* sono accompagnate da un dolo specifico, consistente nella volontà, scientemente perseguita, di diffondere notizie ingannevoli, bisogna chiedersi se sia possibile una qualche forma di tutela (e repressione) penale in tal senso[138].

A parere di chi scrive (ma soprattutto di autorevole dottrina) non si potrebbe prendere in considerazione la punibilità di un'ipotesi colposa. Questo comporterebbe un'estensione eccessiva della sfera del penalmente rilevante, soprattutto considerando che il soggetto agente nella maggior parte dei casi non possiede quella professionalità necessaria a generare una posizione di garanzia atta a fondare un obbligo di diligenza[139].

La diffusione di notizie false e i discorsi d'odio non sono fenomeni recenti. Storicamente, la disinformazione e la propaganda hanno sempre avuto un ruolo nel manipolare l'opinione pubblica e influenzare decisioni politiche. Ciò che rende il fenomeno oggi particolarmente preoccupante è il fatto che, con l'avvento dei *social media* e delle tecnologie digitali, la portata dei contenuti viene amplificata, raggiungendo milioni di utenti in tempi molto brevi.

Nel nostro ordinamento spesso il legislatore ha voluto punire quelle manifestazioni del pensiero che fossero da sole idonee a cagionare un'offesa ad altri, attraverso la categoria dei c.d. reati d'opinione[140]. Infatti, esistono già norme che indirettamente

---

138 Si veda l'analisi di L. CALIFANO, *La libertà di manifestazione del pensiero... in rete; nuove frontiere di esercizio di un diritto antico. "Fake news", "hate speech" e profili di responsabilità dei "social network"*, cit., p. 10. Per un approfondimento sulla possibilità di introdurre nuove fattispecie delittuose *ad hoc* si veda anche P. TRONCONE, *Nuove possibili scelte di politica criminale per il reato di pubblicazione o diffusione di notizie false ("fake news"), esagerate o tendenziose*, in *Ind. pen.*, 2/2021, p. 614 ss.

139 Di questo parere sono A. CAVALIERE, *La discussione intorno alla punibilità del negazionismo,* cit., p. 999 ss.; F. DE SIMONE *'Fake news', 'post truth', 'hate speech': nuovi fenomeni sociali alla prova del diritto penale*, in *Arch. pen.*, 1/2018, p. 4 ss.

140 L'espressione si riferisce a una tipologia di reati che comprende molti delitti contro la personalità dello Stato, in particolare quelli legati a propaganda, apologia sovversiva e vilipendio della Repubblica e delle istituzioni costituzionali. Il termine deriva dal fatto che tali reati consistono nella manifestazione di opinioni che attaccano la sfera morale altrui o che non rispettano i parametri costituzionali relativi alla libertà di pensiero. La materia è stata modificata dalla legge n. 85 del 2006, la quale ha adattato queste fattispecie alle esigenze giuridiche contemporanee, poiché molte norme presenti nel titolo I del Libro II del codice penale riflettevano concezioni sociopolitiche ormai obsolete

regolamentano alcune ipotesi di *hate speech*, come nel caso dei reati di diffamazione (art. 595 c.p.), apologia di reato (art. 414 c.p.), propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica o religiosa (art. 604-bis c.p.).

Nei procedimenti riguardanti delitti di opinione, è assai frequente il richiamo all'articolo 51 del codice penale, che disciplina la causa di giustificazione dell'esercizio di un diritto, collegando la condotta al diritto costituzionale alla libera manifestazione del pensiero tutelato dall'art. 21 della Costituzione. In questi casi, si sostiene che la condotta, seppur contestata come offensiva o diffamatoria, dovrebbe essere considerata legittima in quanto rientrante nell'esercizio del diritto di espressione.

Tuttavia, tale difesa non sempre viene accolta dalla giurisprudenza. La Corte di Cassazione, in diverse pronunce, ha chiarito che l'art. 51 c.p. può essere invocato come causa di esclusione della punibilità solo quando l'esercizio del diritto rispetta i limiti della continenza formale e sostanziale. In particolare, la critica deve essere espressa in modo corretto, senza ledere indebitamente la dignità altrui, altrimenti si configura il reato di diffamazione[141].

---

e incompatibili con i valori sanciti dalla Costituzione. In particolare, la nuova disciplina ha eliminato alcuni reati contro la personalità dello Stato, come la propaganda sovversiva o antinazionale (art. 272 c.p.) e i delitti contro i culti riconosciuti dallo Stato (art. 406 c.p.). Al contempo, altre ipotesi di reato, riguardanti l'espressione di opinioni politiche, sono state riformulate, come nel caso degli articoli 241 (attentato contro l'integrità dello Stato), 283 (attentato contro la costituzione) e 289 (attentato contro organi costituzionali). Restano invece invariati i reati di apologia di delitti (art. 414 c.p.) e di istigazione a disobbedire alle leggi (art. 415 c.p.). Per un approfondimento si veda, *ex multis*, A. SPENA, *Libertà di espressione e reati di opinione*, in *Riv. it. dir. e proc. pen.*, 2/2007, p. 689 ss.; C. FIORE, *Libertà d'espressione politica e reati d'opinione*, in *Politica del diritto*, 3/1970, p. 486 ss.; M. PELISSERO, *Osservazioni critiche sulla legge in tema di reati di opinione: occasioni mancate e incoerenze sistematiche*, in *Dir. pen. e proc.*, 8/2006, p. 960 ss.; L. STORTONI, *L'incostituzionalità dei reati di opinione: una questione liquidata?*, in *Foro it.*, 4/1979, p. 899 ss.; L. ALESIANI, *I reati di opinione: una rilettura in chiave costituzionale*, Giuffrè, Milano, 2006; R. PASCARELLI, *La riforma dei reati di opinione: un commento alla nuova disciplina*, in *Ind. pen.*, 2/2006, p. 697 ss.; A. RIDOLFI, *I reati di opinione tra Stato liberale e fascismo*, in *Historia et Ius*, 8/2015, p. 14 ss.

[141] Una delle pronunce più rilevanti in questo ambito è la sentenza n. 37370 del 2021, in cui la Corte ha stabilito che il diritto di critica non può essere esercitato in modo offensivo o ingiurioso. La sentenza ribadisce che il diritto alla libertà di espressione trova un limite quando va a ledere diritti fondamentali altrui, come il diritto alla reputazione, e che il richiamo all'art. 51 c.p. è possibile solo se l'esercizio del diritto si manifesta in modo corretto e rispettoso delle regole del vivere civile. Altre pronunce importanti includono la sentenza n. 13562 del 2000 e la sentenza n. 5192 del 1985, in cui la Cassazione ha specificato che la critica è legittima solo se espressa nei limiti della continenza, intesa come correttezza formale e sostanziale, e non deve mai sconfinare in attacchi personali o gratuiti.

Quindi, mentre il diritto alla libertà di espressione è fondamentale, non giustifica automaticamente condotte che sfociano in reati, soprattutto se tali espressioni superano i limiti del lecito, trasformandosi in attacchi personali o diffamazioni. Atti come l'insulto fine a se stesso, che non rappresentano una reale manifestazione di pensiero o un'opinione strutturata, non rientrano nella sfera protetta dalla libertà di espressione. L'insulto verbale o il vilipendio che non comunica informazioni, valutazioni, o stati d'animo non gode della tutela dell'art. 21.

La giurisprudenza della Corte Europea dei Diritti dell'Uomo, dal canto suo, ha scelto di interpretare l'articolo 10 della Convenzione in modo estensivo, riconducendovi anche espressioni di disapprovazione emotiva, sarcasmo, scetticismo o frasi scurrili. Pertanto, le esagerazioni e le forme volgari possono essere protette non tanto per il loro contenuto specifico, ma per la funzione stilistica che svolgono all'interno della comunicazione[142].

Tuttavia, in molti hanno ritenuto che le caratteristiche del contesto sociale attuale e la portata del fenomeno delle *fake news* e dei discorsi d'odio *online* necessitino di normative ad hoc.

Per tale ragione nel 2017 venne depositato il Disegno di legge Gambaro, n. 2688, contenente «Disposizioni per prevenire la manipolazione dell'informazione *online*, garantire la trasparenza sul *web* e incentivare l'alfabetizzazione mediatica»[143]. Il disegno si proponeva di regolare la responsabilità e gli obblighi di sorveglianza dei gestori di siti *web* o piattaforme digitali[144], ma avanzava anche ipotesi di criminalizzazione specifiche attraverso l'inserimento nel codice penale di tre nuove fattispecie criminose.

La prima ipotesi di reato è configurata come una contravvenzione, introdotta con l'art. 656 *bis*, intitolato «Pubblicazione o diffusione di notizie false, esagerate o

---

[142] Si può far riferimento alle sentenze della Corte EDU *Handyside* c. Regno Unito, ric. n. 5493/72 e *Savva Terentyev* c. Russia, ric. n. 10692/09.

[143] Si precisa sin d'ora che il disegno di legge non è mai stato né discusso né approvato. Il disegno di legge viene analizzato da F. DE SIMONE *'Fake news', 'post truth', 'hate speech': nuovi fenomeni sociali alla prova del diritto penale*, cit., p. 9 ss. Si veda inoltre M. LAMANUZZI, *La disinformazione ai tempi dei social media: una nuova sfida per il diritto penale?*, in *Arch. Pen.*, 1/2020, in particolare p. 12 ss.

[144] Viene loro imposto un duplice obbligo di monitoraggio dei contenuti diffusi e di rimozione nel caso di pubblicazione di notizie non attendibili. L'omessa rimozione configura una nuova ipotesi di contravvenzione, sanzionata con la stessa ammenda prevista dall'art. 656 *bis* c.p.

tendenziose, atte a turbare l'ordine pubblico, attraverso piattaforme informatiche»[145]. Erano previsti poi gli artt. 265 *bis* e *ter* c.p., relativi alla «Diffusione di notizie false che possono destare pubblico allarme o fuorviare settori dell'opinione pubblica» e alla «Diffusione di campagne d'odio volte a minare il processo democratico»[146].

Ci furono anche altre proposte sul tema, come il Disegno di legge Zanda-Zeppelin, incentrato sull'introduzione di una forma di responsabilità per i gestori delle piattaforme social, e il Disegno di legge De Girolamo, volto a colpire l'anonimato e a riconoscere il diritto all'oblio.

Nessuna di queste proposte, tuttavia, ha portato all'emanazione di una legge.

Sarebbe comunque opportuno riflettere sull'utilità di introdurre una nuova ipotesi di illecito, o piuttosto valutare la modifica di fattispecie di reato già esistenti. Si potrebbe intervenire sull'art. 658 del codice penale[147], includendo esplicitamente i casi

---

[145] Si tratta di un reato comune con una forma specifica, in quanto le condotte incriminate di pubblicazione o diffusione devono avvenire necessariamente tramite piattaforme informatiche destinate all'informazione pubblica. Il testo proposto del 656 *bis* è il seguente: «1. Chiunque pubblica o diffonde, attraverso piattaforme informatiche destinate alla pubblicazione o diffusione di informazione presso il pubblico, con mezzi prevalentemente elettronici o comunque telematici, notizie false, esagerate o tendenziose che riguardino dati o fatti manifestamente infondati o falsi, è punito, se il fatto non costituisce un più grave reato, con l'ammenda fino a euro 5.000. 2. Nel caso in cui le fattispecie previste dall'articolo 656-*bis* del codice penale, introdotto dal comma 1 del presente articolo, comportino anche il reato di diffamazione, la persona offesa può chiedere, oltre il risarcimento dei danni ai sensi dell'articolo 185 del codice penale, una somma a titolo di riparazione. La somma è determinata in relazione alla gravità dell'offesa e alla diffusione della notizia, ai sensi dell'articolo 12 della legge 8 febbraio 1948, n. 47. Si applica altresì il terzo comma dell'articolo 595 del codice penale. 3. L'articolo 656-*bis* del codice penale, introdotto dal comma 1 del presente articolo, non si applica ai soggetti e ai prodotti di cui alla legge 8 febbraio 1948, n. 47, e di cui all'articolo 1, comma 3-bis, della legge 7 marzo 2001, n. 62».

[146] Testo dell'art. 265 *bis*: «Chiunque diffonde o comunica voci o notizie false, esagerate o tendenziose, che possono destare pubblico allarme, o svolge comunque un'attività tale da recare nocumento agli interessi pubblici o da fuorviare settori dell'opinione pubblica, anche attraverso campagne con l'utilizzo di piattaforme informatiche destinate alla diffusione online, è punito con la reclusione non inferiore a dodici mesi e con l'ammenda fino a euro 5.000»; Art. 265 *ter*: «Ai fini della tutela del singolo e della collettività, chiunque si rende responsabile, anche con l'utilizzo di piattaforme informatiche destinate alla diffusione online, di campagne d'odio contro individui o di campagne volte a minare il processo democratico, anche a fini politici, è punito con la reclusione non inferiore a due anni e con l'ammenda fino a euro 10.000».

[147] L'art. 658 c.p., rubricato «Procurato allarme presso l'Autorità», recita: «Chiunque, annunziando disastri, infortuni o pericoli inesistenti, suscita allarme presso l'Autorità, o presso enti o

in cui l'allarme è generato attraverso la diffusione di false informazioni tramite piattaforme informatiche. Questa modifica risponderebbe all'esigenza di evitare una proliferazione ingiustificata di nuove fattispecie criminose, che potrebbero facilmente essere messe in discussione in termini di legittimità. Inoltre, avrebbe il vantaggio culturale di ridurre l'enfasi mediatica attorno a tale fenomeno, attualmente amplificata dalle preoccupazioni politiche, e limitare così la creazione di nuove ipotesi di reato, anche se di pericolo concreto.

L'analisi delle normative e delle disposizioni riguardanti l'uso del *web* mette in evidenza una certa frammentazione nelle misure di protezione previste. Da un lato, emerge chiaramente una diffusa preoccupazione sociale legata ai pericoli connessi all'utilizzo della rete, ma, dall'altro, non c'è una visione omogenea su quali rischi siano effettivamente prioritari e quali siano le migliori soluzioni per affrontarli. Questa ambiguità sembra derivare da una strategia di tutela poco coerente: mentre si promuovono politiche volte a favorire l'accesso diffuso a *internet*, migliorare le competenze e includere più persone nell'era digitale, allo stesso tempo si invocano controlli più rigorosi e limitanti sul *web*.

Occorrerebbe forse considerare il web come un semplice mezzo di comunicazione di massa, non diverso da quelli che abbiamo conosciuto in passato. *Internet* è, infatti, un prezioso mezzo di comunicazione globale, e i contenuti che vi si trovano dovrebbero essere protetti dalle stesse norme che regolano la libertà di espressione, come sancito dall'art. 21 della Costituzione italiana. In questo senso, la Corte di Cassazione ha stabilito che, quando un contenuto viene pubblicato su uno spazio web, la sua diffusione deve essere considerata come una comunicazione destinata a un pubblico vasto, potenzialmente accessibile a chiunque abbia i mezzi tecnici e legali per accedervi[148].

Questo contesto comunque sottolinea le difficoltà intrinseche nella regolamentazione del *web*, sia per la complessità tecnica di bloccare un contenuto, sia per il vasto numero di persone che possono accedere all'informazione.

---

persone che esercitano un pubblico servizio, è punito con l'arresto fino a sei mesi o con l'ammenda da euro 10 a euro 516».

[148] Si veda Cass., Sez. V, 27 dicembre 2000 n. 4741, in *DeJure.it*.

Come accade in molte altre situazioni, anche nell'ambito digitale è possibile che si verifichino abusi di diritto o la commissione di reati. Tuttavia, l'ordinamento giuridico prevede già adeguati strumenti di tutela, poiché il mezzo attraverso il quale si diffonde un contenuto non ne altera la natura sostanziale. Attualmente, nel diritto penale, le condotte diffamatorie via *internet* rientrano nella disciplina della diffamazione semplice[149]. È vero, però, che la capacità di diffusione ampia e rapida del mezzo telematico aumenta la potenzialità offensiva del fatto, il che potrebbe giustificare sanzioni più severe.

Inoltre, ci sono circostanze in cui si può ricorrere all'aggravante della diffamazione a mezzo stampa (art. 595 c.p., comma 3), qualora la piattaforma utilizzata presenti caratteristiche assimilabili ai tradizionali mezzi di informazione. La giurisprudenza, in questo ambito, ha fatto significativi progressi: ad esempio, le Sezioni Unite della Corte di Cassazione hanno equiparato le testate giornalistiche online a quelle cartacee, contribuendo a chiarire come le norme sui media tradizionali possano applicarsi anche al contesto digitale[150].

---

[149] L'art. 595 c.p., rubricato «Diffamazione» prevede che: «1. Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a milletrentadue euro. 2. Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della reclusione fino a due anni, ovvero della multa fino a duemilasessantacinque euro. 3. Se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a cinquecentosedici euro. 4. Se l'offesa è recata a un Corpo politico, amministrativo o giudiziario, o ad una sua rappresentanza, o ad una Autorità costituita in collegio, le pene sono aumentate». Per un approfondimento sul reato di diffamazione v. A. GULLO, *Diffamazione e legittimazione dell'intervento penale*, Aracne, Roma, 2013; V. PEZZELLA, *La diffamazione*, Utet Giuridica, Milano, 2016; A. TESAURO, *La diffamazione come reato debole e incerto*, Giappichelli, Torino, 2005; F. BICO, A. SORGATO, *Diffamazione. Aspetti pratici e nuove problematiche*, Giappichelli, Torino, 2007; G. FABRI, *Sul reato di diffamazione*, in *Foro it.*, 10/2023, p. 551 ss.; M. ALESCI, *Rilievi sul delitto di diffamazione e sul valore scriminante della critica*, in *Cass. pen.*, 10/2019, p. 3523 ss.; M. CERASE, *Riforma della diffamazione: rintocchi della giurisprudenza e auspici legislativi*, in *Cass. pen.*, 11/2020, p. 4120 ss; A. VISCONTI, *Onore, reputazione e diritto penale*, EDUCatt, Milano, 2011.

[150] Cfr. Cass. pen. SS.UU., 29 gennaio 2015 n. 31022, in *DeJure.it*, secondo cui la testata giornalistica *online* è equiparata in quanto assimilabile funzionalmente a quella tradizionale e soggiace alla normativa per questa prevista. Tale orientamento è stato poi recepito dai proponenti il Disegno di legge Costa sulla riforma della diffamazione a mezzo stampa. Per un approfondimento dottrinale sulla diffamazione a mezzo stampa v. F. VERDE, *Diffamazione a mezzo stampa e l'esimente dell'esercizio del diritto*, Cacucci, Bari, 2009; M. CHIAROLLA, *La diffamazione a mezzo stampa. Analisi critica della normativa tra diritto di cronaca, diffamazione, privac*y, Experta, Forlì, 2004; M. L. TAMPONI, *In tema di diffamazione a*

Anche le contravvenzioni già previste dall'ordinamento giuridico possono effettivamente essere applicate per contrastare alcune forme di illeciti commessi via *internet*, come ad esempio la diffusione di contenuti illeciti o pericolosi. Tuttavia, potrebbe essere necessario, o comunque opportuno, un aggiornamento normativo per adattarle al contesto digitale moderno. Questo potrebbe comportare sia un ampliamento dell'ambito di applicazione delle contravvenzioni esistenti, includendo specificamente i reati commessi attraverso mezzi digitali, sia una revisione del trattamento sanzionatorio, in modo da garantire che le pene siano adeguate alla gravità delle violazioni commesse *online*.

Interventi normativi di questo tipo potrebbero migliorare l'efficacia della lotta contro i crimini digitali, rendendo la legislazione più conforme ai nuovi mezzi tecnologici e alle forme di comunicazione attuali, senza dover necessariamente creare nuove fattispecie di reato, ma adattando quelle esistenti. Questo approccio avrebbe anche il vantaggio di evitare una proliferazione eccessiva di nuove norme, semplificando l'applicazione del diritto e rendendo più chiara la distinzione tra il lecito e l'illecito in ambito digitale.

2.2.3. La responsabilizzazione dei Socialbot

Abbiamo visto che l'assenza di meccanismi di verifica dell'identità degli utenti e il mancato controllo sui contenuti pubblicati sui *social media* ha facilitato la commissione di reati contro i diritti fondamentali. L'anonimato garantito da *internet* e dai *social*

---

mezzo stampa, in *Giur. it.*, 11/2006, p. 2145 ss.; M. POLVANI, *La diffamazione a mezzo stampa*, CEDAM, Padova, 1998; A. MANNA, *Problemi vecchi e nuovi in tema di diffamazione a mezzo stampa*, in *Arch. pen.*, 3/2012, p. 989 ss.; M. MASCALZONI, *Sulla responsabilità del direttore di un quotidiano on line per diffamazione*, in *Giur. it.*, 6/2011, p. 1378 ss. In particolare, per la diffamazione sul *web* v. D. CHINDEMI, *Diffamazione a mezzo stampa (radio-televisione-Internet)*, Giuffrè, Milano, 2006; S. PERON, *Diffamazione tramite mass-media*, CEDAM, Padova, 2006; V. PEZZELLA, *La diffamazione. Le nuove frontiere della responsabilità penale e civile e della tutela della privacy nell'epoca dei social, delle fake news e degli hate speeches*, Utet Giuridica, Milano, 2020; P. MOSCARINI, *Libertà d'informare, tutela dell'onore e punibilità della diffamazione "mediatica"*, in *Dir. pen. e proc.*, 10/2022, p. 1357 ss.; D. PETRINI, *Diffamazione "on line": offesa recata con "altro mezzo di pubblicità" o col mezzo della stampa?*, in *Dir. pen. e proc.*, 11/2017, p. 1485 ss.; A. RANGHINO, *Diffamazione e "social network": l'attribuzione del "post" all'imputato tra prova logica e prova diretta*, in *MediaLaws*, 3/2023, p. 200 ss.; F.P. DI FRESCO, *In tema di diffamazione telematica*, in *Foro it.*, 9/2007, p. 486 ss.

network è stato spesso utilizzato per compiere reati come diffamazione, adescamento e sostituzione di persona, spesso finalizzati a truffe.

Le tecnologie digitali non solo facilitano, ma amplificano questi crimini, incrementandone l'impatto. Per quanto riguarda la diffamazione, in particolare, la Corte di Cassazione ha riconosciuto che i *social media* possono aggravare la lesione alla reputazione delle vittime, poiché aumentano l'ampiezza e la rapidità della diffusione di contenuti dannosi. In particolare, nella sentenza n. 50 del 2 gennaio 2017 la Corte ha dichiarato che «la diffusione di un messaggio diffamatorio attraverso l'uso di una bacheca "*Facebook*" integra un'ipotesi di diffamazione aggravata». [151].

Anche la Corte costituzionale ha recentemente sottolineato come la velocità e l'estensione con cui un messaggio offensivo si propaga su *internet* possano causare danni molto più gravi rispetto agli stessi comportamenti *offline*[152].

Ad amplificare ulteriormente i contenuti dannosi vi sono poi alcuni *software*, detti *socialbot*, capaci di simulare comportamenti umani su piattaforme *social* e agire autonomamente. Questi *bot*, grazie alla loro capacità di adattarsi all'ambiente digitale, sono in grado di replicare e diffondere contenuti lesivi senza intervento umano diretto, aumentando il rischio di danni per i diritti degli individui[153].

---

[151] Si vedano inoltre le sentenze Cass. pen., sez. V, 23 gennaio 2017, n. 8482, e Cass. pen., sez. V, 6 settembre 2018, n. 40083, in *DeJure.it*.

[152] V. Corte cost., ord. 2 giugno 22 n. 132. La Corte ha sottolineato la «rapidissima e duratura amplificazione degli addebiti diffamatori determinata dai *social networks* e dai motori di ricerca in *internet*, il cui carattere lesivo per la vittima - in termini di sofferenza psicologica e di concreti pregiudizi alla propria vita privata, familiare, sociale, professionale, politica - e per tutte le persone a essa affettivamente legate risulta grandemente potenziato rispetto a quanto accadeva anche solo in un recente passato» (punto 7.3. del Considerato in diritto).

[153] Per un approfondimento sulla nozione di *socialbot* si veda A. TEDESCHI TOSCHI, *Il reato di sostituzione di persona "online" di fronte a "socialbot" e ritratti "AI-generated" ["Artificial Intelligence" - Intelligenza Artificiale]. In favore di una interpretazione estensiva dell'art. 494 del codice penale*, in *MediaLaws*, 3/2023, p. 90 ss.; A. TEDESCHI TOSCHI, G. BERNI FERRETTI, *Il contrasto legislativo ai "socialbot". Alcuni spunti per una riforma in Italia*, in *Inf. dir.*, 1/2023, p. 155 ss.; A. TEDESCHI TOSCHI, G. BERNI FERRETTI, *Social media, profili artificiali e tutela della reputazione. Come l'avvento dei social bot per la gestione dei profili social possa rappresentare una grave minaccia per la reputazione delle persone e quali potrebbero essere le risposte a tale pericolo*, in *Inf. dir.*, 3/2021, p. 107 ss. S. CRESCI, R. DI PIETRO, M. PETROCCHI, A. SPOGNARDI, M. TESCONI, *The paradigm-shift of social spambots: Evidence, theories, and tools for the arms race*, in *Proceedings of the 26th international conference on world wide web companion*, 2019, p. 963 ss.; S. FRANKLIN, A. GRAESSER, *Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents*, in J.P. Müller, M.J. Wooldridge, N.R. Jennings (a

Le attività sui *social network* sono spesso strutturate in forme di interazione predeterminate e standardizzate, grazie alla presenza di pulsanti virtuali specifici come «Mi piace», «Condividi» o «Commenta». Questa configurazione facilita l'automazione delle azioni sui social tramite bot, in particolare i *socialbot*, che possono essere programmati per interagire con i contenuti basandosi su criteri predefiniti[154].

Questa capacità di riconoscere eventi specifici e rispondere in modo preimpostato rende semplice per i bot navigare nei contesti digitali dei social media, imitando il comportamento umano. I *socialbot*, quindi, non solo automatizzano le interazioni, ma potenziano anche la portata e l'impatto di certe operazioni *online*, amplificando le dinamiche tipiche delle piattaforme *social*. Ne consegue che le varie tipologie di reato già analizzate che spesso vengono commesse con l'uso dei *social network* potrebbero essere integrate mediante l'utilizzo di questi *bot*.

---

cura di), *Intelligent Agents III Agent Theories, Architectures, and Languages*, Springer, Berlino, 1996, p. 21 ss.; N. ABOKHODAIR, D. YOO, D.W. MCDONALD, *Dissecting a social botnet: Growth, content and influence in Twitter*, in *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*, 2015, p. 839 ss.; E. FERRARA, O. VAROL, C. DAVIS, F. MENCZER, A. FLAMMINI, *The rise of social bots*, in *Communications of the ACM*, , 2021, p. 9 ss., consultabile sul sito *web* www.dl.acm.org; S. STIEGLITZ, B. ROSS, A.K. JUNG, *Do social bots dream of electric sheep? A categorisation of social media bot accounts*, in *Proceedings of the 28th Australasian Conference on Information Systems (ACIS*), 2017, p. 89 ss.; Y. BOSHMAF, I. MUSLUKHOV, K. BEZNOSOV, M. RIPEANU, *The socialbot network: when bots socialize for fame and money*, in *Proceedings of the 27th annual computer security applications conference*, 2011, p. 93 ss. Simili ai *socialbot*, ma utilizzati per fini diversi sono i c.d. *chatbot*, utilizzati su piattaforme di messaggistica (come *WhatsApp, Facebook Messenger, Telegram*) o sui siti *web* per conversazioni più complesse con gli utenti, sono progettati per simulare una conversazione e interagire direttamente con gli utenti rispondendo a domande, fornendo informazioni, o assistendo in attività specifiche, risoluzione di problemi o supporto clienti. A differenza dei *socialbot*, i *chatbot* sono programmati per avere interazioni più complesse basate sulle richieste degli utenti. Possono utilizzare tecnologie avanzate come l'intelligenza artificiale e il machine learning per comprendere e rispondere in modo naturale alle domande poste dagli utenti, migliorando nel tempo attraverso l'apprendimento automatico. Per approfondire il concetto di *chatbot* si veda P. SAMMARCO, *Osservazioni sulla responsabilità da informazioni inesatte fornite da un "chatbot"*, in *Dir. inform.*, 1/2024, p. 133 ss.; G.M. BACCARI, M. MARRAFFINO, *Le prospettive di utilizzo delle "chatbot" nel procedimento penale*, in *Dir. pen. e proc.*, 8/2021, p. 1008 ss.; A. ROMEO, *"Bad Man" e "Puzzled Man" davanti ad un "chatbot". Il bisogno di accesso cognitivo al diritto e le promesse dell'intelligenza artificiale*, in *dirittifondamentali.it*, 1/2024, p. 22 ss.

[154] Ad esempio, un *socialbot* può essere istruito a riconoscere automaticamente quando un post su *Facebook* non ha ancora ricevuto un Mi piace da parte sua e attivarsi per eseguire questa azione al verificarsi di tali condizioni.

Possiamo prendere in considerazione l'ipotesi di creazione di contenuti originali (come la pubblicazione di post e commenti) ad opera di un *socialbot*. È piuttosto semplice immaginare che, grazie a una programmazione adeguata, un *socialbot* possa pubblicare autonomamente contenuti di natura diffamatoria. Questo scenario diventa ancora più realistico se consideriamo i recenti progressi nelle intelligenze artificiali basate sul *machine learning*, che sono in grado di generare testi in modo autonomo e coerente.

Anche l'azione di condivisione di contenuti lesivi su piattaforme, come la diffusione di messaggi denigratori, costituisce un comportamento delittuoso. Questo perché i *social media*, tramite funzionalità semplici come il pulsante «Condividi», facilitano la propagazione dei contenuti creati da altri utenti. In tal caso, la diffusione di messaggi lesivi non richiede alcuna creatività o abilità, ma semplicemente l'interazione con un tasto predisposto dalla piattaforma stessa. Programmare un *socialbot* per eseguire queste azioni diventa ancora più semplice. Tuttavia, questa automazione può avere conseguenze impreviste. Se un *socialbot* condivide contenuti senza analizzare preventivamente il loro significato o la loro legalità, la sua azione si svolge al buio, ossia senza consapevolezza del messaggio o delle implicazioni legali che esso comporta. Pertanto, il *bot* potrebbe propagare contenuti penalmente rilevanti senza alcun discernimento.

La Corte di Cassazione ha recentemente chiarito che anche l'apposizione di un semplice *like* può essere interpretato come una forma di adesione e condivisione dei messaggi pubblicati, con conseguenze giuridiche rilevanti[155]. I giudici hanno stabilito che una reazione a contenuti di terzi potrebbe integrare essa stessa un reato poiché contribuisce alla visibilità e diffusione del messaggio verso un pubblico più ampio. Questa dinamica si basa sulle caratteristiche dell'algoritmo delle piattaforme, dove le

[155] V. Cass. pen., sez. I, 9 febbraio 2022, n. 4534, in *DeJure.it*. La Corte di Cassazione, al punto 1 del Considerato in diritto, ha affermato che «la diffusione dei messaggi inseriti nelle bacheche *Facebook*, già potenzialmente idonei a raggiungere un numero indeterminato di persone, dipende dalla maggiore interazione con le pagine interessate da parte degli utenti. La funzionalità "*newsfeed*" ossia il continuo aggiornamento delle notizie e delle attività sviluppate dai contatti di ogni singolo utente è, infatti, condizionata dal maggior numero di interazioni che riceve ogni singolo messaggio. Sono le interazioni che consentono la visibilità del messaggio ad un numero maggiore di utenti i quali, a loro volta, hanno la possibilità di rilanciarne il contenuto. L'algoritmo scelto dal *social network* per regolare tale sistema assegna, infatti, un valore maggiore ai post che ricevono più commenti o che sono contrassegnati dal "mi piace" o "*like*"».

interazioni degli utenti aumentano la visibilità dei contenuti, che vengono poi propagati ad altri utenti, amplificando così il potenziale offensivo o illegale dei messaggi.

Gli algoritmi che regolano la diffusione dei contenuti rendono particolarmente semplice per i *socialbot* automatizzare interazioni con i contenuti di terzi. Questo può portare alla diffusione di messaggi potenzialmente lesivi nei confronti di un numero indeterminato di persone.

Uno degli aspetti peculiari dei *socialbot*, che assume particolare rilievo in questo contesto, è che per operare correttamente essi necessitano solo di una connessione a *internet*, senza vincoli geografici o limitazioni legate a un luogo specifico. Questa caratteristica permette ai *socialbot* di condurre attività come campagne propagandistiche, diffamatorie o di disinformazione a livello globale, anche da località fuori dai confini in cui si trovano le vittime. Di conseguenza, le azioni di questi agenti *software* possono sottrarsi alla giurisdizione delle autorità nazionali competenti per la tutela dei diritti degli individui danneggiati, complicando così l'applicazione delle leggi e l'adozione di misure contro le attività illecite *online*.

Questa capacità di agire in uno spazio digitale privo di confini giuridici rafforza il potenziale dei *socialbot* come strumenti pericolosi, poiché possono aggirare i sistemi di regolamentazione di specifici Paesi e continuare a diffondere contenuti dannosi al di fuori del controllo delle autorità locali. Appare, pertanto, necessaria ed urgente un'attività di cooperazione internazionale che conduca all'emanazione di norme globali più efficaci per contrastare l'uso illecito di queste tecnologie in rete.

Attraverso l'utilizzo dei *socialbot* può inoltre essere integrato il reato di sostituzione di persona (art. 494 c.p.)[156]. La giurisprudenza ha da tempo ampliato il campo

[156] L'art. 494 c.p. recita: «Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino ad un anno». Per un approfondimento sul reato di sostituzione di persona si veda G. A. JACOVONE, *Il delitto di sostituzione di persona*, Jovene, Napoli, 1974; R. CAPPITELLI, *La sostituzione di persona nel diritto penale italiano*, in *Cass. pen.*, 10/2005, p. 2994 ss.; In particolare, quando il reato è commesso su *internet*, G. STAMPANONI BASSI, *Sostituzione di persona commessa nella rete Internet*, in *Cass. pen.*, 1/2014, p. 146 ss.; E. MENGONI, *"Chattare" con un "nickname" riconducibile ad altri (e comunicare il*

di applicazione della fattispecie, facendovi rientrare anche condotte legate alla creazione di *account* falsi o all'uso illecito dell'identità altrui *online*. La Corte di Cassazione ha più volte ribadito che il reato di sostituzione di persona si verifica non solo quando qualcuno assume l'identità di un altro individuo nel mondo fisico, ma anche quando crea e utilizza un account *online* con le generalità di un'altra persona, ingannando gli utenti della rete. Questo comportamento può indurre altre persone a credere erroneamente di interagire con il titolare dell'identità abusata.

Già nel 2007, infatti, la Cassazione aveva confermato la condanna all'imputato che aveva creato un *account* di posta elettronica utilizzando il nome della vittima, ledendone l'immagine e la dignità attraverso l'allacciamento di rapporti con altre persone[157]. La Suprema Corte ha invero sottolineato che la sostituzione di persona può configurarsi anche quando il danno arrecato non è di natura economica, ma riguarda lesioni alla reputazione, all'immagine o alla dignità della persona colpita.

Occorre chiedersi se l'articolo 494 c.p. possa essere applicato anche ai casi di dissimulazione dell'identità *online* perpetrata per mezzo di un *socialbot,* e soprattutto a chi debba essere attribuita la responsabilità. Infatti, alcuni aspetti della natura di questi agenti autonomi sollevano complessità interpretative che rendono l'applicazione della norma meno immediata di quanto sembri.

Innanzitutto, la norma prevede che il reato di sostituzione di persona si realizzi quando un soggetto attribuisce a sé o ad altri un'identità o caratteri non propri. Tuttavia, i *socialbot* non sono persone fisiche ma *software* che operano in modo autonomo sulla base di una programmazione. Questo solleva il dubbio su come si possa applicare l'art. 494 c.p. ai *socialbot*, dato che il reato sembra riferirsi esclusivamente a soggetti umani, e non a beni immateriali come un *software*. A tal proposito, se è pur vero che i *socialbot* agiscono autonomamente, ciò non implica che abbiano una capacità

loro numero telefonico) integra il reato di sostituzione di persona, in *Cass. pen.*, 1/2014, p. 148 ss.; A. TEDESCHI TOSCHI, *Il reato di sostituzione di persona "online" di fronte a "socialbot" e ritratti "AI-generated",* cit.

[157] V. Cass. pen., sez. V, 14 dicembre 2007, n. 46674, in *DeJure.it*. Lo stesso orientamento è stato ripreso da successive pronunce: Cass. pen., sez. III, 3 aprile 2012, n. 12479; Cass. pen., sez. V, 29 aprile 2013, n. 18826; Cass. pen., sez. V, 16 giugno 2014, n. 25774; Cass. pen., sez. V, 8 giugno 2018, n. 33862; Cass. pen., sez. II, 17 maggio 2019, n. 21705; Cass. pen., sez. II, 02 luglio 2020, n. 23760; Cass. pen., sez. V, 6 luglio 2020, n. 22049; Cass. pen., sez. V, 5 febbraio 2021, n. 12062.

decisionale indipendente. Essi seguono un codice preimpostato dal programmatore o dall'amministratore. Nonostante la loro capacità di adattarsi agli *input* dell'ambiente digitale in cui operano, le loro azioni sono il risultato di una serie di comandi predefiniti, e non di vere e proprie decisioni autonome.

Non bisogna confondere questa autonomia d'azione con una forma di autonomia decisionale dei *socialbot*, rischiando di attribuire responsabilità penali ai *software* stessi. Almeno allo stato attuale dell'avanzamento tecnologico dell'IA, un *socialbot* non è un soggetto imputabile in quanto non dotato di volontà o coscienza. La responsabilità penale dovrebbe sempre essere attribuita a chi programma, gestisce o utilizza il *bot* per compiere azioni illecite[158].

È importante comunque distinguere le responsabilità tra chi crea il *software* e chi lo utilizza effettivamente. Il creatore del *socialbot* non è automaticamente responsabile per tutte le azioni compiute attraverso il suo *software*, poiché la sua responsabilità è limitata alla progettazione e alle capacità che ha conferito al *bot*. È l'utilizzatore che determina quando e come queste funzionalità vengano attivate, decide quando farlo intervenire in base a determinati *trigger* (come l'interazione con specifici contenuti su una piattaforma *social*).

L'art. 494 del Codice Penale, pertanto, non si applica automaticamente ai *socialbot*, poiché essi non sono soggetti giuridici autonomi ma sono strumenti tecnologici al servizio del loro amministratore. Le azioni compiute dai *socialbot,* come già sottolineato, ricadono sotto la responsabilità di chi li programma o li utilizza, rendendo necessario un approccio più complesso per affrontare l'utilizzo di tali strumenti nell'ambito della dissimulazione di identità *online* e delle condotte illecite. Anche qualora il *software* sia dotato di sistemi di IA di tipo generativo, che gli consentano di creare e pubblicare contenuti in modo autonomo, la responsabilità sarà sempre di chi lo ha programmato per agire o di chi gli ha chiesto di operare in un certo modo.

---

158 V. A. TEDESCHI TOSCHI, G. BERNI FERRETTI, *La responsabilità per la diffamazione compiuta da un'Intelligenza artificiale. Possibili scenari costruiti partendo dall'esempio dell'IA Tay*, in *Ciberspazio e diritto*, 2/2023, p. 173 ss.

3. Le applicazioni in ambito di diritto penale

3.1. Polizia predittiva

L'intelligenza artificiale si è dimostrata estremamente efficace nel settore delle attività investigative condotte dalle forze di polizia, dove ha portato innovazioni di grande rilievo. Grazie all'introduzione di tecnologie basate sull'IA, è stato possibile sviluppare metodologie di indagine innovative e dinamiche, particolarmente utili per la prevenzione dei crimini, l'orientamento delle indagini e l'identificazione di relazioni e connessioni tra eventi o individui. La capacità dell'IA di elaborare grandi quantità di dati in modo rapido ed efficiente consente di implementare strategie di prevenzione più mirate ed efficaci, migliorando significativamente le capacità di investigazione e contrasto della criminalità.

Si parla in questo caso di polizia predittiva, nozione che fa riferimento ad un insieme di attività che utilizzano metodi statistici e algoritmi per cercare di prevedere chi potrebbe commettere un reato, oltre a individuare dove e quando un crimine potrebbe avvenire, con l'obiettivo di prevenirlo prima che si verifichi[159].

Recentemente, l'uso di *software* basati sull'intelligenza artificiale ha rivoluzionato la polizia predittiva, permettendo la raccolta e l'elaborazione di enormi quantità di dati, rivelando connessioni che in precedenza sfuggivano all'analisi umana, aiutando forze dell'ordine non solo nel contesto strettamente investigativo, ma anche per il

[159] Per un approfondimento sulla nozione di polizia predittiva v. L. ALGERI, *Intelligenza artificiale e polizia predittiva*, in *Dir. pen. e proc.*, 6/2021, p. 724 ss.; A. BONFANTI, *"Big data" e polizia predittiva: riflessioni in tema di protezione del diritto alla "privacy" e dei dati personali*, in *MediaLaws*, 3/2018, p. 206 ss.; R. PELLICCIA, *Polizia predittiva: il futuro della prevenzione criminale?*, in *cyberlaws.it*, 9 maggio 2019; B. PEREGO, *Predictive policing: trasparenza degli algoritmi, impatto sulla privacy e risvolti discriminatori*, in *BioLaw Journal*, 2/2020, p. 447 ss.; W.L. PERRY, B. MCINNIS, C.C. PRICE, S.C. SMITH, J.S. HOLLYWOOD, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, Rand, Santa Monica, 2013; L. BENNET MOSES, J. CHAN, *Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability*, in *Policing and Society*, 2016, p. 1 ss.; G. MASTROBUONI, *Crime is Terribly Revealing: Information Technology and Police Productivity*, in *Review of Economic Studies*, 6/2020, p. 2727 ss.; C. MORELLI, *Furti e rapine: a sventarli ci pensa l'intelligenza artificiale!*, in *Altalex.com*, 6 maggio 2019; E. THOMAS, *Why Oakland Police Turned Down Predictive Policing*, in *vice.com*, 28 dicembre 2016.

controllo del territorio e la sua analisi geografica. Grazie alle sue capacità avanzate, l'IA permette di analizzare con maggiore precisione le dinamiche sociali, facilitando l'individuazione di schemi o comportamenti anomali.

In questo contesto, le intercettazioni, sia telefoniche che ambientali, rivestono un ruolo di particolare rilievo, insieme all'utilizzo dei captatori informatici, ovvero *software* installati da remoto su dispositivi mobili. Questi strumenti permettono di raccogliere ingenti volumi di dati e informazioni, rappresentando una delle principali fonti per l'analisi investigativa. Tuttavia, i dati ottenuti sono per lo più non strutturati, ma grazie all'impiego di tecniche avanzate come quelle criptografiche si riesce ad elaborarli in modo da garantire la sicurezza delle informazioni e permettere una gestione più efficace delle informazioni raccolte.

Tra l'altro, proprio la disciplina delle intercettazioni è spesso oggetto di critiche. Uno dei problemi principali è quello di evitare gli abusi dell'autorità. Le intercettazioni devono essere autorizzate solo quando strettamente necessarie per fini legittimi, altrimenti si ricadrebbe in un fenomeno di sorveglianza di massa eccessivamente invasivo rispetto allo scopo perseguito.

Le intercettazioni comportano anche la raccolta, la conservazione e l'elaborazione di grandi quantità di dati personali, il che solleva questioni legate alla tutela dei dati. Le informazioni raccolte possono essere sensibili e devono essere gestite in conformità con normative specifiche, come il GDPR.

Per tali ragioni la normativa riguardante le intercettazioni è stata recentemente oggetto di riforma. La legge Nordio (n. 114/2024)[160] ha introdotto significative modifiche finalizzate a rafforzare la tutela della riservatezza nei procedimenti penali e a limitare la possibilità di diffondere informazioni sensibili derivanti dalle intercettazioni, proteggendo sia gli indagati che i soggetti terzi[161].

---

[160] Pubblicata nella G.U. n. 187 del 10 agosto 2024, recante «Modifiche al codice penale, al codice di procedura penale, all'ordinamento giudiziario e al codice dell'ordinamento militare», entrata in vigore il 25 agosto 2024.

[161] Il nuovo comma 2-*bis* dell'art. 114 c.p.p. sancisce che è vietata la pubblicazione, anche parziale, delle intercettazioni, a meno che non siano riprodotte in un provvedimento del giudice o utilizzate nel dibattimento. Con la modifica dell'art. 116 c.p.p., viene stabilito che la copia delle intercettazioni non può essere rilasciata a soggetti diversi dalle parti e dai loro difensori, salvo che venga

Una funzione particolarmente rilevante è quella della categorizzazione delle immagini. Questa capacità permette di identificare con elevata precisione la natura dell'oggetto rappresentato in una fotografia o video e di analizzare le immagini per cercare e individuare elementi di interesse. Ad esempio, è possibile estrarre dettagli come la targa di un veicolo o particolari di oggetti che potrebbero risultare cruciali per l'investigazione.

Le tecnologie consentono anche operazioni di pulizia e filtraggio delle immagini, migliorando la qualità visiva e rendendo più evidenti dettagli altrimenti trascurabili. Un altro aspetto significativo è la capacità di comparazione delle immagini. Confrontando una serie di figure tra loro, l'IA può individuare similitudini e analogie che potrebbero indicare legami o correlazioni rilevanti per l'indagine, come la connessione tra diversi eventi, luoghi o oggetti che possano essere associati ad un determinato reato[162].

In aggiunta alla categorizzazione e analisi delle immagini, l'intelligenza artificiale consente di individuare con precisione il momento temporale in cui si verifica un determinato evento rappresentato. Attraverso un'accurata analisi dell'immagine o del video di riferimento, è possibile ricostruire l'esatta sequenza temporale degli avvenimenti, offrendo un quadro dettagliato delle dinamiche. L'analisi di elementi visibili come paesaggi, edifici o segnaletiche può essere utilizzata anche per localizzare con precisione un punto di interesse geografico.

---

dimostrata la necessità per un altro procedimento. Le modifiche agli articoli 268 e 291 c.p.p. impongono di eliminare dai verbali delle intercettazioni informazioni sensibili non rilevanti, salvo che queste siano necessarie per motivare richieste di misure cautelari. Questo mira a proteggere la *privacy* di individui terzi, non coinvolti direttamente nei procedimenti. Per un approfondimento sul tema delle intercettazioni e sugli ultimi aggiornamenti v. M. GIALUZ, *Le novità della "manovra Nordio" in materia processuale: quando l'ideologia rischia di provocare un'eterogenesi dei fini*, in *Sistema Penale*, 22 Luglio 2024; M. TORRE, *Considerazioni su perquisizione, sequestro e intercettazioni digitali*, in *Dir. pen. e proc.*, 6/2024, p. 811 ss.; S. TOGNAZZI, *Il diritto di difesa e l'accesso alle intercettazioni in fase cautelare*, in *Foro it.*, 3/2024, p. 124 ss.; F. CENTORAME, *La disciplina delle intercettazioni (ancora) nel mirino legislativo: chiose a margine della l. 9 ottobre 2023, n. 137*, in *Proc. pen. e giust.*, 2/2024, p. 478 ss.; L. GIORDANO, *Una nuova riforma della disciplina delle intercettazioni*, in *Dir. pen. e proc.*, 1/2024, p. 11 ss.; L. LUDOVICI, *Disegno di legge c.d. Nordio: nuove garanzie processuali tra fughe in avanti e false partenze*, in *Leg. pen.*, 2/2024, p. 112 ss.

[162] v. C. PISTILLI, *L'utilizzo dell'intelligenza artificiale nel campo delle attività investigative delle forze dell'ordine,* cit., p. 155.

Un altro strumento particolarmente efficace è quello di analisi del testo ed elaborazione del linguaggio naturale. Il sistema descritto utilizza diversi moduli per svolgere attività di analisi, trasformando dati non strutturati, come testi semplici, in dati strutturati, cioè in conoscenza e informazioni utili di vario tipo[163].

Altri sistemi particolarmente efficaci sono quelli basati sulla cosiddetta criminologia ambientale, che identificano le cosiddette «zone calde» (*hotspots*), le aree che potrebbero diventare il teatro di futuri reati[164]. In questo modo le autorità riescono a comprendere meglio il territorio, potenziando così la loro capacità di intervento e prevenzione, oltre a migliorare l'efficienza nel monitoraggio delle aree più sensibili o soggette a rischio.

Da segnalare, inoltre, l'esistenza di *software* basati sul *crime linking*, che si concentrano sulla serialità criminale di determinati individui, sia già identificati che ancora da individuare. L'obiettivo è prevedere dove, come e quando tali soggetti potrebbero

[163] I moduli sono efficacemente esplicati dal lavoro di C. PISTILLI, *L'utilizzo dell'intelligenza artificiale nel campo delle attività investigative delle forze dell'ordine,* cit., p. 161 ss. Tra i vari moduli rileva l'estrattore di parole chiave, che identifica le parole chiave presenti in un documento, assegnando un peso a ciascuna in base alla frequenza con cui compare. Il risultato è una lista di termini con un peso associato, dove le parole più grandi sono quelle utilizzate più frequentemente. Vi è poi l'estrattore delle entità (o *named entity recognition*), che riconosce le entità nel testo e le classifica in categorie come persone, date, luoghi o oggetti. Un altro *task* importante è la *summarization*, ovvero la creazione di riassunti. Questo può essere fatto in due modi: il riassunto estrattivo, che elimina le parti meno rilevanti mantenendo le frasi più importanti, e il riassunto astrattivo, che riformula il testo con termini semantici simili, cercando di esprimere gli stessi concetti con frasi nuove e più sintetiche. Ancora, il *topic extractor* è un modulo che individua i temi principali all'interno di un documento. Le parole con significati simili vengono raggruppate in rettangoli colorati che rappresentano i vari argomenti trattati nel testo, lasciando all'operatore il compito di comprendere il significato di ciascun *topic*. Il sistema può anche produrre una mappa della conoscenza in forma di grafo orientato. I nodi rappresentano le entità ricavate dal testo, mentre gli archi indicano le relazioni e le azioni tra di esse. Questo permette di visualizzare le connessioni e le gerarchie presenti nel testo. Infine, il modulo di analisi del *sentiment* è utilizzato per determinare il tono emotivo o l'atteggiamento del testo. Questo strumento assegna un'etichetta che indica il livello di considerazione o soddisfazione rispetto a una persona, prodotto o evento, misurando così il *sentiment* che emerge dal contenuto analizzato.

[164] Un esempio di questa categoria è il sistema informatico *X-LAW*, sviluppato originariamente dalla Questura di Napoli, che ha già mostrato risultati promettenti in Italia nella prevenzione di specifiche tipologie di crimini. I caratteri di questo sistema sono approfonditi sul sito *web* www.xlaw.it.

commettere il prossimo reato, analizzando il *modus operandi* che emerge dalla loro serie di crimini[165].

La predizione si fonda essenzialmente sull'analisi attuariale di una vasta gamma di dati, che includono informazioni sui reati già commessi, i movimenti e le attività di individui sospettati, le aree in cui si verificano frequentemente azioni criminali e le caratteristiche di tali luoghi, oltre a fattori stagionali o condizioni meteorologiche associate a specifici crimini. Tra i dati utilizzati, possono comparire anche dettagli riguardanti l'etnia, il livello di istruzione, la situazione economica e le caratteristiche fisiche di individui associati a determinate categorie criminologiche, come i potenziali terroristi.

Più in generale, si possono effettuare anche procedure di *big data analytics*, ossia processi che permettono di estrarre conoscenza e valore dall'enorme quantità di dati che viene continuamente generata da molteplici dispositivi interconnessi, come *smartphone*, sensori IoT, e *computer*.

L'adozione di queste metodologie di indagine, basate sull'intelligenza artificiale, è diventata sempre più comune nel panorama investigativo attuale. L'utilizzo di tecniche di IA si è diffuso al punto da rappresentare, in alcuni casi, l'unica strada percorribile per ottenere nuove conoscenze nascoste nei dati raccolti durante le indagini. Grazie alla capacità di analizzare grandi quantità di informazioni non strutturate e di individuare *pattern* e correlazioni non evidenti a priori, l'IA consente di estrarre informazioni preziose che, altrimenti, potrebbero rimanere inesplorate, fornendo così un supporto essenziale alle forze dell'ordine[166].

I sistemi di polizia predittiva offrono indubbi vantaggi, ma sollevano anche numerose preoccupazioni. Innanzitutto, sono efficaci solo per un ristretto numero di reati, come quelli legati alla criminalità di strada, ma non necessariamente per quelli più minacciosi per la democrazia e le libertà individuali. Inoltre, il loro utilizzo

---

[165] Un esempio noto di questa categoria è il *software* Delia, creato dalla società KeyCrime, le cui caratteristiche sono consultabili sul sito *web* www.keycrime.com.

[166] Sul punto si veda *L'impatto dell'Intelligenza Artificiale (AI Artificial Intelligence) sul ciclo di intelligence e sugli strumenti a disposizione per i pianificatori militari e le forze dell'ordine*, a cura del Centro Alti Studi per la Difesa, cit., p. 69 ss.

potrebbe entrare in conflitto con la protezione della *privacy*, dato il vasto numero di dati personali raccolti, e con il principio di non discriminazione, specialmente se collegano pericolosità a caratteristiche etniche, religiose o sociali.

Questi sistemi, alimentandosi dei dati che essi stessi producono, rischiano di creare circoli viziosi: un'area designata come «zona calda» vedrà intensificarsi i controlli di polizia, aumentando così i reati rilevati e confermando ulteriormente il suo status, mentre altre aree potrebbero rimanere trascurate e non adeguatamente monitorate.

Un ulteriore aspetto problematico è la tendenza di questi sistemi a promuovere una prevenzione dei crimini attraverso una maggiore sorveglianza poliziesca, piuttosto che affrontare le radici sociali, ambientali ed economiche del crimine.

Infine, la maggior parte di questi *software* è brevettata da aziende private, che proteggono gelosamente i loro segreti industriali e commerciali. Questo limita la trasparenza e la possibilità di una verifica indipendente dei risultati, oltre al fatto che, anche se i meccanismi fossero resi pubblici, potrebbero rimanere incomprensibili a causa della complessità e dell'autonomia del *machine learning* (la cosiddetta «scatola nera»). Sarebbe, pertanto, di grande importanza se tali dati fossero facilmente accessibili agli operatori autorizzati e potessero essere archiviati e elaborati in modo efficace per garantire il loro riuso, facilitando il processo investigativo e ottimizzando le risorse disponibili.

3.2. Gli algoritmi decisionali e il giudice-robot

Da qualche tempo sono sempre più utilizzati i cosiddetti *automated decision systems*, algoritmi basati sull'intelligenza artificiale impiegati per prendere decisioni in una vasta gamma di settori[167]. Tra le molteplici scelte che tali algoritmi possono prendere, vi sono anche quelle relative alla risoluzione e prevenzione delle controversie.

[167] Gli algoritmi decisionali sono utilizzati da tempo in materia tributaria e amministrativa. Per un approfondimento sull'utilizzo di tali algoritmi nei processi tributari si veda F. FARRI, *Questioni in*

In particolare, nel campo della composizione delle liti in materia penale[168], le nuove tecnologie hanno sviluppato strumenti estremamente avanzati. Grazie alla capacità di analizzare enormi quantità di dati provenienti da fonti come banche dati

tema di giustizia predittiva in materia tributaria, in *Il processo*, 3/2023, p. 841 ss.; E. DELLA VALLE, *Il giudice tributario robot*, in *Riv. dir. trib.*, 2022, p. 15 ss.; G. INGRAO, A. BUCCISANO, *L'intelligenza artificiale e la giustizia predittiva alla luce del progetto "Prodigit"*, in *Riv. dir. trib.*, 2022, p. 70 ss.; V. MASTROIACOVO, *Sulla giustizia predittiva ovvero di quel che accade quando il mito della calcolabilità del diritto incontra i pregiudizi sulla materia tributaria*, in *Riv. dir. trib.*, 1/2024, p. 43 ss.; P. GIACALONE, *Intelligenza artificiale, giustizia predittiva e processo tributario: problemi e prospettive*, in *Riv. dir. trib.*, 3/2023, p. 299 ss.; C. SACCHETTO, *Processo tributario telematico e giustizia predittiva in ambito fiscale*, in *Rass. trib.*, 1/2020, p. 41 ss. Si veda altresì per i processi amministrativi F. COSTANTINO, *Algoritmi, intelligenza artificiale e giudice amministrativo*, in *Giur. it.*, 6/2022, p. 1527 ss.; E. CARLONI, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm.*, 2/2020, p. 273 ss.; G. M. ESPOSITO, *Al confine tra algoritmo e discrezionalità. Il pilota automatico tra procedimento e processo*, in *Diritto e processo amministrativo*, 1/2019, p. 39 ss.; D.U. GALETTA, J.G. CORVALÀN, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *federalismi.it*, 3/2019, p. 2 ss.; G. BOTTO, *Giustizia predittiva e sentenza in forma semplificata: alcuni spunti per una (razionale) applicazione dell'intelligenza artificiale nel processo amministrativo*, in *Diritto e processo amministrativo*, 2/2023, p. 493 ss. Per un ulteriore approfondimento anche in tema di diritto civile e del lavoro si veda M. BIASI, A. LOMBARDI, *Processo del lavoro e giustizia predittiva: prime riflessioni*, in *Riv. it. dir. lav.*, 3/2023, p. 361 ss.; C. ROMEO, *Perplesse valutazioni su giustizia predittiva: vicende di mutazione epocale e riflessi nell'ambito del lavoro*, in *Mass. giur. lav.*, 3/2023, p. 519 ss.; F. BARBIERI, *L'intelligenza aumentata nell'organizzazione dell'ufficio giudiziario*, in *Giusto proc. civ.*, 3/2021, p. 843 ss.; E. FABIANI, *Intelligenza artificiale e accertamento dei fatti nel processo civile*, in *Giusto proc. civ.*, 1/2021, p. 45 ss.; E. BATTELLI, *Giustizia predittiva, decisione robotica e ruolo del giudice*, in *Giust. civ.*, 2/2020, p. 281 ss.; G. ZACCARIA, *Figure del giudicare: calcolabilità, precedenti, decisione robotica*, in *Riv. dir. civ.*, 2/2020, p. 277 ss.; A. DE LA OLIVA SANTOS, *"Giustizia predittiva", interpretazione matematica delle norme, sentenze robotiche e la vecchia storia del "Justizklavier"*, in *Riv. trim. dir. proc. civ.*, 3/2019, p. 883 ss.

[168] Sul punto si veda M. CATERINI, *Il giudice penale "robot"*, in *Leg. pen.*, 12/2020; E. AMODIO, *Il processo come gioco tra letteratura e diritto vivent*e, in *Riv. it. dir. e proc. pen.*, 4/2020, p. 1663 ss.; F. CORONA, *La decisione del giudice tra precedente giudiziale e predizione artificiale*, in *Democrazia e Diritti Sociali*, 1/2023, p. 83 ss.; S. ARDUINI, *La "scatola nera" della decisione giudiziaria*, cit., p. 453 ss.; M. MIRAVALLE, *I nodi gordiani della giustizia penale ad alta intensità tecnologica. Verso il giudice bocca della tecnologia?*, in *Materiali per una storia della cultura giuridica*, 1/2020, p. 301 ss.; S. QUATTROCOLO, *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"*, in *Cass. pen.*, 4/2019, p. 1748 ss.; G. FRANSONI, *Bridoye e il potere di decidere. Considerazioni su giustizia predittiva, giustificabilità della decisione e indipendenza dei giudici*, in *Politica del diritto*, 3/2023, p. 297 ss.; M. DELL'UTRI, *La giustizia predittiva. Introduzione*, in *Giur. it.*, 7/2022, p. 1759 ss.; A. SANTOSUOSSO, G. SARTOR, *La giustizia predittiva: una visione realistica*, in *Giur. it.*, 7/2022, p. 1760 ss.; A. SIGNORELLI, *La prevedibilità delle e nella decisione giudiziaria*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, E M. Proto (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, cit. p. 997 ss.; K.D. ASGLEY, *Artificiale Intelligence and Legal Analytics, New Tools for Law Practice in the Digital Age*, Cambridge University Press, Cambridge, 2017.

giurisprudenziali, normative e raccolte di precedenti legali, l'IA riesce ad affrontare e risolvere le dispute in modo efficace e rapido[169].

L'impiego della giustizia predittiva solleva una serie di rischi significativi, tra cui la possibilità di introdurre discriminazioni e automatismi nel processo decisionale. La maggior parte dei software sono capaci di rispondere secondo logiche binarie o probabilistiche, ma è improbabile che tali strumenti possano esprimere valutazioni che richiedono un intervento da parte di una persona fisica, con fattori irriducibilmente legati all'esperienza e alla sensibilità umana. Pertanto, la capacità di un algoritmo di applicare la regola basata sull'«oltre ogni ragionevole dubbio» (art. 533, comma 1, c.p.p.) sembra difficilmente immaginabile.

Vi sono poi dei contrasti con il dettato costituzionale[170]. La dottrina più critica ritiene infatti che sia impossibile rispettare la garanzia del giudice naturale precostituito per legge ex art. 25 comma 1 Cost in presenza di un «giudice-macchina» difficilmente localizzabile. Inoltre, dubbi vengono sollevati anche in relazione al fatto che un software possa essere in grado di amministrare la giustizia «in nome del popolo», come richiesto dall'art. 101 Cost. Inoltre, anche il fatto che il giudice robot sia vincolato ad un algoritmo e ad un'analisi dei dati e dei precedenti potrebbe portarlo a non essere «soggetto soltanto alla legge» (art. 101, comma 2, Costituzione)[171].

---

169 Questi sistemi utilizzano varie strategie, anche applicando la c.d. la teoria dei giochi. Si tratta di una disciplina matematica che studia le situazioni di interazione strategica tra soggetti (detti giocatori), i quali prendono decisioni che influenzano i risultati reciproci. In altre parole, la teoria dei giochi si occupa di analizzare come individui o gruppi prendono decisioni razionali in scenari di conflitto o cooperazione, cercando di massimizzare i propri benefici o minimizzare le perdite, considerando anche le mosse degli altri partecipanti. Modelli della teoria dei giochi possono essere usati per analizzare le interazioni tra il sistema giudiziario e gli imputati, in particolare quando si considerano decisioni riguardo alla libertà condizionale o al rilascio su cauzione. Gli algoritmi possono valutare le probabilità che un imputato, una volta rilasciato, commetta di nuovo un crimine, e tali probabilità possono essere modellate come un gioco strategico tra il sistema e l'imputato.

170 F. BASILE, *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione,* cit., p. 10.

171 Per delle opinioni critiche sulla giustizia predittiva si veda M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *Dir. pen. cont.*, 29 maggio 2019; S. GABORIAU, *Libertà e umanità del giudice: due valori fondamentali della giustizia. La giustizia digitale può garantire nel tempo la fedeltà a questi valori?*, in *Quest. giust.*, 4/2018, p. 11 ss.; G. CANZIO, *Il dubbio e la legge*, in *Dir. pen. cont.*, 20 luglio 2018; A. NATALE, *Introduzione. Una giustizia (im)prevedibile?*, in *Quest. giust.*, 4/2018, p. 7 ss.; C. CASTELLI, D. PIANA, *Giustizia predittiva. La qualità della giustizia in*

Nonostante questi dubbi, tra i vantaggi che potrebbe portare la giustizia predittiva vi è certamente quello di ridurre significativamente i tempi di decisione e comportare notevoli risparmi economici, sia per le parti interessate, sia per le istituzioni responsabili della risoluzione delle controversie. Inoltre, l'adozione di questi sistemi si basa su una metodologia che viene percepita dai soggetti coinvolti come oggettiva e libera da pregiudizi[172].

3.3. Algoritmi predittivi e valutazione della pericolosità criminale

Un altro degli ambiti di dialogo tra intelligenza artificiale e diritto penale è quello relativo alla valutazione della pericolosità criminale per mezzo di algoritmi predittivi. Questi ultimi, attraverso l'analisi di una serie di dati, cercano appunto di prevedere la probabilità che un individuo pregiudicato possa commettere in futuro nuovi reati[173].

---

due tempi, in *Quest. giust.*, 4/2018, p. 153 ss.; M. NUZZO, *Il problema della prevedibilità delle decisioni: calcolo giuridico secondo i precedenti*, in A. Carleo (a cura di), *Calcolabilità giuridica*, Il Mulino, Bologna, 2017, p. 137 ss.; C. V. GIABARDO, *Il giudice e l'algoritmo (in difesa dell'umanità del giudicare)*, in *Giustizia insieme*, 9 luglio 2020; E. GABELLINI, *La "comodità del giudicare": la decisione robotica*, in *Riv. trim. dir. proc. civ.*, 2019, p. 1309 ss.; F. DONATI, *Impieghi dell'Intelligenza artificiale a servizio della giustizia. Tra rischi e opportunità*, in *AI Anthology*, *Profili giuridici, economici e sociali dell'intelligenza artificiale*, Il Mulino, Bologna, 2022, p. 179 ss.; E. RULLI, *Giustizia predittiva, intelligenza artificiale e modelli probabilistici. Chi ha paura degli algoritmi?*, in *Analisi giuridica dell'economia*, 2018, p. 533 ss.

[172] Di questo parere è J. KAPLAN in *Intelligenza artificiale. Guida al futuro prossimo*, Luiss University Press, Roma, II ed., 2018, p. 72.

[173] Per un approfondimento sugli algoritmi predittivi si veda 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 *Arch. pen.*, 1/2021, p. 3 ss.; E. FALLETTI, *Uso di algoritmi predittivi con scopo investigativo e violazione costituzionale del "Persönlichkeitsrecht"*, in *Foro it.*, 6/2023, p. 298 ss.; A. VALSECCHI, *Il nuovo volto della discrezionalità giudiziaria: prospettive e pericoli a partire dalla giurisprudenza americana sui "risk assessment tools" impiegati nel "sentencing"*, in *federalismi.it*, 17/2023, p. 303 ss.; M. DI FLORIO, *"Calculate criminal law"? Criticità nell'uso degli algoritmi di pericolosità sociale*, in *Leg. pen.*, 1/2023, p. 327 ss.; L. CASTELLETTI, G. RIVELLINI, E. STRATICÒ, *Efficacia predittiva degli strumenti di Violence Risk Assessment e possibili ambiti applicativi nella psichiatria forense e generale italiana*, in *Journal of Psychopathology*, 2014, p. 153 ss.; G. ROCCA, C. CANDELLI, I. ROSSETTO, F. CARABELLESE, *La valutazione psichiatrico forense della pericolosità sociale del sofferente psichico autore di reato: nuove prospettive tra indagine clinica e sistemi attuariali*, in *Riv. it. med. leg. dir. san.*, 4/2012, p. 1442 ss.; D. COLOMBO, *Valutare per rieducare. Alternative al carcere e "risk assessment tools"*, in *Dir. pen. cont.*, 1/2024, p. 262 ss.; E. PIETROCARLO, *Predictive Policing: criticità e prospettive dei sistemi di identificazione dei potenziali criminali*, cit., p. 114 ss.

Tali sistemi cercano di calcolare, attraverso l'elaborazione di una quantità enorme di dati, quale sia la probabilità che un individuo con determinate caratteristiche possa commettere un nuovo reato in futuro, individuando relazioni, coincidenze e correlazioni che consentirebbero di profilare una persona e prevederne i comportamenti futuri, compresi quelli di rilevanza penale. Questa è una domanda cruciale in diversi contesti giuridici, come l'applicazione di misure di sicurezza, l'adozione di misure cautelari o di prevenzione, e persino la concessione della sospensione condizionale della pena o l'affidamento in prova al servizio sociale.

Oggi, in alcuni Paesi (soprattutto negli Stati uniti) tali valutazioni prognostiche della pericolosità criminale sono affidate a specifici algoritmi (*risk assessment tools*, o algoritmi predittivi), capaci di rielaborare una serie di dati al fine di profilare una persona e prevederne i successivi comportamenti di rilevanza penale.

Si ottengono così dei fattori di rischio, funzionali ad un'indagine di tipo statistico: viene assegnato un punteggio a ciascun fattore sulla base della probabilità che, dalla sua presenza, possa derivare il rischio di recidiva.

Il risultato di questo lavoro è una serie di «scale di valutazione» della pericolosità criminale, che si differenziano tra loro sulla base, fra l'altro, del campione di popolazione cui si riferiscono: avremo quindi scale applicabili agli uomini e alle donne, ai pazienti psichiatrici, agli ex detenuti. Esistono poi scale generiche, riferite a tutti i tipi di reati, e specifiche, relative a singole tipologie di reati come quelli violenti o sessuali[174].

Sebbene costituiscano una novità per il diritto penale, scale del genere sono già utilizzate da tempo in altri settori, come nel caso dei contratti di assicurazione: ad esempio, per la stipulazione di polizze sulla vita, le compagnie sviluppano delle stime sulla base di fattori di rischio come età, sesso, fumo, luogo di residenza ecc., la cui unione statistica produce una stima predittiva per ciascun contraente.[175]

Negli Stati Uniti già da anni sono in uso algoritmi predittivi nell'ambito dei procedimenti penali, al fine di valutare la pericolosità criminale. Tra i vari algoritmi

---

[174] F. BASILE, *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione,* cit.

[175] L. CASTELLETTI, G. RIVELLINI, E. STRATICÒ, *Efficacia predittiva degli strumenti di Violence Risk Assessment e possibili ambiti applicativi nella psichiatria forense e generale italiana*, cit., p. 153 ss.

utilizzati, merita menzione quello denominato COMPAS (*Correctional offender management profiling for alternative sanctions)*. Si tratta di uno strumento di gestione dei casi e supporto decisionale sviluppato da Northpointe (ora Equivant), utilizzato dai tribunali statunitensi per valutare la probabilità che un imputato diventi recidivo. I risultati ottenuti da questo sistema vengono utilizzati per valutare la possibilità di carcerazione preventiva, nonché per la determinazione del trattamento penitenziario e l'accesso a misure alternative alla detenzione[176].

Il metodo utilizzato dal software COMPAS inizia con la formulazione all'individuo di 137 domande, finalizzate a studiarne la personalità, il carattere, le idee. Tra queste domande, alcune come: «uno dei tuoi genitori è mai stato mandato in prigione?», «quanti tuoi amici/conoscenti stanno assumendo droghe illegalmente?» e «quante volte hai litigato a scuola?». Il questionario chiede inoltre alle persone di essere d'accordo o in disaccordo con affermazioni come «una persona affamata ha il diritto di rubare» e «se le persone mi fanno arrabbiare o perdono la pazienza, posso essere pericoloso»[177].

Le domande predisposte dal *software* possono apparire quantomeno atipiche. Tuttavia, dalle risposte fornite dagli individui intervistati il COMPAS trae informazioni riguardo alla loro tendenza a delinquere, alla pericolosità sociale, alla possibilità di recidiva. Ebbene, tali risultanze paiono senza dubbio compatibili con quell'attività già svolta dai giudici dei nostri tribunali ai sensi dell'art. 133 c.p.: i criteri di valutazione descritti dalla norma in esame - il carattere e la vita del soggetto, le sue condizioni di vita individuale, familiare e sociale, eccetera - servono per individuare la capacità di delinquere del reo e, di conseguenza, l'attitudine dello stesso a commettere nuovi reati.

Pertanto, almeno con riferimento alla tipologia dei dati raccolti, pare che il sistema COMPAS non sia in contrasto con quella che è, generalmente, la valutazione del giudice-uomo.

Tuttavia, le critiche mosse a questo sistema riguardano, più che il punto di partenza, i suoi risultati.

---

176 Si veda la pagina *Wikipedia* relativa a COMPAS (*software*).

177 E. XINLAN, *137 Questions: Criminal Risk Assessment Algorithms as a Case Study for Data Ethics*, in *Stanford Rewired*, 2020, consultabile sul sito *web* https://stanfordrewired.com/post/137-questions.

Già nel 2014, l'allora procuratore generale degli Stati Uniti Eric Holder, riteneva che i sistemi predittivi potessero introdurre pregiudizi nei tribunali: « Sebbene queste misure siano state elaborate con le migliori intenzioni, sono preoccupato che inavvertitamente minino i nostri sforzi per garantire una giustizia individualizzata ed equa», ha affermato, aggiungendo, «possono esacerbare disparità ingiustificate che sono già troppo comuni nel nostro sistema di giustizia penale e nella nostra società»[178].

Anche a seguito di questo appello, una redazione indipendente, ProPublica[179], ha avviato un'indagine che ha evidenziato significative disparità razziali negli esiti dell'elaborazione di dati del software COMPAS.

Nell'ambito di questo studio sono stati presi in considerazione i punteggi di rischio assegnati a più di 7.000 persone arrestate in Florida, nel 2013 e nel 2014. Si è successivamente verificato quante sono state le persone effettivamente accusate di nuovi crimini nei due anni successivi.

È emerso come, in molti casi, gli imputati neri che erano stati contrassegnati dal *software* come «ad alto rischio di recidiva» non abbiano commesso nuovi crimini. Al contrario, alcuni imputati bianchi che erano stati (erroneamente) etichettati «a basso rischio» sono stati accusati di nuovi reati.

Ma le critiche non si fermano alla questione razziale. È stato, infatti, evidenziato che, essendo questo *software* di proprietà di una società privata, la struttura dell'algoritmo è coperta da segreto industriale. Questo elemento ha non poche conseguenze dal punto di vista dei risultati ottenuti dal software. Infatti, nel concepire l'architettura di un algoritmo, il programmatore fa delle scelte che necessariamente influenzano il risultato dell'operazione. Quando la struttura di un algoritmo è protetta da diritti di proprietà intellettuale, è sottratta alla possibilità di controllo, verifica e confutazione da parte del giudice, della difesa e, più in generale, della comunità degli utenti.

---

[178] Si veda, nel sito *web* del dipartimento di giustizia USA (www.justice.gov), il discorso di Eric Holder «*Attorney General Eric Holder Speaks at the National Association of Criminal Defense Lawyers 57th Annual Meeting and 13th State Criminal Justice Network Conference*».

[179] ProPublica è una redazione indipendente senza scopo di lucro con sede a New York City. Nel 2010 è diventata la prima fonte di notizie online a vincere un Premio Pulitzer. Per lo studio in esame si veda https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Paradigmatico è il caso Loomis[180], dal nome di un imputato che fece ricorso alla Corte Suprema del Wisconsin per contestare l'entità della pena che gli era stata inflitta dalla Corte locale, la quale si era per l'appunto avvalsa di COMPAS: la difesa del Loomis lamentava il difetto di trasparenza relativo al meccanismo di funzionamento del *software*. La Corte suprema del Wisconsin ha escluso che fosse possibile per la difesa di Loomis prendere in visione la struttura dell'algoritmo (trattandosi di prodotto protetto da diritti di proprietà intellettuale).

L'accusa principale di Loomis era che l'uso di COMPAS violasse il suo diritto a una sentenza basata su una valutazione individualizzata. Sosteneva inoltre che il *software* avesse preso in considerazione il suo genere, potenzialmente discriminandolo, senza possibilità per lui di contestare direttamente il funzionamento dell'algoritmo, per via del segreto industriale.

Sia le corti del Wisconsin che la Corte Suprema degli Stati Uniti rigettarono le sue istanze, sottolineando che i giudici avevano la possibilità di valutare criticamente i risultati di COMPAS e di prendere decisioni autonome rispetto a queste valutazioni[181]. Tuttavia, venne riconosciuto che COMPAS non poteva produrre risultati individualizzati, ma basati su gruppi di individui con caratteristiche simili.

In questa sede la Corte suprema ha anche precisato che l'esito dell'algoritmo predittivo – avendo un rilievo statistico – non può costituire l'unico criterio deliberativo, essendo diritto dell'imputato l'essere destinatario di una decisione individualizzata[182].

---

[180] Wisconsin S.C., State v. Loomis, 881, N.W.2d 749 (2016). Per un approfondimento si veda K. FREEMAN, *Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in State v. Loomis*, in *North Carolina Journal of Law & Technology*, 18/2016, p. 76 ss.

[181] In particolare, a pagina 764 della sentenza si legge: «*If a COMPAS risk assessment were the determinative factor considered at sentencing this would raise due process challenges regarding whether a defendant received an individualized sentence. As the defense expert testified at the post-conviction motion hearing, COMPAS is designed to assess group data. He explained that COMPAS can be analogized to insurance actuarial risk assessments, which identify risk among groups of drivers and allocate resources accordingly; Just as corrections staff should disregard risk scores that are inconsistent with other factors, we expect that circuit courts will exercise discretion when assessing a COMPAS risk score with respect to each individual defendant. [Ultimately, we disagree with Loomis because consideration of a COMPAS risk assessment at sentencing along with other supporting factors is helpful in providing the sentencing court with as much information as possible in order to arrive at an individualized sentence*]».

[182] A. NATALE, *Introduzione. Una giustizia (im)prevedibile?*, cit.

Tuttavia, alla luce delle criticità emerse, perché ciò sia possibile occorre, innanzitutto, assicurarsi che l'intelligenza artificiale agisca correttamente, nel rispetto dell'uguaglianza di tutti i cittadini di fronte alla legge e del diritto di difesa.

Un caso simile fu quello *Ewert v. Canada* del 2017[183]. Jeffrey Ewert, un prigioniero appartenente a una popolazione indigena del Canada, contestava l'uso di strumenti psicologici per la profilazione e la valutazione del rischio da parte del *Correctional Service of Canada* (*CSC*). Ewert sosteneva che questi strumenti, sviluppati principalmente su popolazioni non indigene, non fossero affidabili per essere usati nei confronti di membri delle minoranze etniche.

La Corte Suprema canadese ha accolto le argomentazioni di Ewert, affermando che il *CSC* non aveva condotto sufficienti verifiche sull'affidabilità di questi strumenti quando utilizzati per persone appartenenti a minoranze culturali ed etniche. La sentenza ha messo in luce il rischio di discriminazioni sistemiche, poiché le minoranze indigene, statisticamente, tendono a ricevere pene più severe e valutazioni di rischio peggiori rispetto ad altri gruppi etnici. In questo modo, l'introduzione di strumenti tecnologici nel processo decisionale giudiziario potrebbe aggravare questi pregiudizi, nascondendoli dietro l'apparente oggettività tecnica degli algoritmi[184].

A differenza del caso Loomis, dove la corte americana ha mostrato grande fiducia nella capacità dei giudici di interpretare e correggere i risultati degli algoritmi, la Corte Suprema canadese ha adottato un approccio più prudente e consapevole, evidenziando la necessità di una rigorosa verifica della qualità delle tecnologie impiegate.

---

[183] *Ewert v. Canada*, 2018 SCC 30 [2018] 2 S.C.R. 165.

[184] V. *Ewert v. Canada*, par. 65-66: «*The clear danger posed by the CSC's continued use of assessment tools that may overestimate the risk posed by Indigenous inmates is that it could unjustifiably contribute to disparities in correctional outcomes in areas in which Indigenous offenders are already disadvantaged. For example, if the impugned tools overestimate the risk posed by Indigenous inmates, such inmates may experience unnecessarily harsh conditions while serving their sentences, including custody in higher security settings and unnecessary denial of parole. Overestimation of the risk may also contribute to reduced access to rehabilitative opportunities, such as a loss of the opportunity to benefit from a gradual and structured release into the community on parole before the expiry of a fixed-term sentence. Another effect of an overestimation of the risk is that it could bar an inmate from participation in Indigenous-specific programming that is contingent on an offender having a low security classification or being eligible for an escorted temporary absence […] In the context of the case at bar, this required, at the very least, that the CSC take seriously the credible concerns that have been repeatedly raised according to which information derived from the impugned tools is of questionable validity with respect to Indigenous inmates because the tools fail to account for cultural differences*».

Secondo la Corte, gli strumenti tecnologici dovrebbero servire a mitigare i pregiudizi presenti nelle decisioni giudiziarie, e non bisognerebbe affidarsi ai giudici per neutralizzare i *bias* che gli algoritmi stessi potrebbero introdurre.

Questa decisione riflette una maggiore consapevolezza delle sfide legate all'uso dell'IA nei sistemi giudiziari e invita a una maggiore trasparenza e responsabilità nell'adozione di questi strumenti.

Nonostante i rischi associati e le frequenti espressioni di scetticismo da parte dei giuristi, che sottolineano la necessità di cautela nel rispetto delle garanzie durante la raccolta di informazioni per la valutazione del rischio e malgrado le preoccupazioni riguardanti le implicazioni legali e etiche, si assiste ad una rapida diffusione delle tecniche predittive.

Per tale ragione la comunità internazionale sta ponendo grande attenzione a garantire che l'arricchimento delle fonti informative a disposizione del giudice e le predizioni generate dai *software* siano sempre conformi ai principi fondamentali del giusto processo[185]. L'obiettivo è assicurare che l'innovazione tecnologica nel campo delle previsioni giudiziarie non comprometta le garanzie tradizionali di equità e trasparenza che costituiscono il cuore del sistema legale.

In conclusione, a parere di chi scrive non possono trascurarsi le potenzialità dei sistemi predittivi. Se un sistema di intelligenza artificiale potesse prevedere con precisione quali imputati commetteranno nuovi crimini e quali no, ciò potrebbe portare ad un sistema di giustizia penale più equo e più selettivo, con degli importanti (e ad oggi fondamentali) effetti deflattivi.

A tal fine, un ruolo fondamentale gioca la possibilità di verificare il processo decisionale del *software*: così come il giudice-uomo è tenuto a motivare accuratamente il percorso logico-argomentativo seguito per la formazione del suo convincimento, il giudice-artificiale non può esimersi dal fare altrettanto.

---

[185] Sul punto, la «*Carta etica sull'uso dell'intelligenza artificiale nei sistemi giudiziari e nel loro ambiente*», adottata il 3 dicembre 2018 dalla Commissione europea per l'efficienza dei sistemi di giustizia (CEPEJ) ha sancito il principio secondo il quale la coerenza logica del calcolo algoritmico deve sempre essere verificata in un processo d'integrazione fra le misurazioni quantitative, ricche e imponenti, da esso offerte con il percorso cognitivo e decisorio del giudice, nel rispetto dei valori dell'ordinamento.

4. La discriminazione algoritmica

Dall'analisi svolta è possibile dedurre che l'integrazione di tecnologie digitali in diversi settori ha ridotto significativamente l'errore umano e ha migliorato la precisione, velocità e uniformità dei risultati. Specialmente a partire dalla rivoluzione industriale, le macchine hanno automatizzato, totalmente o parzialmente, molte attività, consentendo una produzione di massa più efficiente e standardizzata.

In passato, i prodotti erano realizzati manualmente da artigiani, il che li rendeva unici ma anche costosi e spesso difettosi. L'automazione ha reso questi beni più accessibili, abbassando i costi e garantendo una maggiore uniformità. Inoltre, le macchine non sono soggette agli errori tipici degli esseri umani, come quelli dovuti alla fatica o alle distrazioni, contribuendo così a ridurre i difetti di lavorazione. Questo fenomeno non si è limitato all'industria manifatturiera, ma si è esteso anche ad altri settori, come quello sanitario e dei servizi, in cui l'automazione ha migliorato la qualità e l'efficienza dei processi[186].

Anche lo sviluppo del *computer* ha rivoluzionato molte attività, rendendole più precise, semplici e meno soggette a errori, grazie alla possibilità di automatizzare operazioni complesse come il calcolo, la progettazione, la scrittura, il disegno e l'archiviazione di informazioni. Tutto ciò ha creato una percezione diffusa di efficienza e

[186] Si parla in questo caso di rivoluzione informatica o di «quarta rivoluzione industriale». Per un approfondimento v. G. PIERACCINI, *La Costituzione e la rivoluzione informatica*, in *Rassegna Parlamentare*, 1/1997, p. 13 ss.; S. CHIARLONI, *Giurisprudenza e dottrina nell'era della rivoluzione informatica (note sui sistemi di documentazione)*, in *Riv. dir. proc.*, 2/1992, p. 590 ss.; F. LAVIOLA, *Regolazione della tecnologia e dimensione del tempo*, in *Osservatorio sulle fonti*, 3/2021, p. 1163 ss.; A. PUNZI, *Il dialogo delle intelligenze tra umanesimo e tecnoscienza*, in Persona e Mercato, 2/2023, p. 161 ss.; C. ROMEO, *L'era degli algoritmi e la sua incidenza nell'ambito della certezza del diritto: un connubio sospetto*, in *Law. giur.*, 1/2024, p. 5 ss.; F. TRAPELLA, *La rivoluzione digitale alla prova della riforma*, in *Arch. pen.*, 3/2022, p. 999 ss.; A. F. SPAGNUOLO, E. SORRENTINO, *Alcune riflessioni in materia di trasformazione digitale come misura di semplificazione*, in *federalismi.it*, 8/2021, p. 275 ss.; V. FALCE, G. FINOCCHIARO, *La "digital revolution" nel settore finanziario. Una nota di metodo*, in *Analisi Giuridica dell'Economia*, 1/2019, p. 313 ss. Per alcuni spunti sul tema del presente paragrafo v. G. GIORGINI PIGNATIELLO, *Il contrasto alle discriminazioni algoritmiche: dall'anarchia giuridica alle "Digital Authorities"?*, in *federalismi.it*, 16/2021, p. 114 ss.

affidabilità nelle tecnologie digitali, che si è estesa anche alle tecnologie più recenti legate all'intelligenza artificiale.

Tuttavia, i sistemi di IA, soprattutto quelli che utilizzano il *machine learning*, sono progettati per analizzare enormi quantità di dati e fornire soluzioni o previsioni basate su modelli statistici derivati dall'elaborazione di precedenti simili. Sebbene questi sistemi possano trattare una mole di dati impensabile per un essere umano, il risultato prodotto è sempre legato a un certo margine d'errore, per quanto piccolo. Questo è dovuto al fatto che, anche se estremamente precisi, gli algoritmi non sono infallibili e le loro indicazioni possono sempre essere migliorate. Ciò li differenzia dalle tecnologie precedenti, come il *personal computer*, dove l'errore era prevalentemente umano e poteva essere corretto direttamente dall'utente.

Inoltre, poiché i sistemi di IA prendono decisioni e svolgono valutazioni complesse, la loro percezione di neutralità è spesso più ambigua rispetto a tecnologie più tradizionali. Gli algoritmi, infatti, riflettono i dati con cui sono stati addestrati, e questi possono contenere pregiudizi o limiti che influiscono sulle loro *performance*, rendendo il problema dell'accuratezza più profondo rispetto alle tecnologie basate su calcoli o operazioni semplici.

Non solo l'IA viene percepita come più neutrale e obiettiva di quanto in realtà non sia, ma le persone tendono anche ad accettare le sue indicazioni in modo meno critico rispetto ad altre tecnologie. Questo comportamento ha implicazioni gravi a lungo termine, poiché rischia di portare a una perdita delle competenze e conoscenze necessarie per prendere decisioni in autonomia, senza l'ausilio dell'intelligenza artificiale, creando una vera e propria dipendenza da essa che potrebbe compromettere la capacità di affrontare situazioni non prevedibili o insolite.

L'adozione e l'uso dell'intelligenza artificiale nei processi decisionali richiederà in futuro un grande sforzo di sensibilizzazione, soprattutto per contrastare alcune tendenze culturali che favoriscono una fiducia eccessiva nelle macchine. Studi recenti hanno evidenziato un fenomeno noto come «distorsione dell'automazione», secondo il quale le persone, affiancate da strumenti di IA, tendono a fare troppo affidamento

sulle decisioni della macchina, riducendo progressivamente la loro attenzione e la capacità di analizzare criticamente le informazioni fornite[187].

Sul punto si è espresso anche il Consiglio di Stato nel 2019, affermando che «In molti campi gli algoritmi promettono di diventare lo strumento attraverso il quale correggere le storture e le imperfezioni che caratterizzano tipicamente i processi cognitivi e le scelte compiute dagli esseri umani, messe in luce soprattutto negli ultimi anni da un'imponente letteratura di economia comportamentale e psicologia cognitiva. In tale contesto, le decisioni prese dall'algoritmo assumono così un'aura di neutralità, frutto di asettici calcoli razionali basati su dati»[188].

Alla luce di questo fenomeno, il rischio principale è che gli errori generati dal *software* possano essere meno evidenti e più difficili da identificare. In particolare, tra questi errori meritano attenzione i c.d. *bias* algoritmici, ovvero quegli errori che portano un algoritmo a produrre risultati non neutrali, spesso generando discriminazioni[189].

---

[187] Questo concetto è esplicato nell'opera A. GARAPON, J. LASSEGUE, *Justice Digitale: révolution-graphique et ruptureanthropologique*, PUF, Parigi, 2018. In particolare, gli autori parlano di effetto «*moutonnier*», da tradurre come effetto «pecorone». Per un approfondimento sul tema v. E. FRONZA, *"Code is Law". Note a margine del volume di Antoine Garapon e Jean Lassègue, Justice Digitale. Révolution graphique et rupture anthropologique*, in *Dir. pen. cont.*, 11 dicembre 2018. Parte della dottrina ritiene che questo fenomeno possa essere arginato grazie alla previsione di una integrazione attiva e continua dell'essere umano nei processi decisionali e operativi controllati da sistemi automatizzati o basati sull'intelligenza artificiale. Si parla in questo caso di «*human in the loop*»: «l'essere umano nel circolo» contribuisce a mitigare i rischi legati a un eccessivo affidamento sulla tecnologia e garantisce che i sistemi agiscano in modo etico e sicuro. Sul punto v. P. BENANTI, *Human in the loop. Decisioni umane e intelligenze artificiali*, Mondadori, Milano, 2022; I. P. DI CIOMMO, *La prospettiva del controllo nell'era dell'Intelligenza Artificiale: alcune osservazioni sul modello "Human In The Loop"*, in *federalismi.it*, 9/2023, p. 68 ss.; D. GALETTA, *"Human-stupidity-in-the-loop"? Riflessioni (di un giurista) sulle potenzialità e i rischi dell'Intelligenza Artificiale*, in *federalismi.it*, 5/2023, p. 4 ss.; V. BERLINGÒ, *Per una rilettura dei servizi di "Vessel Traffic Service" (VTS) e di pilotaggio alla luce delle implicazioni giuridiche del metodo matematico dell'HITL ("Human in the Loop")*, in *Dir. mar.*, 4/2022, p. 694 ss.

[188] v. Consiglio di Stato, sez. VI, 13 dicembre 2019, n. 8474, par. 7.1.

[189] Per un approfondimento v. D. MORONDO TARAMUNDI, *Le sfide della discriminazione algoritmica*, in *GenIUS*, 1/2022, p. 22 ss.; P. DUNN, *Moderazione automatizzata e discriminazione algoritmica: il caso dell'"hate speech"*, in *Inf. dir.*, 1/2022, 2, p. 133 ss.; G. CARAPEZZA FIGLIA, *Decisioni algoritmiche tra diritto alla spiegazione e divieto di discriminare*, in *Persona e Mercato*, 4/2023, p. 638 ss.; N. LETTIERI, *La discriminazione nell'era delle macchine intelligenti. Modelli possibili di analisi, critica e tutela*, in *GenIUS*, 1/2022, p. 10 ss.; M. BARBERA, *Discriminazioni algoritmiche e forme di discriminazione*, in *Labour & Law Issues*, 1/2021, p. 3 ss.; B. BALDINI, *Città intelligenti, decisioni "biased" e rischi di esclusione*, in *federalismi.it*, 10/2024, p. 1

Ancora il Consiglio di Stato, al riguardo, ha precisato che «è emersa altresì una lettura critica del fenomeno, in quanto l'impiego di tali strumenti comporta in realtà una serie di scelte e di assunzioni tutt'altro che neutre: l'adozione di modelli predittivi e di criteri in base ai quali i dati sono raccolti, selezionati, sistematizzati, ordinati e messi insieme, la loro interpretazione e la conseguente formulazione di giudizi sono tutte operazioni frutto di precise scelte e di valori, consapevoli o inconsapevoli; da ciò ne consegue che tali strumenti sono chiamati ad operare una serie di scelte, le quali dipendono in gran parte dai criteri utilizzati e dai dati di riferimento utilizzati, in merito ai quali è apparso spesso difficile ottenere la necessaria trasparenza»[190].

Il termine *bias* originariamente indicava qualsiasi deviazione rispetto a uno *standard* di riferimento, ma nel contesto dell'algoritmica e dell'intelligenza artificiale, ha assunto una connotazione negativa legata alla discriminazione[191].

Un *bias* può sorgere già nel momento della programmazione del *software*, quando i dati utilizzati per addestrare un algoritmo sono sbilanciati, ovvero contengono una rappresentazione errata o incompleta di alcune variabili.

Inoltre, un algoritmo può funzionare correttamente nel contesto per cui è stato addestrato, ma generare errori o discriminazioni quando viene impiegato in un ambiente diverso[192]. Tra l'altro, è possibile che attraverso il *software* vengano riprodotti e amplificati i pregiudizi già presenti nella società. Un sistema progettato per automatizzare le selezioni lavorative, basato su decisioni prese storicamente dalle aziende, potrebbe, ad esempio, discriminare le donne se riflette la scarsa presenza femminile in ruoli dirigenziali.

---

ss.; M. A. WÓJCIK-SUFFIA, *Algorithmic Discrimination in M-Health: Rethinking the US Nondiscrimination Legal Framework Through the Lens of Intersectionality*, in *BioLaw Journal*, 1/2024, p. 367 ss.; A. INGRAO, *Critica della ragione artificiale. La discriminazione algoritmica intersezionale e gli obblighi di parità di trattamento in ipotesi di impiego di sistemi decisionali automatizzati*, in *Riv. giur. lav.*, 2/2024, p. 170 ss. Infine, si veda anche il *Report* della *European Union Agency for Fundamental Rights* (*FRA*), *Bias in algorithms artificial intelligence and discrimination*, 8 dicembre 2022, consultabile sul sito *web* www.fra.europa.eu.

[190] v. Consiglio di Stato, 13 dicembre 2019, n. 8474, cit., par. 7.2.

[191] Il temine *bias* deriva dal francese *biais*, che significa orientamento, piega, inclinazione. V. *Bias*, in *Treccani vocabolario online*. Sul tema v. D. KAHNEMAN, A. TWERSKY, P. SLOVIC, *Judgment under uncertainity. Heuristics and biases*, cit.

[192] Ad esempio, un sistema di guida autonoma addestrato in un paese con guida a destra potrebbe avere difficoltà se utilizzato in un paese con guida a sinistra.

Le discriminazioni, come sappiamo, sono vietate quantomeno nel rapporto tra il cittadino e l'autorità grazie all'applicazione del principio di uguaglianza *ex* art. 3 Cost[193].

Il principio di eguaglianza negli ordinamenti democratici ha, infatti, solitamente una valenza verticale: ciò significa che il Legislatore e le autorità pubbliche sono vincolati da questo principio, il quale impedisce loro di adottare comportamenti discriminatori o di trattare i cittadini in modo arbitrariamente differenziato senza una giustificazione ragionevole. Il Legislatore non può creare leggi che trattino gruppi o individui in modo discriminatorio senza una ragione fondata su esigenze giuridiche o sociali legittime. Allo stesso modo, le autorità amministrative, pur avendo una discrezionalità nelle loro decisioni, devono agire secondo criteri di eguaglianza, evitando trattamenti differenziati immotivati.

Diversamente, i privati non sono vincolati nello stesso modo al rispetto del principio di eguaglianza nelle loro scelte personali e nelle attività quotidiane. Un individuo può scegliere con chi interagire in base a preferenze personali, come l'aspetto fisico, le credenze religiose o altri fattori.

---

193 Per una disamina generale sul principio di uguaglianza nella costituzione e la sua applicazione nel diritto penale v., *ex multis*, G. DODARO, *Uguaglianza e diritto penale. Uno studio sulla giurisprudenza costituzionale*, Giuffrè, Milano, 2012; A. DE LIA, *Il principio di uguaglianza ed il diritto penale sostanziale: una sintetica analisi del rapporto*, in *federalismi.it*, 23/2017, p. 15 ss.; C. ROSSANO. *L'eguaglianza giuridica nell'ordinamento costituzionale*, Jovene, Napoli, 1966; A. GIORGIS, *La costituzionalizzazione dei diritti all'uguaglianza sostanziale*, Jovene, Napoli, 1999; N. BOBBIO, *Eguaglianza e libertà*, Einaudi, Torino, 1995; A. CERRI, *L'eguaglianza*, Laterza, Bari, 2005; P. MOROZZO DELLA ROCCA, *Principio di uguaglianza e divieto di compiere atti discriminatori*, Edizioni Scientifiche Italiane, Napoli, 2002; L. FERRAJOLI, *Sul significato del principio di uguaglianza. Una replica*, in *Notizie di Politeia*, 133/2019, p. 259 ss.; L. GIACOMELLI, *Ripensare l'eguaglianza. Effetti collaterali della tutela antidiscriminatoria*, Giappichelli, Torino, 2018; D. CARUSI, *Principio di eguaglianza, diritto singolare e privilegio*, Edizioni Scientifiche Italiane, Napoli, 1998; C. STARCK, *L'applicazione del principio di uguaglianza*, in *Dir. soc.*. 2/1985, p. 237 ss.; A. GALASSO, *Il principio di uguaglianza nella Costituzione europea. Diritti fondamentali e rispetto della diversità*, Franco Angeli, Milano, 2007; A. CERRI, *Appunti sul sindacato di costituzionalità relativo al principio di eguaglianza*, in *Giur. cost.*, 3/1973, p. 860 ss.; C. GIORGI, *Il progetto costituzionale dell'uguaglianza*, Futura, Perugia, 2014; M. MILITELLO, *Principio di uguaglianza e di non discriminazione tra Costituzione italiana e Carta dei diritti fondamentali dell'Unione Europea*, in *Rassegna di diritto pubblico europeo*, 1/2010, p. 85 ss.; M. F. DE TULLIO, *Uguaglianza sostanziale e nuove dimensioni della partecipazione politica*, Editoriale Scientifica, Napoli, 2020.

Tuttavia, vi sono normative specifiche che limitano alcune forme di discriminazione anche nei rapporti tra privati[194]. Le esigenze di tutela dell'eguaglianza hanno portato alla creazione di vincoli significativi all'autonomia privata, con l'introduzione di norme che limitano la possibilità dei privati di discriminare su base sessuale, razziale, religiosa.

Fin dagli anni '70, l'UE ha adottato numerose direttive per armonizzare le leggi degli Stati membri in materia di discriminazione sul lavoro. Una delle prime preoccupazioni fu promuovere l'occupazione femminile e garantire la parità di trattamento tra uomini e donne, vietando ogni tipo di discriminazione sessuale nell'ambito lavorativo, dalle assunzioni al pensionamento[195]. A livello internazionale, diverse convenzioni hanno ulteriormente rafforzato la protezione contro le discriminazioni, molte delle quali elaborate nell'ambito dell'Organizzazione Internazionale del Lavoro (OIL), che ha sviluppato *standard* specifici in materia di parità di trattamento nel mondo del lavoro[196].

A partire dagli anni 2000, l'Unione ha esteso il divieto ad altri tipi di discriminazioni, come quelle basate su origine etnica, età, orientamento sessuale, religione, convinzioni politiche e disabilità[197]. Queste normative non si limitano al contesto

---

[194] Per esempio, i licenziamenti per motivi esclusivamente religiosi o legati al genere e all'orientamento sessuale sono vietati.

[195] Per un approfondimento sul principio di uguaglianza applicato ai rapporti di lavoro v. A. PERULLI, *Discriminazione e lavoro autonomo nella prospettiva della Corte di Giustizia*, in *Labor*, 4/2023, p. 408 ss.; E. M. INCUTTI, *Il principio di non discriminazione nei rapporti contrattuali di lavoro autonomo*, in *Nuova giur. civ. comm.*, 6/2023, p. 1241 ss.; E. TRIGGIANI, *Osservazioni sulla discriminazione in materia di lavoro nel diritto internazionale e nel diritto interno*, in *Riv. trim. dir. pubbl.*, 4/1976, p. 1526 ss.; V. BERTI, *Osservatorio di giurisprudenza e politiche comunitarie del lavoro - Non discriminazione e pari opportunità: un impegno rinnovato a livello comunitario*, in *Dir. relaz. ind.*, 4/2008, p. 1227 ss.; A. CAPROTTI, *L'effettività del principio di non discriminazione sul luogo di lavoro: un discorso in continua evoluzione*, in *DPCE online*, 4/2018, p. 1159 ss.; S. MAGAGNOLI, *Divieti di discriminazione e lavoro autonomo: un primo passo nella ridefinizione dei confini del diritto del lavoro*, in *Dir. relaz. ind.*, 2/2023, p. 544 ss.

[196] Ad esempio, la Convenzione n. 111 dell'OIL, del 1958, vieta ogni forma di discriminazione in materia di impiego e professione.

[197] Il quadro normativo si è consolidato con la Direttiva 2000/43/CE e la Direttiva 2000/78/CE, che rappresentano i pilastri del diritto antidiscriminatorio europeo. Alcune delle principali Direttive UE sul tema, dalla meno recente: Direttiva 2000/43/CE, vieta la discriminazione basata sulla razza e sull'origine etnica in vari settori, incluso l'impiego. Si applica sia al settore pubblico che a quello privato e copre l'accesso al lavoro, le condizioni di impiego, e la formazione

lavorativo, ma coprono anche altri ambiti, tra cui l'accesso a servizi essenziali come la sanità, l'istruzione e l'assistenza sociale[198].

In Italia, fu rilevante l'introduzione nel 1993 della Legge Mancino, finalizzata a sanzionare atti di discriminazione razziale, etnica e religiosa[199]. La normativa prevede pene detentive e pecuniarie per atti di violenza e istigazione alla violenza per motivi di discriminazione razziale, etnica o religiosa. Viene punito non solo chi commette atti di discriminazione o violenti, ma anche chiunque faccia parte di organizzazioni, associazioni o movimenti che perseguono tali finalità.

---

professionale; Direttiva 2000/78/CE, vieta ogni forma di discriminazione basata su religione, convinzioni personali, disabilità, età e orientamento sessuale; Direttiva 2004/113/CE, estende il principio di parità di trattamento tra uomini e donne all'accesso a beni e servizi, inclusi i servizi essenziali come la sanità e la protezione sociale; Direttiva 2006/54/CE, relativa all'attuazione del principio delle pari opportunità e della parità di trattamento fra uomini e donne in materia di occupazione e impiego; Direttiva 2006/123/CE, contribuisce a migliorare l'accesso ai servizi, compresi alcuni servizi sociali, rendendo più facile la prestazione transfrontaliera di servizi all'interno dell'UE, inclusi i servizi educativi e sanitari; Direttiva 2010/41/UE, riguarda l'uguaglianza di trattamento tra uomini e donne nell'attività autonoma, con particolare riferimento alla protezione sociale durante la maternità; Direttiva 2011/24/UE, garantisce ai cittadini dell'UE il diritto di accedere a cure sanitarie in altri Stati membri dell'Unione, include il rimborso delle cure ricevute all'estero e stabilisce le regole per il coordinamento tra i sistemi sanitari nazionali; Direttiva 2019/1158 (Direttiva *Work-Life Balance*), mira a migliorare l'equilibrio tra vita privata e professionale per genitori e prestatori di assistenza, promuove la parità di genere e vieta qualsiasi discriminazione legata all'esercizio dei diritti familiari o di cura.

[198] Con riferimento all'applicazione del principio di eguaglianza alla salute v. S. ROSSI, *Il diritto alla salute tra equità e sostenibilità. Colloquio sulle forme dell'eguaglianza in sanità*, in *BioLaw Journal*, 2/2019, p. 7 ss.; A. PIOGGIA, *Il diritto alla salute alla prova della differenziazione: autonomie, organizzazione e diseguaglianza*, in *Istit. federalismo*, 1/2020, p. 37 ss.; I. CIOLLI, *La salute come diritto in movimento. Eguaglianza, universalismo ed equità nel sistema sanitario nazionale, oggi*, in *BioLaw Journal*, 2/2019, p. 13 ss.; S. GAMBINO, *Stato regionale, principio di eguaglianza, diritti sociali. Problematiche di effettività con particolare riguardo alla tutela della salute*, in *DPCE online*, 2/2021, p. 2461 ss. Per quanto attiene, invece, all'istruzione v. A. LAURO, *Un "devoir de justice": le sfide dell'uguaglianza nel diritto all'istruzione scolastica*, in *Costituzionalismo.it*, 1/2023, p. 27 ss.; S. PUDDU, *Diritto all'istruzione e contrasto alle diseguaglianze: profili amministrativistici e spunti dall'agenda 2030*, in *Dir. e proc. amm.*, 1/2024, p. 181 ss.; R. CALVANO, *L'istruzione, il Covid-19 e le diseguaglianze*, in *Costituzionalismo.it*, 3/2020, p. 57 ss.

[199] La Legge n. 205 del 25 giugno 1993 prende il nome dall'allora Ministro dell'Interno, Nicola Mancino. Recentemente c'è stato un tentativo di estendere la portata di questa legge anche ai reati di omo-transfobia. Questa proposta, nota come DDL Zan, mirava ad estendere le tutele della Legge Mancino anche ai reati di discriminazione e violenza basati sull'orientamento sessuale e sull'identità di genere, oltre che alla misoginia e alla disabilità, grazie a emendamenti introdotti durante la discussione parlamentare. La legge è stata approvata alla Camera dei deputati il 4 novembre 2020 con 265 voti favorevoli, 193 contrari e un astenuto, ma non è stata approvata dal Senato durante la seduta del 27 ottobre 2021.

Da questa disamina emerge che i privati non sono soggetti al principio di eguaglianza come lo sono i poteri pubblici – che sono obbligati a trattare i cittadini in modo imparziale sempre e comunque – ma sono, tuttavia, tenuti a rispettare specifici divieti di discriminazione stabiliti dalla legge nazionale o sovranazionale. Questo comporta delle notevoli conseguenze in tema di discriminazione algoritmica, dato che i *software* in esame spesso sono sviluppati e gestiti da attori privati. Nel paragrafo precedente abbiamo già analizzato alcuni casi di cronaca che hanno visto al centro del processo proprio l'utilizzo di un algoritmo di proprietà di un'azienda privata[200].

Una prima ipotesi per affrontare il problema della discriminazione algoritmica potrebbe essere quello di aggiornare le leggi esistenti, al fine di meglio adeguarle alla natura privatistica dei sistemi di IA, tenendo conto di tutte le loro caratteristiche peculiari.

Tuttavia, un aspetto da considerare è che il problema principale delle tecnologie prima analizzate, come illustrato nei casi *Ewert* e *Loomis*, non riguarda tanto la creazione di nuove forme di discriminazione, ma piuttosto il rischio che le disparità tradizionali vengano occultate da decisioni apparentemente neutre. Gli algoritmi potrebbero infatti basarsi su dati viziati, mantenendo o addirittura amplificando discriminazioni già esistenti.

Di conseguenza, la regolamentazione della discriminazione algoritmica dovrebbe concentrarsi innanzitutto sulla necessità di minimizzare la presenza di *bias* negli algoritmi, anche garantendo che gli sviluppatori e gli utilizzatori mettano in atto meccanismi per ridurre al minimo i pregiudizi nascosti nei dati che alimentano questi sistemi. Poiché gli algoritmi imparano dai dati esistenti, è cruciale che questi siano «puliti».

Inoltre, qualora queste misure prese a monte non siano sufficienti, sarà essenziale poter identificare e correggere eventuali decisioni discriminatorie. Questo potrebbe richiedere una maggiore trasparenza nei meccanismi decisionali automatizzati e la possibilità per individui e istituzioni di contestare le scelte prese dagli algoritmi.

---

[200] V. le sentenze della Corte Suprema USA *Ewert* e *Loomis* descritte nel paragrafo precedente.

Il GDPR regola l'utilizzo delle tecnologie di IA nei processi decisionali automatizzati attraverso l'art. 22 e il Considerando 71[201]. In particolare, l'art. 22 sancisce il diritto degli individui a non essere soggetti a decisioni esclusivamente basate su processi automatizzati, salvo alcune eccezioni. Queste eccezioni includono situazioni in cui vi è il consenso dell'interessato oppure la scelta è necessaria per l'esecuzione di un contratto o è autorizzata dalla legge. Anche in questi casi, l'individuo ha il diritto di richiedere un intervento umano, esprimere la propria opinione e contestare la decisione[202].

Il Considerando 71 rafforza queste disposizioni, stabilendo che il titolare del trattamento deve adottare misure tecniche e organizzative adeguate a correggere eventuali inesattezze nei dati e ridurre il rischio di errori. Queste valutazioni devono anche evitare effetti discriminatori basati su fattori come razza, origine etnica, opinioni politiche, religione, orientamento sessuale o stato di salute. Nonostante la natura interpretativa di questa norma, essa evidenzia l'intenzione di ridurre al minimo i *bias* che possono portare a discriminazioni attraverso l'uso delle tecnologie di IA[203].

---

[201] Per un commento su questi aspetti del GDPR v. F. RAGNO, *Il diritto fondamentale alla tutela dei dati personali e la dimensione transnazionale del "private enforcement" del GDPR*, in *OIDU - Ordine Internazionale e Diritti Umani*, 4/2020, p. 818 ss.; E. FALLETTI, *Alcune riflessioni sull'applicabilità dell'art. 22 GDPR ["General Data Protection Regulation" - Regolamento generale sulla protezione dei dati] in materia di "scoring" creditizio*, in *Dir. inform.*, 1/2024, p. 110 ss.; G. M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, 2018; P. FALLETTA, A. MARSANO, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR*, in *Inf. dir.*, 1/2024, p. 119 ss.; A. ODDENINO, *Decisioni algoritmiche e prospettive internazionali di valorizzazione dell'intervento umano*, in *DPCE online*, 1/2020, p. 199 ss.; A. ORTALDA, S. LEUCCI, *Identità digitale e protezione dei dati personali: punti di incontro e rischi nelle discipline eIDAS e RGPD*, in *Inf. dir.*, 1/2022, p. 145 ss.

[202] L'art. 22 del GDPR recita: «1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. 2. Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato. 3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione».

[203] Il Considerando 71 del GDPR recita: «L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo

Anche l'*AI Act* affronta il tema dei rischi di discriminazione algoritmica, in particolare per quanto riguarda la protezione dei diritti fondamentali e la necessità di garantire che i sistemi di intelligenza artificiale siano affidabili, trasparenti e privi di pregiudizi[204].

Il Considerando 31 si concentra sui già citati *risk assesment tools*, classificati come sistemi ad alto rischio. Il testo sottolinea che, per prevenire risultati discriminatori e ingiusti, è essenziale che tali sistemi siano progettati, sviluppati e implementati in modo da minimizzare il rischio di distorsioni nei processi decisionali automatizzati. Stabilisce la necessità di controlli rigorosi per evitare che i sistemi di IA perpetuino pregiudizi e discriminazioni, proteggendo così i diritti fondamentali degli individui nell'uso di queste tecnologie[205].

---

riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani. […] Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti».

[204] Sul punto v. F. FEDORCZYK, *Addressing AI-driven gender discrimination: the role of the forthcoming EU AI Act and Corporate Social Responsibility*, in *Rivista di Diritti Comparati*, 3/2023, p. 239 ss.; C. NARDOCCI, *Artificial Intelligence-based Discrimination: Theoretical and Normative Responses. Perspectives from Europe*, in *DPCE online*, 3/2023, p. 2367 ss.; Il Considerando 7 dell'*AI Act* afferma che «Al fine di garantire un livello costante ed elevato di tutela degli interessi pubblici in materia di salute, sicurezza e diritti fondamentali, è opportuno stabilire regole comuni per i sistemi di IA ad alto rischio. Tali regole dovrebbero essere coerenti con la Carta, non discriminatorie e in linea con gli impegni commerciali internazionali dell'Unione. Dovrebbero inoltre tenere conto della dichiarazione europea sui diritti e i principi digitali per il decennio digitale e degli orientamenti etici per un'IA affidabile del gruppo di esperti ad alto livello sull'intelligenza artificiale (*AI HLEG*)».

[205] Al Considerando 31, infatti, il Regolamento prevede un divieto per quei sistemi di IA che permettono ad attori pubblici o privati di attribuire un punteggio sociale alle persone fisiche, affermando che questi ultimi «possono portare a risultati discriminatori e all'esclusione di determinati gruppi. Possono inoltre ledere il diritto alla dignità e alla non discriminazione e i valori di uguaglianza e giustizia. Tali sistemi di IA valutano o classificano le persone fisiche o i gruppi di persone fisiche sulla base di vari punti di dati riguardanti il loro comportamento sociale in molteplici contesti o di

Il Considerando 67 affronta invece il tema dell'uso dei dati per l'addestramento degli algoritmi di intelligenza artificiale. In particolare, sottolinea come sia fondamentale che i *set* di dati utilizzati per il *training*, *testing* e convalida degli algoritmi siano di alta qualità, pertinenti e rappresentativi per evitare i *bias*, al fine di evitare che queste distorsioni si traducano in risultati discriminatori o dannosi. Inoltre, stabilisce che la raccolta e l'uso di questi dati devono rispettare le normative esistenti sulla protezione dei dati e i diritti fondamentali, specialmente quando gli algoritmi di IA sono impiegati in contesti che riguardano decisioni rilevanti per i diritti e le libertà individuali[206].

Le normative analizzate tentano di offrire soluzioni per contrastare la discriminazione algoritmica, ma seguono approcci differenti. Il GDPR si concentra sul ruolo dell'essere umano, cercando di garantire che sia adeguatamente attrezzato per

caratteristiche personali o della personalità note, inferite o previste nell'arco di determinati periodi di tempo. Il punteggio sociale ottenuto da tali sistemi di IA può determinare un trattamento pregiudizievole o sfavorevole di persone fisiche o di interi gruppi in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti, o a un trattamento pregiudizievole che risulta ingiustificato o sproporzionato rispetto alla gravità del loro comportamento sociale. I sistemi di IA che comportano tali pratiche inaccettabili di punteggio aventi risultati pregiudizievoli o sfavorevoli dovrebbero pertanto essere vietati. Tale divieto non dovrebbe pregiudicare le pratiche lecite di valutazione delle persone fisiche effettuate per uno scopo specifico nel rispetto del diritto dell'Unione e nazionale».

[206] Qui il testo del Considerando 67 «Dati di alta qualità e l'accesso a dati di alta qualità svolgono un ruolo essenziale nel fornire una struttura e garantire le prestazioni di molti sistemi di IA, in particolare quando si utilizzano tecniche che prevedono l'addestramento di modelli, al fine di garantire che il sistema di IA ad alto rischio funzioni come previsto e in maniera sicura e che non diventi una fonte di discriminazione vietata dal diritto dell'Unione. Per disporre di set di dati di addestramento, convalida e prova di elevata qualità è necessario attuare adeguate pratiche di *governance* e gestione dei dati. I *set* di dati di addestramento, convalida e prova, incluse le etichette, dovrebbero essere pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista del sistema. Al fine di agevolare il rispetto del diritto dell'Unione in materia di protezione dei dati, come il regolamento (UE) 2016/679, le pratiche di *governance* e di gestione dei dati dovrebbero includere, nel caso dei dati personali, la trasparenza in merito alla finalità originaria della raccolta dei dati. I *set* di dati dovrebbero inoltre possedere le proprietà statistiche appropriate, anche per quanto riguarda le persone o i gruppi di persone in relazione ai quali il sistema di IA ad alto rischio è destinato a essere usato, prestando particolare attenzione all'attenuazione di possibili distorsioni nei *set* di dati, suscettibili di incidere sulla salute e sulla sicurezza delle persone, di avere un impatto negativo sui diritti fondamentali o di comportare discriminazioni vietate dal diritto dell'Unione, specie laddove gli output di dati influenzano gli *input* per operazioni future (*feedback loops*, ossia "circuiti di *feedback*"). Le distorsioni possono ad esempio essere intrinseche ai *set* di dati di base, specie se si utilizzano dati storici, o generate quando i sistemi sono attuati in contesti reali».

individuare e prevenire distinzioni causate dall'uso della tecnologia[207]. L'*AI Act*, invece, cerca di ridurre i rischi di trattamenti differenziati attraverso un insieme di norme tecniche che regolano direttamente lo sviluppo e l'applicazione degli algoritmi. Questo approccio punta a minimizzare i *bias* e a garantire che i *dataset* utilizzati siano di alta qualità, contribuendo a limitare i risultati distorti.

Nonostante l'ambizione di queste normative, sorgono dubbi sulla loro fattibilità tecnica ed economica[208]. Le perplessità emergono soprattutto riguardo alla capacità reale di implementare tali regole senza ostacolare l'innovazione tecnologica e il mercato. Tuttavia, è innegabile che queste misure, anche se complesse, siano cruciali per mitigare i rischi connessi all'uso dell'IA, tra cui, in modo particolare, la discriminazione algoritmica. Le critiche che sostengono la preferenza per una regolamentazione meno stringente sembrano trascurare la necessità di affrontare problemi concreti già presenti che potrebbero avere effetti significativi sui diritti individuali e, a lungo termine, sullo sviluppo tecnologico stesso.

---

[207] Questo è evidente nell'art. 22, che garantisce il diritto a non essere sottoposti a decisioni esclusivamente automatizzate, e nel Considerando 71, che richiede misure per minimizzare i rischi di errori e discriminazioni.

[208] Per una disamina dei maggiori dubbi riguardanti l'*AI Act* v. A. MALASCHINI, *Il regolamento europeo sull'intelligenza artificiale (IA), l'orientamento italiano e i diversi indirizzi di Stati Uniti e Regno Unito*, in *Rass. parl.*, 1/2024, p. 35 ss.; G. SMORTO, *Distribuzione del rischio e tutela dei diritti nel regolamento europeo sull'intelligenza artificiale. Una riflessione critica*, in *Foro it.*, 5/2024, p. 208 ss.; A. ALAIMO, *Il Regolamento sull'Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico?*, in *federalismi.it*, 25/2023, p. 133 ss.; D. PIANA, G. VICICONTE, *Considerazioni critiche sulla proposta regolativa europea in materia di intelligenza artificiale con attenzione ai profili attuativi*, in *Riv. C. conti*, 4/2022, p. 7 ss.; M. GRANIERI, *Una sinopsi comparativa e una prospettiva critica sui tentativi di regolazione dell'intelligenza artificiale*, in *Comparazione e diritto civile*, 2/2023, p. 703 ss. Con riferimento, invero, al GDPR v. G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, in *federalismi.it*, 16/2020, p. 266 ss.; A. MESSINA, *Profili di criticità e di invalidità delle norme sanzionatrici del GDPR*, in *Ciberspazio e Diritto*, 1/2021, p. 3 ss.; A. ORTALDA, S. LEUCCI, *Identità digitale e protezione dei dati personali: punti di incontro e rischi nelle discipline eIDAS e RGPD*, in *Inf. dir.*, 1/2022, p. 145 ss.; M. SOLINAS, *Tutela penale della privacy dopo il GDPR: la frettolosa giustapposizione delle fonti è scaturigine di un sistema farraginoso, che crea confusione*, in *Resp. civ. prev.*, 2/2020, p. 663 ss.; T. SCANNICCHIO, *Tutela individuale e collettiva del consumatore nei casi di violazioni della "privacy": una mancata occasione di coordinamento con il GDPR*, in *giustiziacivile.com*, 6/2018.

5. Coinvolgimento di un sistema di IA nella commissione di un reato

Uno dei settori che sta diventando sempre più rilevante riguarda l'evoluzione della responsabilità penale tradizionale, quella che attribuiamo agli esseri umani, in un contesto in cui i reati non sono commessi direttamente dalla persona, ma attraverso l'uso di strumenti dotati di intelligenza artificiale[209].

Le straordinarie capacità dell'IA, infatti, possono essere sfruttate anche per scopi illeciti, aprendo la strada a modalità di commissione di reati che solo pochi anni fa sarebbero state impensabili[210].

L'immissione massiva di questi prodotti intelligenti nella società non può che riportare in primo piano il problema della sicurezza per utenti e terzi, un tema che

[209] Per un approfondimento si veda, fra tutti: C. PIERGALLINI, *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?*, in *Riv. it. dir. e proc. pen*., 4/2020, p. 1743 ss.; I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, cit., p. 83 ss.; G.R. MINELLI, *Quando l'autore del reato è un robot: tra vecchi modelli imputativi e nuovi possibili paradigmi di responsabilità penale*, in F. Basile, M. Caterini, S. Romano (a cura di), *Il sistema penale ai confini delle hard sciences*, cit., p. 57 ss.; A. GIANNINI, *Intelligenza artificiale, human oversight e responsabilità penale*, cit., p. 249 ss.; M. B. MAGRO, *Robot, cyborg e intelligenze artificiali*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Cybercrime*, Utet Giuridica, Milano, 2019, p. 1179 ss.; 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 ss.; U. PAGALLO, *Saggio sui robot e il diritto penale*, in S. Vinciguerra, F. Dassano (a cura di), *Scritti in memoria di Giuliano Marini*, Edizioni Scientifiche Italiane, Napoli, 2010, p. 595 ss.; R. BORSARI, *Intelligenza Artificiale e responsabilità penale: prime considerazioni*, in *MediaLaws*, 3/2019, p. 262 ss.; V. MANES, *L'oracolo algoritmico e la giustizia penale*, cit., p. 2 ss.; P. SEVERINO, *Intelligenza artificiale e diritto penale*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020, p. 533 ss.; C. MINELLI, *La responsabilità "penale" tra persona fisica e corporation*, cit., p. 50 ss.; A. CAPPELLINI, *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale*, in *Criminalia*, 2018, p. 499 ss.; S. RIONDATO, *Robotica e diritto penale (robot, ibridi, chimere, "animali tecnologici")*, in D. Provolo, S. Riondato, F. Yenisey (a cura di), *Genetics, Robotics, Law, Punishment*, Padova University Press, p. 600 ss.; V. ARAGONA, *I Robot: the criminal liability of artificial intelligences*, in *TransJus Working Papers Publications*, 4/2019, p. 83 ss.

[210] Due esempi emblematici sono l'uso di droni e sottomarini senza equipaggio, controllati a distanza, per il trasporto di stupefacenti e armi illegali, e l'impiego di BOT sui *social media*, utilizzati per diffondere molestie, diffamazioni e manipolare l'opinione pubblica attraverso *tweet*, *retweet* e altre tecniche simili.

tradizionalmente rientra nell'ambito della responsabilità per danno da prodotto[211]. Tuttavia, in questo contesto, tale problematica sembra estendersi fino a coinvolgere ambiti più classici della responsabilità per colpa. Tra le molteplici possibilità in cui i reati previsti dall'ordinamento possono intrecciarsi con l'uso di strumenti dotati di intelligenza artificiale, un aspetto che merita un'attenzione particolare è quello relativo ai reati colposi contro la vita e l'incolumità personale[212].

I sistemi di intelligenza artificiale possono rientrane nella figura, già nota al diritto penale, di mezzo o strumento del reato, senza però modificare la responsabilità del soggetto umano che lo impiega, proprio come accade con qualunque oggetto utilizzato per scopi illeciti. Nei reati colposi, in particolare, quando un evento lesivo è causato da un uso improprio o da un difetto di progettazione o costruzione di un prodotto, la responsabilità può ricadere sull'utilizzatore o sul produttore umano, a condizione che sussistano gli estremi della colpa. La complessità del prodotto o del processo industriale coinvolto può rendere più difficili e articolati i giudizi relativi alla causalità materiale e, soprattutto, alla colpa, ma non altera il principio di fondo: la responsabilità penale rimane saldamente ancorata alla condotta dell'agente umano.

Può sussistere unicamente una sorta di prevedibilità del comportamento: in presenza di certe situazioni o comandi, il sistema reagirà sempre nello stesso modo, basandosi sulla sua programmazione algoritmica. In tal senso, l'uomo che lo utilizza o lo progetta è in grado, a priori, di prevedere gli effetti delle proprie azioni attraverso quel prodotto. Questa prevedibilità diminuisce con l'aumentare dell'automazione del

---

[211] Sulla responsabilità penale per danno da prodotto si veda: R. BARTOLI, *Danno da prodotto e responsabilità penale*, in *Riv. it. dir. e proc. pen*, 4/2004, p. 1163 ss.; A.L. BITETTO, *In tema di responsabilità per danno da prodotto difettoso*, in *Foro it.*, 10/2009, p. 441 ss.; C. PIERGALLINI, *Danno da prodotto e responsabilità penale*, cit.; D. CASTRONUOVO, *Responsabilità da prodotto e struttura del fatto colposo*, in *Riv. it. dir. e proc. pen.*, 1/2005, p. 301 ss.; A. BERNARDI, *La responsabilità da prodotto nel sistema italiano: profili sanzionatori*, in *Riv. trim. dir. pen. econ.*, 1/2003, p. 1 ss.; R. BERTOLESI, *Intelligenza artificiale e responsabilità penale per danno da prodotto*, Università degli Studi di Milano, Tesi dottorale, A.A. 2018/2019; F. CONSULICH, *Flash offenders. Le prospettive di accountability penale nel contrasto alle intelligenze artificiali devianti*, cit., p. 1015 ss.; L. M. PUENTE ABA, *Criminal product liability, causal link and big data: a first approach - Responsabilità penale per il prodotto, causalità e dati massivi: una prima approssimazione*, in *Studi sulla questione criminale*, 3/2023, p. 41 ss.

[212] A. CAPPELLINI, *Reati colposi e tecnologie dell'intelligenza artificiale*, cit., p. 3 ss.

sistema intelligente, grazie alla sua capacità di apprendimento e di agire anche in assenza di comandi diretti[213].

Nel mondo fisico, le fattispecie criminali come il furto, la frode, la diffamazione o la violazione della *privacy* si manifestano attraverso azioni dirette e materiali. Tuttavia, quando queste stesse condotte avvengono *online*, assumono una forma diversa: vengono eseguite attraverso il trasferimento di dati, la manipolazione di informazioni digitali o l'uso di identità false. Sebbene "azione stessa sia immateriale (per esempio, il furto di dati informatici non implica lo spostamento fisico di un oggetto), gli effetti che ne derivano sono tangibili e spesso devastanti, tanto da causare danni economici, psicologici e, in alcuni casi, anche fisici alle vittime[214].

Ad esempio, crimini informatici come il furto di identità possono portare a conseguenze finanziarie dirette, mentre la diffamazione o il *cyberbullismo* possono causare traumi emotivi o, nei casi estremi, indurre le vittime a gesti autolesionistici. Il concetto di immaterialità dell'azione criminale non riduce quindi l'impatto del reato stesso, ma pone piuttosto una sfida interpretativa e applicativa per i sistemi giuridici, che devono adattarsi per riconoscere e punire queste condotte con la stessa severità dei reati commessi nel mondo fisico[215].

---

213 Si fa riferimento al *machine learning*, di cui si è detto nel capitolo 1.

214 Per un approfondimento sui caratteri della criminalità informatica v. S. LORUSSO, *"Digital evidence", "cybercrime" e giustizia penale 2.0*, in *Proc. pen. e giust.*, 4/2019, p. 821 ss.; B. ROMANO, *In the Era of AI. Exploring New Frontiers in Cybercrime and Safeguarding Personal and Health Data*, in *Corti Supreme e Salute*, 1/2024, p. 461 ss.; A. IANNUZZI, *Considerazioni sul disegno di legge "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (AC 1717). Audizione informale innanzi alle Commissioni riunite I (Affari costituzionali) e II (Giustizia) della Camera dei Deputati*, in *Inf. dir.*, 1/2024, p. 59 ss.; A. MATTARELLA, *Il "cybercrime" nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite*, in *Dir. pen. e proc.*, 6/2022, p. 809 ss.; V. S. BONAMINI PEPOLI, *Profili di contrasto al "cybercrime" "in iure condito" e "de iure condendo"*, in *Inf. dir.*, 2/2022, p. 109 ss.; P. ANNICCHINO, *(In)sicurezza dei dati, contromisure e attività di contrasto alla criminalità informatica*, in *Dir. pen. e proc.*, 9/2022, p. 1155 ss.: S. PIETROPAOLI, *Un'occasione (forse) mancata. Considerazioni sulla revisione dei reati informatici proposta con il DDL Cybersicurezza*, in *Inf. dir.*, 1/2024, p. 47 ss.; L. PICARELLA, *Il "cybercrime" come nuova sfida definitoria al concetto di criminalità organizzata*, in *Studi sulla questione criminale*, 1/2024, p. 105 ss.; R. CALCAGNO, *Nuove disposizioni per il contrasto ai fenomeni di criminalità informatica*, in *Dir. pen. e proc.*, 8/2012, p. 934 ss.

215 Cfr. P. TRONCONE, *La tutela penale della riservatezza e dei dati personali,* cit., p. 79 ss. Per un approfondimento si veda anche F. GIUNTA, *Oltre la logica della punizione: linee evolutive e ruolo del diritto penale*, in E. Dolcini; C.E. Paliero (a cura di), *Studi in onore di Giorgio Marinucci,* cit., p. 356 ss.

Alcune categorie di reato trovano nella rete il contesto ideale per la loro consumazione: i reati di opinione[216], quelli contro la reputazione e la dignità personale, i reati contro la libertà sessuale e i minori, quelli contro il patrimonio e, in particolare, i reati di falso. L'uso aggressivo e pervasivo della rete può rendere qualsiasi individuo debole e vulnerabile. In questo contesto, è fondamentale rafforzare la risposta sanzionatoria, introducendo circostanze aggravanti specifiche per proteggere coloro che, nel mondo fisico, possono difendersi, ma che nel *cyberspazio* risultano praticamente impotenti di fronte alla violenza di uno strumento con un potenziale dannoso indiscutibile.

La giurisprudenza sta iniziando a utilizzare l'aggravante della «minorata difesa» prevista dall'art. 61, n. 5 c.p., per reati commessi «nel luogo di *Internet*», come sancito dalla Cassazione, Sez. II penale, con la Sentenza n. 40045 del 6 settembre 2018: «In punto di diritto, va rilevato che la giurisprudenza di questa Corte è ormai consolidata nel senso che sussista l'aggravante della minorata difesa, con riferimento alle circostanze di luogo, note all'autore del reato e delle quali egli, ai sensi dell'articolo 61 c.p., n. 5, abbia approfittato, nell'ipotesi di truffa commessa attraverso la vendita di prodotti *on-line*, poiché, in tal caso, la distanza tra il luogo ove si trova la vittima, che di norma paga in anticipo il prezzo del bene venduto, e quello in cui, invece, si trova l'agente, determina una posizione di maggior favore di quest'ultimo, consentendogli di schermare la sua identità, di non sottoporre il prodotto venduto ad alcun efficace controllo preventivo da parte dell'acquirente e di sottrarsi agevolmente alle conseguenze della propria condotta»[217].

Il mondo immateriale della rete rimane, in generale, poco influenzato dalla minaccia del carcere e dalla privazione della libertà personale, strumenti tipici di punizione nel mondo reale che richiedono azioni ed eventi tangibili. Questa è la naturale conseguenza della materialità attenuata dal *web*, dove lo schermo dell'anonimato e la smaterializzazione dell'offesa riducono il livello di consapevolezza e la volontà

[216] V. paragrafo 2.2.2., *Fake news* e *Hate speech*.

[217] Sez. 6, Sentenza n. 17937 del 22/03/2017 Cc. (dep. 10/04/2017) Rv. 269893.

colpevole. In questo contesto, il modello tradizionale di sanzione penale non risulta più efficace né adeguato agli obiettivi di politica criminale che si intendono perseguire[218].

Il potenziale deterrente della sanzione si indebolisce, compromettendo anche le finalità rieducative e riabilitative della pena. La rete, con il suo schermo protettivo, aumenta i rischi di elusione della responsabilità e della punizione. In questo contesto, non solo il concetto di afflittività della pena, perde rilevanza, ma anche il principio di punibilità si deteriora a causa della mancanza di concretezza e della difficile percezione del nucleo del reato. Senza l'effettività delle regole, la sanzione penale perde di efficacia e, di conseguenza, anche la funzione rieducativa viene compromessa.

Piuttosto che una finalità afflittiva e repressiva, la pena qui dovrebbe tendere alla prevenzione dei reati commessi con il mezzo della rete. L'obiettivo finale dovrebbe essere quello di rendere le misure di prevenzione e repressione sufficientemente convincenti a dissuadere i trasgressori.

Un ruolo rieducativo potrebbe essere svolto da una forma di prevenzione che imponga una temporanea interdizione dall'uso di mezzi informatici come misura inabilitativa, includendo anche la confisca dei dispositivi utilizzati per commettere il reato o altri tipi di sanzioni anche civili[219].

Le buone pratiche possono servire come strumenti educativi efficaci per prevenire e scoraggiare comportamenti illeciti online. Ad esempio, una prassi utile potrebbe essere quella di fornire informazioni chiare e facilmente comprensibili sui dati,

---

[218] Cfr. P. TRONCONE, *La tutela penale della riservatezza e dei dati personali,* cit., p. 80; S. SEMINARA, *Considerazioni su privacy, anonimato e internet*, in L. Fioravanti (a cura di), *La tutela penale della persona. Nuove frontiere, difficili equilibri*, Giuffrè, Milano, 2001, p. 355 ss.

[219] Sulla funzione di deterrenza delle sanzioni in questo contesto v. E. DI AGOSTA, *Punizione, deterrenza e ruolo della pena nei copyright crimes: appunti sul tema statunitense*, in *Ind. pen*., 3/2015, p. 495 ss.; E. TOSI, *Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo*, in *Contr. impr*., 3/2020, p. 1115 ss.; E. NAVARRETTA, *Il risarcimento in forma specifica e il dibattito sui danni punitivi tra effettività, prevenzione e deterrenza*, in *Resp. civ. prev*., 1/2019, p. 6 ss.; M. DELLACASA, *"Punitive damages", risarcimento del danno, sanzioni civili: un punto di vista sulla funzione deterrente della responsabilità aquiliana,* in *Contr. impr*., 4/2017, p. 1142 ss.; R. SIMONE, *La responsabilità civile non è solo compensazione: "punitive damages" e deterrenza*, in *Foro it*., 9/2017, p. 2644 ss.; M. S. ROMANO, *Danni punitivi ed eccesso di deterrenza: gli (incerti) argini costituzionali*, in *Foro it*., 4/1990, p. 175 ss.

specificando la loro destinazione e modalità di trattamento, e di avvertire gli utenti con messaggi personalizzati e tempestivi riguardo ai comportamenti vietati, che potrebbero essere dettagliatamente elencati. Inoltre, potrebbe essere utile richiedere un impegno specifico per l'uso di una determinata postazione informatica e adottare strumenti tecnologici per bloccare l'accesso in caso di violazione di tale impegno.

Tuttavia, è fondamentale che queste pratiche non impongano restrizioni tali da compromettere la reputazione futura dell'individuo o danneggiare irrimediabilmente la sua immagine digitale.

In tale contesto, è compito del legislatore prestare particolare attenzione alla fase di progettazione della normativa, e, adottando un approccio educativo, definire singole fattispecie di reato in modo che le modalità di condotta siano chiaramente identificabili nelle descrizioni astratte dei comportamenti proibiti. È fondamentale evitare l'uso di formule generali, rinvii complessi e definizioni indeterminate basate su casi specifici. Pertanto, emerge come cruciale la questione relativa alla fonte del diritto e al processo normativo che dà vita alla disciplina penale.

Man mano che cresce il livello di intelligenza di tali prodotti, l'imprevedibilità tecnologica tende ad amplificarsi, rendendo ancora più complessa la gestione dei rischi associati al loro utilizzo.

Si parla in tal caso di opacità tecnologica, che ha un impatto significativo sul tradizionale meccanismo di attribuzione della responsabilità per reati colposi: l'imprevedibilità degli effetti paralizza infatti il giudizio di imputazione per colpa, creando un *responsibility gap*[220], un vuoto di responsabilità. Man mano che i margini di autonomia dei soggetti artificiali intelligenti aumentano è prevedibile che cresca anche il numero di eventi lesivi per l'incolumità umana causati dai loro comportamenti, eventi che rischiano di rimanere privi di una corrispondente responsabilità penale.

[220] Per un approfondimento sul concetto di *responsibility gap* si veda: M. B. MAGRO, *Biorobotica, robotica e diritto penale*, in D. Provolo, S. Riondato, F. Yenisey (a cura di), *Genetics, Robotics, Law, Punishment*, cit., p. 515 ss.; B. PANATTONI, *Intelligenza Artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale*, in *Dir. inform.*, 2/2021, p. 317 ss.; J. DANAHER, *Robots, Law and the Retribution Gap*, in *Ethics and Information Technology*, 2016, p. 299 ss.

Anche se si riuscisse a superare le difficoltà legate all'individuazione del singolo responsabile umano all'interno di una complessa rete di produzione e programmazione, rimarrebbe comunque un problema fondamentale: il comportamento imprevedibile della macchina, per sua stessa natura, difficilmente potrebbe essere imputato per colpa al soggetto umano.

Quando viene meno la possibilità di imputare un eventuale risultato lesivo a un utilizzatore che non ha più alcun controllo sull'azione pericolosa, essendo ormai escluso dalla sua gestione, ciò che resta è la possibilità del fortuito oppure di un fatto proprio del soggetto artificiale, una situazione che solleva questioni significative e complesse riguardo alla sua diretta responsabilità.

Capitolo 3
Mobilità avanzata e responsabilità penale

1. I veicoli a guida autonoma

1.1. Inquadramento normativo

Il recente sviluppo dell'intelligenza artificiale e del *Machine Learning* sta conducendo ad una progressiva sostituzione dell'uomo nello svolgimento di attività che, fino a qualche tempo fa, si pensava potessero essere realizzate soltanto con l'intelligenza umana[1].

La guida di veicoli autonomi è una realtà sempre più diffusa e in rapida evoluzione. Se da un lato promette di rendere le strade più sicure e aumentare l'efficienza del traffico, essa pone anche importanti questioni giuridiche, in particolare riguardo alla responsabilità penale. Oltre alla questione della responsabilità penale in caso di sinistri, i veicoli autonomi presentano sfide specifiche anche per quanto riguarda la sicurezza stradale e la protezione dei dati[2]. Ad esempio, i dati raccolti dai sensori dei veicoli autonomi possono essere utilizzati per scopi commerciali o per la sorveglianza governativa, e la protezione di questi dati è una preoccupazione significativa.

---

[1] Sul punto si veda I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, cit., p. 83; C. MINELLI, *La responsabilità "penale" tra persona fisica e corporation,* cit., p. 50; L. LUPÀRIA DONATI, G. FIORELLI, *Diritto probatorio e giudizi criminali ai tempi dell'Intelligenza Artificiale*, in *Dir. pen. cont.,* 2/2022, p. 39 ss. In particolare, sui vantaggi del *machine learning* v. O. DI GIOVINE, *Il judge-bot e le sequenze giuridiche in materia penale (intelligenza artificiale e stabilizzazione giurisprudenziale)*, relazione al convegno su *Il principio di legalità fra legislatore e giudice*, Università di Foggia, 25 settembre 2019, in *Cass. pen.*, 3/2020, p. 953 ss.

[2] Sul punto si veda A. PISANI TEDESCO, *Rischi satellitari e informatici*, in D. Cerini, A. Pisani Tedesco (a cura di), *Smart mobility, smart cars e intelligenza artificiale: responsabilità e prospettive*, Giappichelli, Torino, 2019, p. 79 ss.; F. COSTANTINI, *Il problema della sicurezza tra informatica e diritto: una prospettiva emergente dalle "smart cars"*, in *Inf. dir.*, 1/2016, p. 95 ss.; M.C. GAETA, *La protezione dei dati personali nell'IoT, l'esempio dei veicoli autonomi*, in *Dir. inform.*, 1/2018, p. 147 ss.

In molti Paesi, la responsabilità penale per incidenti causati da veicoli autonomi è attualmente incerta[3].

Un aspetto importante da considerare nella determinazione della responsabilità penale è il grado di autonomia del veicolo[4].

Esistono diversi livelli di automazione per i veicoli autonomi, che vanno da veicoli completamente guidati da umani a veicoli autonomi senza alcun intervento umano. La SAE (*International Society of Automotive Engineers*)[5] ha catalogato sei classi di funzionalità per distinguere il grado di automazione dei veicoli[6]:

- Livello 0: veicolo completamente condotto dall'uomo.
- Veicoli a guida assistita (livello 1): sono dotati di sistemi avanzati di assistenza alla guida, come il cruise control, ma richiedono la presenza di un conducente pronto a prendere il controllo in qualsiasi momento.
- Veicoli a guida semi-autonoma (livello 2): possono gestire alcune funzioni di guida, come la guida in autostrada e il mantenimento della corsia, ma richiedono sempre la presenza di un conducente per le situazioni di emergenza.

[3] Sul punto cfr. L. PICOTTI, *Profili di responsabilità penale per la circolazione di veicoli a guida autonoma*, cit.; G. CALABRESI, E. AL MUREDEN, *Driveless cars, Intelligenza artificiale e futuro della mobilità*, cit.; A. BERTOLINI, *Robots as Products: The Case for a Realistic Analysis of Robotic Application and Liability Rules*, cit. p. 214 ss.; E. AL MUREDEN, *Sicurezza "ragionevole" degli autoveicoli e responsabilità del produttore nell'ordinamento giuridico italiano e negli Stati Uniti*, cit.; K. VAN WEES, K. BROOKHUIS, *Product Liability for ADAS: legal and human factors perspectives*, cit., p. 357 ss.; A. BERTOLINI, E. PALMERINI, *Regulating robotics: A challenge for Europe*, cit., p. 169 ss.; J. MANIKA, *Big Data: the next frontier for innovation, competition and productivity, Technical report,* cit.; S. STEFANIZZI, *Riflessioni metodologiche sul concetto e sull'uso dei Big Data*, cit., p. 17 ss.; C. SEVERONI *Prime considerazioni su un possibile inquadramento giuridico e sul regime di responsabilità nella conduzione dei veicoli a guida autonoma*, cit., p. 331 ss.; D. CERINI, *Dal Decreto Smart Roads in avanti ridisegnare responsabilità e soluzioni assicurative*, cit., p. 401 ss.

[4] Se il veicolo fosse progettato per essere completamente autonomo e non richiedere intervento umano, la responsabilità penale potrebbe essere attribuita al produttore del veicolo o del *software*. Tuttavia, se il veicolo richiede l'intervento umano in alcune situazioni, la responsabilità potrebbe essere attribuita all'utilizzatore del veicolo.

[5] Si tratta di un'associazione con oltre centomila ingegneri impegnati nel settore dei trasporti, che opera quale ente di normazione nel campo dell'industria automobilistica.

[6] Si veda *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, *on line* sul sito *web* www.sae.org, aggiornato al 30 aprile 2021.

- Veicoli a guida autonoma di livello 3: possono gestire completamente la guida in determinate situazioni, come la guida in autostrada, ma richiedono comunque la presenza del conducente.
- Veicoli a guida autonoma di livello 4: sono in grado di gestire completamente la guida in molte situazioni, ma sono limitati a determinate aree geografiche e situazioni specifiche, come la guida in una zona urbana.
- Veicoli a guida autonoma di livello 5: sono completamente autonomi e non richiedono la presenza di un conducente.

Le questioni legate alla guida autonoma si pongono a partire dal livello 3, posto che i livelli 1 e 2 descrivono i sistemi di guida assistita e non autonoma[7].

Attualmente, non sono ancora presenti sulle strade veicoli di livello 4 e 5, mentre ci sono casi di sperimentazione di veicoli di livello 3[8].

Già la Convenzione di Vienna del 1968, all'art. 8, richiede che all'interno di un veicolo in movimento sia sempre presente un conducente che ne abbia costantemente il controllo[9]. Anche il Codice della strada all'art. 46 definisce veicoli «tutte le macchine di qualsiasi specie, che circolano sulle strade guidate dall'uomo».

---

[7] In tal senso v. G. TORCHIANI, *Auto a guida autonoma: cosa sono e come funzionano*, 18 maggio 2021, sul sito *web* www.ai4business.it.

[8] V. per tutti D.G. GLEAVE, R. FRISONI, A. DALL'OGLIO, C. NELSON, J. LONG, C. VOLLA, D. RANGHETTI, S. MCMINIMY, *Self Piloted Cars: the Future of Road Transport?, Research for the Transport and Tourism Committee of the European Parliament*, 2016, consultabile sul sito *web* del Parlamento europeo.

[9] La Convenzione, all'art. 8 par. 1 afferma che «Ogni veicolo in movimento o ogni complesso di veicoli in movimento deve avere un conducente». Il par. 5 precisa che «Ogni conducente deve avere costantemente il controllo del proprio veicolo». Infine, il par. 5 bis: «I sistemi di bordo che influiscono sulla guida del veicolo sono considerati conformi al paragrafo 5 del presente articolo e al primo paragrafo dell'articolo 13 se sono conformi alle disposizioni in materia di costruzione, montaggio e utilizzo previste negli strumenti giuridici internazionali riguardanti i veicoli a ruote e gli equipaggiamenti e componenti montati e/o utilizzati sugli stessi. I sistemi di bordo che influiscono sulla guida del veicolo e non conformi alle disposizioni in materia di costruzione, montaggio e utilizzo summenzionate sono considerati conformi al paragrafo 5 del presente articolo e al primo paragrafo dell'articolo 13 se possono essere neutralizzati o disattivati dal conducente». Per un commento critico, sul punto, C. COULON, *Révision de la Convention de Vienne sur la circulation routière: les voiture autonomes (pas tout à fait) sur la ligne de départ*, in *Resp. civ. et assurance*, alerte 17, 6/2016, p. 57 ss.; V. BATTISTELLA, *Spunti di riflessione sulla conduzione dei veicoli altamente automatizzati nella circolazione stradale in una prospettiva de iure condendo*, in *Dir. trasp.*, 2021, p. 953 ss.; I. VINGIANO-VIRICEL, *Véhicule autonome: qui est responsable?, Impacts de la délégation de conduite sur les régimes de responsabilité*, LexisNexis, New York, 2019.

Per quanto riguarda le implicazioni giuridiche, il grado di automazione influisce sulla responsabilità in caso di incidente. In generale, può già anticiparsi che quanto più alto è il livello di automazione, maggiore è la responsabilità del produttore o del proprietario del veicolo, rispetto alla responsabilità del conducente. Tuttavia, in alcuni casi, il conducente può ancora essere ritenuto responsabile, ad esempio se il veicolo è stato modificato o se non è stato utilizzato correttamente[10]. Oltre ai produttori, possono essere presi in considerazione anche gli sviluppatori del *software*. Il sensore e gli algoritmi sviluppati e installati nei veicoli autonomi svolgeranno un ruolo più cruciale rispetto ai componenti delle auto convenzionali. Per tale ragione, gli sviluppatori dovranno progettare, testare e ispezionare le parti dei componenti prima di vendere veicoli autonomi per non incorrere in ipotesi di responsabilità[11].

A livello europeo, tra i vari tentativi di regolamentazione per rispondere al rapido sviluppo dell'intelligenza artificiale, un documento di particolare rilevanza è il Libro Bianco pubblicato nel febbraio 2019 dalla Commissione europea al fine di gettare le basi della tutela dei diritti dei consumatori e per promuovere l'innovazione nel campo dell'IA. Si tratta del primo esempio al mondo di una regolamentazione sistematica in questo ambito, e pone l'Europa all'avanguardia nella disciplina di questo settore. Tuttavia, è importante sottolineare che il Libro Bianco non affronta in modo specifico la questione dei veicoli senza conducente[12].

Anche la recente adozione dell'*AI Act* ha posto diverse sfide per i produttori di veicoli autonomi. In primo luogo, la necessità di conformarsi ai requisiti di trasparenza significa che le aziende devono essere in grado di spiegare come i loro algoritmi prendono decisioni. Questi requisiti sono delineati in Titolo III, Capitolo 2 dell'AI Act, che riguarda la gestione dei rischi, la robustezza e la trasparenza dei sistemi AI ad alto rischio, compresi quelli installati nei veicoli autonomi e semi-autonomi.

---

[10] A. KASAP, *Autonomous vehicles, tracing the Locus of regulation and liability*, Edward Elgar Publishing, Cheltenham, 2022, p. 89 ss.; C. BJOLA, *Diplomacy in the Age of Artificial Intelligence, in Intelligence artificielle, défise et perspectives*, Bruylant, Bruxelles, 2021, p. 61 ss.

[11] A. KASAP, *Autonomous vehicles*, cit., p. 90.

[12] Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia, 19.02.2020, sul sito *web* dell'Ufficio delle pubblicazioni dell'Unione europea, www.op.europa.eu.

Inoltre, l'obbligo di valutazione del rischio impone ai produttori di effettuare test rigorosi e dimostrare che i loro sistemi sono sicuri in una varietà di condizioni. Questo include non solo condizioni di guida *standard*, ma anche scenari di emergenza e situazioni insolite. Tuttavia, queste sfide rappresentano anche un'opportunità per l'industria di dimostrare il valore e la sicurezza delle loro tecnologie, potenzialmente aumentando la fiducia dei consumatori.

La normativa italiana che regola il funzionamento e l'utilizzo dei veicoli autonomi, è ancora in fase di sviluppo. Attualmente la fonte più rilevante in materia è costituita dal D.M. 28 febbraio 2018[13] (c.d. Decreto *Smart Roads*) che ha dato seguito al «Piano di azione nazionale sui Sistemi intelligenti di trasporto – ITS», adottato con decreto del medesimo Ministro delle infrastrutture e dei trasporti in data 12 febbraio 2014, n. 44, in attuazione della Direttiva 2010/40/UE del Parlamento europeo e del Consiglio del 7 luglio 2010[14].

Tale decreto offre, innanzitutto, una definizione di veicolo a guida automatica, che deve essere «dotato di tecnologie capaci di adottare e attuare comportamenti di guida senza l'intervento attivo del guidatore, in determinati ambiti stradali e condizioni esterne».

---

[13] Decreto 28 febbraio 2018, su modalità attuative e strumenti operativi della sperimentazione su strada delle soluzioni di *Smart Road* e di guida connessa e automatica (c.d. Decreto *Smart Road*), GU serie gen. n. 90 del 18 aprile 2018, www.gazzettaufficiale.it. Per un commento sul decreto, si veda S. PELLEGATTA, *Smart cars and smart roads: the italian way for the new mobility test phase*, in *Riv. Dir. dell'Economia, dei Trasporti e dell'Ambiente*, 2022, p. 129 ss.; U. RUFFOLO, *Self driving cars, Auto driverless e responsabilità*, in U. Ruffolo (a cura di), *Intelligenza artificiale e responsabilità*, Giuffrè, Milano, 2017, p. 49 ss.; S. SCAGLIARINI, *Smart Roads e driverless cars: tra diritto, tecnologie, etica pubblica*, Giappichelli, Torino, 2019; M.G. LOSANO, *Verso l'auto a guida autonoma in Italia*, in *Dir. inform.*, 2019, p. 423 ss.; N. MINISCALCO, *Smart area, circolazione dei veicoli autonomi e protezione dei dati personali*, in S. Scagliarini (a cura di), *Smart Roads e Driverless Cars*, cit., p. 27 ss.; D. CERINI, *Dal Decreto Smart Roads in avanti,* cit. p. 401 ss.

[14] Nelle premesse del Piano di azione nazionale si afferma che l'obiettivo della Direttiva è quello di «istituire un quadro a sostegno della diffusione e dell'utilizzo di sistemi di trasporto intelligenti [*ITS*] coordinati e coerenti nell'Unione, in particolare attraverso le frontiere tra gli Stati membri, stabilendo le condizioni generali necessarie a tale scopo». La Direttiva individua poi i settori prioritari: l'uso ottimale dei dati relativi alle strade, al traffico e alla mobilità; la continuità dei servizi *ITS* di gestione del traffico e del trasporto merci; le applicazioni *ITS* per la sicurezza stradale e per la sicurezza del trasporto; il collegamento tra i veicoli e l'infrastruttura di trasporto.

Tuttavia, la norma richiede che la conduzione su strada sia effettuata da un supervisore, il quale «deve essere in grado di commutare tempestivamente tra operatività del veicolo in modo automatico e operatività dello stesso in modo manuale e viceversa» (così art. 10, comma 2 D.M. cit.)[15].

I veicoli cui si riferisce il testo, pertanto, sono quelli fino al livello 3 della classificazione SAE prima descritta, che può essere definita come guida automatica, distinta da quella autonoma relativa ai livelli 4 e 5, non ancora presente allo stato attuale[16].

Occorre chiedersi a chi possa essere attribuita la responsabilità in caso di sinistri, prendendo in considerazione le fattispecie che tipicamente vengono in rilievo, ovvero l'omicidio stradale e le lesioni personali stradali, i quali richiedono che gli eventi dannosi siano cagionati per colpa[17].

1.2. Le implicazioni penalistiche

Può essere mosso un rimprovero per colpa in capo ad un sistema di guida artificiale? Per rispondere a tale quesito occorre tenere in considerazione il fatto che i sistemi più avanzati di intelligenza artificiale hanno una sorta di capacità di apprendimento, derivante dall'elaborazione dei dati esterni al sistema sulla base delle tecnologie di *machine learning*[18].

---

[15] Il sistema italiano ha seguito l'esempio di altri Paesi europei, e in particolare della Germania, che ha recentemente emanato una normativa rigorosa sui veicoli a guida autonoma e relativi test. Sul punto si veda M. LOSANO, *Il Progetto di legge Tedesco sull'auto a guida automatizzata. Appendice: il Progetto di legge e le relazioni illustrative*, in *Dir. inform.*, 2017, p. 3 ss.; M.T. FRANZÉ, *La proposta normativa tedesca sulla guida autonoma, il via ai test sulle strade*, in *Cyberlaws*, 18 settembre 2018, sul sito *web* www.cyberlaws.it; F. HENKEL, J. NOWAK, N.SMIRRA, *Autonomous vehicles: the legal landscape in Germany,* in *Norton Rose Fulbright*, 11 agosto 2016, sul sito *web* www.nortonrosefulbright.com.

[16] V. per tutti C. INGRATOCI, *Autonomous vehicles in smart roads: an integrated management system for road circulation*, in *Dir. trasp.*, 2020, p. 97 ss.

[17] Sul punto si veda S. MAGNOSI, *Circolazione stradale e responsabilità delle automobili autonome: profili penalistici*, in *Dir. trasp., Atti dell'incontro di studi «L'automazione nei trasporti marittimi, aerei e terrestri»*, Cagliari, 9-10 novembre 2018, p. 325 ss.

[18] In tal senso si veda G. GIUFFRIDA, F.M. RINALDI, *Big Data, Intelligenza Artificiale e Machine Learning: tra discriminazione e responsabilità algoritmica*, in *Big Data e processi decisionali*, cit., p. 35 ss.; C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato?*, cit., p. 1746 ss.; I. SALVADORI,

Come abbiamo visto nei paragrafi precedenti, alcuni studiosi hanno ipotizzato la responsabilizzazione diretta della macchina. I sistemi di intelligenza artificiale, infatti, non sono più meri esecutori dei comandi umani, ma operano con un certo grado di autonomia. Tuttavia, questa autonomia, allo stato attuale, non può essere idonea ad ascrivere una responsabilità penale, dal momento che i sistemi di IA non sono ancora dotati di quella coscienza tipica dell'uomo, che sta alla base della possibilità di capire cosa è giusto e cosa è sbagliato. La sanzione penale, finalizzata a controllare e orientare il comportamento dei consociati, non potrebbe avere efficacia nei confronti di un agente artificiale che non ha una personalità suscettibile di percepire il rimprovero collegato alla sanzione[19].

La responsabilità delle «scelte» operate dal sistema di IA sarà quindi da attribuire ad un agente umano, attraverso una ricostruzione dei diversi contributi causali che hanno portato alla condotta posta in essere dal sistema. I soggetti umani che operano attraverso i sistemi di IA possono essere considerati come autori mediati dei fatti agli stessi riconducibili. In tale contesto occorrerà arginare la tendenza ad una diffusione della responsabilità tra i vari soggetti che hanno avuto un ruolo nell'avvenimento[20].

Nel caso di sinistri stradali, una prima ipotesi è quella di attribuire la responsabilità al conducente, anche sulla base di un principio di *vicinitas*. Infatti, sebbene sia vero che, nel momento in cui si attiva il sistema di guida autonoma, colui che si trova a bordo del veicolo potrebbe essere considerato come un semplice passeggero, tuttavia, come abbiamo detto, la normativa italiana richiede la presenza di un conducente che sia pronto a riprendere il dominio del mezzo.

Pertanto, il conducente assume una posizione di controllo sul mezzo, in quanto ha l'obbligo di stabilire se e quando sia necessario commutare l'operatività del veicolo da automatica a manuale. In caso di violazione dell'obbligo di sorveglianza o di

Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale, cit., p. 90 ss.; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1/2019, p. 69 ss.; D. PIVA, *Machina discere, (deinde) delinquere et puniri potest,* cit., p. 681 ss.

[19] Sul punto si veda L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta cambiando il mondo*, cit.

[20] C. MINELLI, *La responsabilità "penale" tra persona fisica e corporation*, cit., p. 55.

passaggio dall'una all'altra modalità di guida, può sorgere una forma di responsabilità colposa omissiva per omesso impedimento dell'evento dannoso.

Se, invece, l'incidente si verifica quando il conducente non ha il controllo della vettura, potrebbe essersi verificato un errore alla guida da parte del sistema. A questo punto, se, come abbiamo detto, questo errore non può essere rimproverato direttamente al sistema di IA, non resta che valutare la possibilità di attribuire la responsabilità al produttore.

Tra le cause del danno in contesti di intelligenza artificiale potrebbe esservi l'azione dell'utilizzatore, o ancora un difetto di programmazione, di costruzione, o di informazione, i quali possono anche interagire *pro quota* (art. 41, commi 1 e 3 c.p.), nonché fattori ambientali esterni (ad esempio una condizione di scarsa visibilità in cui i sensori del veicolo non riescono ad operare correttamente).

Il primo soggetto che viene preso in considerazione è l'utilizzatore, il quale dovrebbe essere in grado di impedire che un malfunzionamento del veicolo cagioni danni altrimenti evitabili nelle ipotesi in cui permanga in capo allo stesso un potere-dovere di intervento, cd. di *override*, sulle scelte della macchina stessa.

Nelle ipotesi base dell'omicidio stradale e delle lesioni personali stradali (contemplate rispettivamente negli artt. 589 bis, comma 1 e 590 bis, comma 1 c.p.)[21] il soggetto attivo del delitto può essere «chiunque» e pertanto, teoricamente, altri rispetto al conducente. La punibilità viene in qualche modo svincolata dall'attività di guida, potendo essere ritenuti responsabili dell'illecito anche coloro su cui incombe una posizione di garanzia protesa alla sicurezza degli utenti della strada. Ne consegue

[21] Sulle fattispecie citate, si veda C. PAVICH, M.V. STURLESE, *Reati stradali. Soluzioni applicative e interpretative*, Giappichelli, Torino, 2018; F. PICCIONI, *L'omicidio stradale. Analisi ragionata della Legge 23 marzo 2016 n. 41*, Giappichelli, Torino, 2016; S. POLLASTRELLI, R. ACQUAROLI, *Il reato di omicidio stradale*, Giuffrè, Milano, 2017; M. NOCERA, *I reati nella circolazione stradale. Alla luce della giurisprudenza*, Dike giuridica, Roma, 2018; G. LOSAPPIO, *Dei nuovi delitti di omicidio e lesioni stradali*, in *Dir. pen. cont.*, 30 giugno 2016; A. MENGHINI, *L'omicidio stradale. Scelte di politica criminale e frammentazione del sistema*, Editoriale Scientifica, Napoli, 2016. Per un commento sulla responsabilità ascrivibile ai veicoli autonomi si veda anche C.G. TERRANOVA, *Responsabilità da circolazione di veicoli*, in *Dig. disc. priv.*, XVII, Torino, 1998, p. 90 ss.; e E.F.D. ENGELHARD, R.W. DE BRUIN, *Liability for damage caused by autonomous vehicles*, Eleven International Publishing, L'Aia, 2019.

che, almeno da un punto di vista soggettivo, i reati in esame parrebbero ascrivibili anche al produttore.

Occorre tuttavia precisare che le fattispecie *ex* art 589 *bis* e 590 *bis* c.p. richiedono una colpa c.d. specifica, concernente la violazione di norme sulla circolazione stradale[22]. Qualora un incidente stradale dipenda dal mancato funzionamento del sistema, che, ad esempio, non abbia segnalato un ostacolo, o non abbia assicurato al veicolo la tenuta della direzione e della velocità dovute, possono certamente ravvisarsi gli estremi della colpa in capo al produttore del veicolo, ma si tratterà di colpa generica, per negligenza o imperizia.

In questo caso la colpa del produttore consisterebbe nella mancata progettazione di un sistema esente da vizi o da difetti che ne hanno comportato il malfunzionamento. Non è stata posta in essere, infatti, ad opera del produttore, alcuna violazione delle norme sulla circolazione stradale. Ciò determina la conseguenza che i reati, eventualmente configurabili in capo ad esso, sono quelli comuni di omicidio colposo o di lesioni personali colpose, puniti meno gravemente delle fattispecie speciali dell'omicidio stradale e delle lesioni personali stradali.

Può senz'altro condividersi l'opinione per cui una responsabilità non sia configurabile per il solo utilizzo del prodotto, ove ciò sia avvenuto conformemente alle informazioni fornite dal produttore, ma presupponga un comportamento attivo di modificazione, di cattivo uso, di omessa o insufficiente custodia del sistema; ancora, in capo all'utilizzatore che mantenga un dominio sulle funzioni esercitate dalla macchina o quantomeno un potere di intervento sulle stesse, a rilevare sarebbe un'omessa o insufficiente supervisione: un addebito di responsabilità, rispettivamente a titolo omissivo e attivo, ben potrebbe configurarsi in caso di omessa attivazione a fronte di un prevedibile fallimento del sistema che renda inoperante l'affidamento dell'utente

[22] Ai sensi dell'art. 589 *bis* c.p. «chiunque cagioni per colpa la morte di una persona con violazione delle norme sulla disciplina della circolazione stradale è punito con la reclusione da due a sette anni». Analogamente, l'art. 590 *bis* prevede che «Chiunque cagioni per colpa ad altri una lesione personale con violazione delle norme sulla disciplina della circolazione stradale è punito con la reclusione da tre mesi a un anno per le lesioni gravi e da uno a tre anni per le lesioni gravissime».

circa il funzionamento dello stesso in conformità agli standard di diligenza ovvero a causa di un errore commesso al momento di riassumere il controllo[23].

In questo contesto, si evidenzia l'importanza di definire un livello minimo di violazione cautelare che possa giustificare l'attribuzione di una responsabilità penale, concentrandosi su casi di colpa grave. Questo concetto implica una significativa sottovalutazione o minimizzazione dei rischi associati alla guida autonoma, in contrasto con gli obblighi di garanzia imposti al produttore.

Considerando le peculiarità del settore, l'intervento punitivo dovrebbe essere limitato a situazioni che rappresentino un disvalore rilevante, prevedibile e incoerente con gli obiettivi di miglioramento della sicurezza. In tal senso, potrebbero essere riprese le riflessioni della dottrina penalistica sulla colpa medica, che suggeriscono di restringere la responsabilità ai comportamenti che non solo deviano da quanto richiesto, ma che comportano rischi irragionevoli.

La ragionevolezza del pericolo residuo associato alla guida autonoma sarà il criterio centrale per delineare un'area di rischio accettabile, guidata da linee-guida di settore oggettive, a cui si aggiungeranno, nei momenti più critici del processo di validazione dei veicoli *smart*, profili di colpa particolarmente qualificati. Se i soggetti coinvolti rispettano questi confini, eventuali danni causati da errori dell'intelligenza artificiale non daranno luogo a responsabilità penale, pur attivando meccanismi risarcitori e compensativi di tipo oggettivo, garantendo così una protezione adeguata per le potenziali vittime. Ad esempio, con riferimento al conducente, i suoi compiti dovrebbero essere limitati alla verifica delle condizioni ambientali prima di attivare il sistema di guida autonoma e, una volta attivato, al monitoraggio costante del veicolo, rimanendo pronto a intervenire in caso di emergenza che il sistema non riesca a gestire.

Non dovrebbe, tuttavia, essere attribuita alcuna colpa al conducente per il modo in cui ha gestito un'eventuale emergenza una volta che questa si è verificata. Valutare l'efficacia di singole azioni o manovre compiute in tali circostanze particolari comporterebbe un giudizio altamente imprevedibile e arbitrario, rischiando di trasformare il

[23] C. MINELLI, *La responsabilità "penale" tra persona fisica e corporation,* cit. p. 58 ss.

conducente in un capro espiatorio per eventi che sfuggono al suo controllo diretto[24]. Come già precisato, il principale vantaggio sociale previsto dai veicoli autonomi è un significativo miglioramento della sicurezza stradale. Lo sviluppo di tali veicoli contribuirà a rendere le strade più sicure, rappresentando quindi un progresso positivo e rilevante anche dal punto di vista precauzionale. Considerando questo aspetto, sarà necessario trovare un equilibrio tra l'esigenza di protezione pubblica e collettiva da una parte, e, dall'altra, quella privata e individuale.

1.3. Le implicazioni etiche

Il caso di Elaine Herzberg[25] è stato uno dei primi incidenti mortali causati da un'automobile a guida autonoma.

Nel marzo 2018, a Tempe, in Arizona, mentre la Herzberg spingeva una bicicletta attraverso una strada a quattro corsie, fuori dalle strisce pedonali venne investita da un'auto delle società Uber e Velodyne che stava operando in modalità guida autonoma con un autista seduto al posto di guida (livello 3).

L'autista della macchina non intervenne in tempo per impedire la collisione. Infatti, solo 1,3 secondi prima dell'impatto il sistema avvertì il conducente di operare una frenata di emergenza, troppo tardi per evitare il pedone. La macchina aveva classificato la Herzberg in un primo momento come un oggetto sconosciuto, successivamente come un veicolo, e solo alla fine come una bicicletta. Questo perché il sistema

---

[24] M. LANZI, *Self-driving cars e responsabilità penale. La gestione del rischio stradale nell'era dell'intelligenza artificiale*, Giappichelli, Torino, 2023, p. 292.

[25] Sulla vicenda, si veda M. SALTORI, *Come decide un'auto senza pilota chi muore in un incidente stradale*, *online* sul sito *web* www.thevision.com; L. COEN, *Uccisa dall'auto autonoma. Pedone vittima di Uber. L'incidente di Uber. Negli Usa una donna è stata investita da una vettura che eseguiva un test senza pilota*, in *Il Fatto Quotidiano*, 20 marzo 2018, p. 13 ss.; W. PAVIA, *Driverless Uber car 'not to blame' for woman's death*, in *The Times*, 21 marzo 2018; D. WAKABAYASHI, *Self-Driving Uber Car Kills Pedestrian in Arizona, Where Robots Roam*, in *The New York Times*, 19 marzo 2018; M. HARRIS, *Exclusive: Arizona governor and Uber kept self-driving program secret, emails reveal*, in *The Guardian*, 28 marzo 2018; B. VLASIC, N.E. BOUDETTE, *Self-Driving Tesla Was Involved in Fatal Crash, U.S. Says*, in *The New York Times*, 30 giugno 2016; F. KUNKLE, *Fatal crash with self-driving car was a first - like Bridget Driscoll's was 121 years ago with one of the first cars*, in *Washington Post*, 22 marzo 2018.

installato non era programmato per riconoscere i pedoni al di fuori delle strisce pedonali.

L'evento appena descritto ha provocato un vivace dibattito in dottrina, circa l'individuazione del soggetto cui ascriverne causalmente la colpa[26].

Una responsabilità potrebbe essere riconosciuta in capo al produttore del sistema, che non ha programmato l'auto in modo da individuare ed evitare una serie sufficientemente vasta di pericoli. Inoltre, si è anche paventata la responsabilità del conducente che, nell'immediatezza dell'urto, verosimilmente a causa di un momento di distrazione, non fece in tempo a prendere il controllo del veicolo.

La vicenda si è conclusa senza risvolti di natura penale contro le società coinvolte. Nel 2019 il procuratore dell'Arizona stabilì che Uber non fosse penalmente responsabile per l'incidente. La società fu però indagata dalla *National Transportation Safety Board*[27], e dal procedimento emersero una serie di problemi e irregolarità in relazione alla sicurezza del sistema.

Quanto alla causa civile intentata dalla famiglia Herzberg, questa è stata risolta con il versamento di una somma non nota da parte di Uber. In seguito, la società ha interrotto la sperimentazione sui veicoli senza conducente e ha venduto la sua divisione dedicata alla guida autonoma.

La vicenda ha sollevato vari interrogativi circa la possibilità per il mezzo autonomo di gestire i comportamenti, non sempre prevedibili, dell'utente umano. Per garantire un grado di sicurezza adeguato, il sistema dovrà essere progettato per riconoscere e reagire al maggior numero possibile di pericoli che possono incontrarsi nella circolazione stradale, nonché per scegliere quali principi seguire qualora si trovi di fronte ad uno scenario imprevisto.

---

[26] Sul punto si veda C. TELESCA, *«Driverless Cars»: profili di responsabilità civile e penale*, in *Riv. Dir. Nav.*, 2019, p. 183; C. SEVERONI *Prime considerazioni su un possibile inquadramento giuridico*, cit., p. 352 ss; N. BUSTO, *Carta europea sulla robotica: una proposta di roboethics per le self driving car*, in *Ciberspazio e dir.*, 2017, p. 289 ss.

[27] Il *National Transportation Safety Board* è un'agenzia federale indipendente incaricata dal Congresso di indagare su ogni incidente dell'aviazione civile negli Stati Uniti ed eventi significativi negli altri modi di trasporto. Si occupa di determinare le probabili cause degli incidenti ed emette raccomandazioni di sicurezza volte a prevenire eventi futuri.

È noto, tuttavia, che le decisioni che l'utente della strada si trova a prendere, spesso esulano da una semplice applicazione meccanica delle leggi sulla circolazione stradale. Al sistema dovrà essere insegnato anche a compiere delle scelte etiche o di convenienza[28], soprattutto nel caso in cui si trovi di fronte ad una situazione in cui non vi sia alcuna possibilità di evitare un incidente mortale: il sistema potrebbe essere progettato per sacrificare una persona al fine di salvarne cinque, o per sacrificare un adulto al fine di salvare un bambino.

Molti studiosi cercano di proporre soluzioni al problema delle decisioni etiche che le intelligenze artificiali devono affrontare, concentrandosi su questioni morali come il celebre dilemma del carrello[29], che viene spesso declinato nella forma di una scelta tragica: decidere, ad esempio, se un veicolo autonomo debba investire un gruppo di pedoni per salvaguardare i passeggeri a bordo o viceversa. Una delle varianti più discusse riguarda la priorità normativa che dovrebbe essere data in base all'età delle persone coinvolte, spingendo alcuni a suggerire che le leggi debbano prioritariamente minimizzare i danni ai bambini, privilegiando quindi una scelta in base alla presenza numerica di minori tra i passeggeri o tra i pedoni. Questa riflessione etica

[28] In tal senso si veda G. BASILE, *La roboetica. Una nuova scienza?*, in *L'Arco di Giano*, 2008, p. 11 ss.; R. MANZOTTI, V. TAGLIASCO, *Etica delle macchine e «coscienza artificiale»*, in *L'Arco di Giano*, 2008, p. 33 ss.; G. TADDEI ELMI, F. ROMANO, *Il robot tra ius condendum e ius conditum*, in *Inf. dir.,* 2016, p. 115 ss.; J. BONNEFON, A. SHARIFF, I. RAHWAN, *The social dilemma of autonomous vehicles*, in *Science*, Vol. 352, 24 giugno 2016, p. 1573 ss.; T. CASADEI, G. ZANETTI, *Tra dilemmi etici e potenzialità concrete: le sfide dell'autonomous driving*, in S. Scagliarini (a cura di), *Smart roads e driverless cars: tra diritto, tecnologie, etica pubblica*, cit., p. 41 ss.; G. FORNASARI, *Dilemma etico del male minore e ticking bomb scenario. Riflessioni penalistiche (e non) sulle strategie di legittimazione della tortura*, Edizioni Scientifiche, Napoli, 2020.

[29] Il noto «dilemma del carrello» venne formulato da Philippa Ruth Foot nel 1967: l'autista di un tram conduce un veicolo capace solo di cambiare rotaia (tramite deviatoio), senza la possibilità di frenare. Sul binario percorso si trovano cinque persone legate e incapaci di muoversi e il tram è diretto verso di loro. Tra il tram e le persone legate si diparte un secondo binario parallelo, sul quale è presente una persona legata e impossibilitata a muoversi. La persona nei pressi del deviatoio si trova di fronte un'alternativa che comporta due sole opzioni: lasciare che il tram prosegua dritto la sua corsa, uccidendo le cinque persone, oppure azionare lo scambio e ucciderne una sola. Immaginiamo ora che quel tram sia stato progettato per viaggiare senza un conducente, e che quindi debba scegliere da solo se cambiare binario o no. Dovrà essere, ab origine, il programmatore a operare la scelta etica proposta dal dilemma, e quindi «insegnare» al veicolo, ad esempio, di sacrificare una persona per salvarne cinque. Per un approfondimento, si veda L. BRUSCO, *Il dilemma morale del carrello. Una vivace ricostruzione storica*, in *Diritto & questioni pubbliche*, 1/2016, p. 16 ss.; S. MARCHIORI, P. SOMMAGGIO, *Break the chains: a new way to consider machine's moral problems*, in *BioLaw Journal*, 3/2018, p. 15 ss.

viene talvolta utilizzata come argomento per richiedere regolamentazioni specifiche che indirizzino tali decisioni[30].

L'etica invita ad una riflessione argomentata che ha lo scopo di intervenire sui precetti morali che dovrebbero orientare le nostre azioni in diverse situazioni. Questo porta all'emergere di punti di riferimento che guidano il comportamento umano. Questi punti di riferimento, distintivi di una società, di una comunità, di una cultura, sono plurali ed evolutivi, nonché difficili da elaborare in quanto nessuno può pretendere di possedere la legittimità sufficiente per governare il comportamento altrui. Risulta pertanto complicato insegnare ad un sistema di IA ad operare una scelta etica.

Per mettere in discussione l'etica dell'IA, occorre innanzitutto accettare il principio secondo il quale tutti i diritti e gli obblighi giuridici applicabili a queste tecnologie e ai loro usi sono obbligatori e devono essere debitamente rispettati. L'IA non nasce in un mondo senza leggi. Ad essa si applica un vasto *corpus* di norme vincolanti, sia a livello europeo che a livello nazionale e internazionale. Ma queste norme non sono necessariamente adeguate. E l'etica è stata concepita come un movente per valutarle. Affinché lo sviluppo, la distribuzione e l'uso dei sistemi di intelligenza artificiale avvengano in un contesto di conformità, è necessario fornire loro un quadro giuridico appropriato[31].

Un gruppo di esperti di alto livello sull'intelligenza artificiale istituito dalla Commissione europea ha predisposto delle linee guida in materia di etica[32]. Esse promuovono una cultura dell'«intelligenza artificiale degna di fiducia per l'Europa» a beneficio dei cittadini nel rispetto dei loro diritti fondamentali, della democrazia e dello stato di diritto. Un tale risultato si potrebbe ottenere attraverso una normazione dell'etica,

---

[30] Sul punto si veda U. RUFFOLO, *Intelligenza Artificiale, "machine learning" e responsabilità da algoritmo*, cit., p. 1702.

[31] B. BARRAUD, *Éthique de l'intelligence artificielle*, in *Le droit d'aujourd'hui*, L'Harmattan, Parigi, 2022, p. 52.

[32] La Commissione europea ha nominato un gruppo di esperti incaricato di fornire consulenza sulla sua strategia di intelligenza artificiale. Durante il primo anno del suo mandato, il gruppo di esperti ad alto livello sull'intelligenza artificiale (*AI HLEG*) ha lavorato a delle «linee guida etiche per un'IA affidabile», presentando 33 raccomandazioni per guidare l'IA affidabile verso la sostenibilità, la crescita, la competitività e l'inclusione.

accompagnata dalla creazione di autorità che possano attestare che il sistema agisca in modo conforme all'etica stessa, che sia trasparente, responsabile e giusto[33].

Da qui la necessità di leggi chiare e precise, ma soprattutto univoche riguardo alle decisioni da insegnare ai sistemi di IA al fine di non lasciare questi dubbi alla libera scelta dei vari programmatori.

Tuttavia, ad oggi, aspettarsi che un sistema di IA sia in grado di prendere decisioni etiche basate, ad esempio, sull'identificazione dell'età di ciascuna persona coinvolta, appare forse troppo pretenzioso. Questa aspettativa non solo rallenterebbe significativamente lo sviluppo dell'IA, ma introdurrebbe anche nuovi rischi di fallibilità. Già oggi, il riconoscimento accurato e il conteggio dei pedoni rappresentano una sfida tecnologica complessa, e pare essere ancora più irrealistico e fantascientifico pensare che l'IA possa censire con precisione età, sesso, statura, e distinguere tra bambini e adulti in tempo reale.

Nei prossimi anni, in un contesto di convivenza tra auto a guida autonoma e veicoli guidati da esseri umani, il conducente del veicolo *self-driving* dovrà essere ritenuto responsabile per eventuali errori di guida automatizzata allo stesso modo in cui è responsabile un conducente umano che guida senza assistenza. Questo scenario è attualmente regolato dalla già citata Convenzione di Vienna del 1968, che richiede la presenza di un conducente a bordo.

Questa responsabilizzazione comporta la difficoltà di chiedere ai sistemi di guida autonoma di rispondere in modo differente rispetto a come farebbe un guidatore umano di fronte a dilemmi etici complessi, come il già citato dilemma del carrello.

Nel periodo di transizione, in cui coesisteranno veicoli a guida autonoma e auto guidate da esseri umani, sarà dunque auspicabile che la programmazione del sistema segua gli stessi criteri di correttezza richiesti a un normale guidatore umano. Ciò significa che il comportamento del sistema di guida autonoma non potrà essere orientato esclusivamente da principi etici ideali, ma piuttosto da *standard* pratici e giuridici già applicati agli esseri umani.

---

[33] C. CASTETS-RENARD, J. EYNARD, *Un droit de l'intelligence artificielle, Entre règles sectorielles et régime général, perspectives compares*, Bruylant, Bruxelles, 2023.

In altre parole, il sistema dovrà adottare decisioni che riflettano una guida prudente e responsabile, come farebbe un buon conducente, anche se tali scelte non sempre coincidono con il massimo etico atteso. Questo comporta che, di fronte a dilemmi etici complessi, come la scelta tra il salvare pedoni o gli occupanti del veicolo, l'algoritmo potrebbe non essere in grado di adottare la soluzione ideale sotto un profilo morale, ma dovrà rispondere in modo conforme alle norme e alle aspettative imposte ai conducenti umani.

1.4. La paura della società

Tra i profili più problematici nell'ambito della circolazione dei veicoli autonomi c'è sicuramente il fatto che la loro catena di sviluppo è estremamente complessa e frammentata, rendendo difficile, come già evidenziato in precedenza, un accertamento affidabile e prevedibile dell'allocazione di responsabilità in caso di danni causati dal veicolo. Il processo di progettazione del *software* e dell'*hardware* che compongono un mezzo intelligente coinvolge un numero imprecisato di attori diversi, e la complessità degli algoritmi di IA rende spesso impossibile individuare con precisione le cause di un evento dannoso[34].

Inoltre, è importante riconoscere che, pur aumentando la sicurezza stradale nel complesso, i veicoli autonomi introdurranno inevitabilmente rischi del tutto nuovi rispetto a quelli legati ai mezzi tradizionali. Sebbene molti incidenti tipici delle auto convenzionali saranno evitati, emergeranno comunque altre situazioni pericolose, che non si sarebbero mai verificate senza la presenza delle auto a guida autonoma.

Ciò accade, principalmente, perchè sistemi di IA sono «intelligenti» nel momento in cui tutti gli utenti della strada rispettano le norme sulla circolazione. Quando

[34] Questo è uno dei motivi per cui, come vedremo nel prosieguo, la proposta di Direttiva in materia di danni da intelligenza artificiale rinuncia a richiedere l'esatto accertamento del nesso causale tra la colpa del produttore e il danno causato dal mezzo intelligente, presumendo invece la sussistenza di tale nesso.

alcuni soggetti non si attengono alle regole – come nella vicenda della Herzberg – può accadere che il sistema non riesca a reagire in tempo.

Se da un lato l'introduzione di agenti intelligenti nell'ambito della circolazione stradale è sempre più massiccia, non si può ipotizzare una integrale sostituzione degli utenti umani, che continueranno a circolare nelle strade per molto tempo, come conducenti o come pedoni[35]. È dunque necessario favorire una interazione di tali utenti, e prevedere regole di comportamento che siano compatibili con le caratteristiche di entrambe le categorie di destinatari, così da garantire reciprocamente la prevedibilità dei comportamenti altrui.

Di qui la necessità di una disciplina in grado di tener conto di questa complessa realtà, che si proietta negli anni futuri, per favorirne un equilibrato sviluppo, senza bloccarlo per l'eccessivo timore della nuova tipologia di rischi che si possono prospettare[36].

Nello specifico, anche assumendo il punto di vista delle possibili vittime, si deve infatti considerare che l'automazione è diretta ad elevare il livello complessivo di sicurezza del traffico ed a ridurre il numero degli incidenti, proprio evitando o limitando considerevolmente quelli causati da errori umani, che ne rappresentano la maggioranza.

È cruciale che i criteri per attribuire la responsabilità penale nella circolazione dei veicoli autonomi siano coordinati a livello internazionale[37]. Tale armonizzazione

---

[35] Sul punto si veda M.E. MCGRATH, *Autonomous Vehicles, Opportunities, Strategies and Disruptions*, Independent Publishing Platform, Varsavia, 2018; M. CAMERON, *Realising the potential of Driverless Vehicles*, Createspace independent publishing, Wellington, 2018; A. HERRMANN, W. BRENNER, R. STADLER, *Autonomous Driving, How the Driverless Revolution Will Change the World*, Emerald Publishing Limited, Bingley, 2018.

[36] Sul punto si veda 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. 21.

[37] In effetti, è ormai ampiamente riconosciuta dalla dottrina penale nazionale l'esistenza di un diritto penale europeo, il quale deriva sia dalle influenze che il diritto dell'Unione esercita sui singoli ordinamenti nazionali – soprattutto attraverso l'obbligo di interpretazione conforme e la disapplicazione delle norme interne in contrasto con il diritto UE – sia dagli interventi diretti dell'Unione nel campo penale. Questi interventi si manifestano mediante l'introduzione di obblighi di tutela adeguata e Direttive mirate ad armonizzare i vari ordinamenti nazionali rispetto a specifiche tipologie di reati. Per un approfondimento sul diritto penale europeo si veda A. PAGLIARO, *Limiti all'unificazione del diritto penale europeo*, in *Riv. trim. dir. pen. econ.*, 1/1993, p. 199 ss.; S. MANACORDA, voce *Diritto penale*

è fondamentale, non solo per rispondere all'esigenza dei produttori di operare all'interno di un quadro normativo coerente, ma anche per agevolare lo sviluppo e la commercializzazione delle tecnologie di guida intelligente.

Con l'accentramento del rischio legale, compreso quello penale, che vedrà la responsabilità spostarsi dagli attuali milioni di conducenti a un ristretto gruppo di dirigenti delle principali aziende del settore, emerge la necessità di stabilire in modo chiaro e globale le «regole del gioco». Questa chiarezza normativa è essenziale per garantire la prevedibilità delle conseguenze giuridiche e penali degli incidenti causati da veicoli dotati di intelligenza artificiale[38].

A tal proposito, come già precisato nel capitolo precedente, il 13 marzo 2024 la Commissione europea con l'*AI Act* ha introdotto nel diritto comunitario una definizione dei sistemi di IA neutra dal punto di vista tecnologico e ne ha stabilito una classificazione basata su requisiti e obblighi diversi secondo un approccio *risk-based*. I sistemi di intelligenza artificiale che comportano rischi considerati inaccettabili saranno vietati. Saranno invece autorizzati una vasta gamma di sistemi di IA ad alto rischio, purché rispettino specifici requisiti e obblighi per poter operare nel mercato

europeo, in *Enciclopedia Treccani*, 2014; J. DELLA VALENTINA, *L'insostenibile leggerezza del principio di prevedibilità di fronte al "diritto penale europeo"*, in *Dir. pen. cont.*, 3/2023, p. 76 ss.; F. SGUBBI, voce *Diritto penale comunitario*, in *Dig. disc. pen.*, IV, Utet Giuridica, Milano, 1990, p. 89 ss.;. L. EUSEBI, *Quale diritto penale nel futuro europeo?*, in *Criminalia*, 2020, p. 87 ss.; V. MANES, M. CAIANIELLO, *Introduzione al diritto penale europeo*, Giappichelli, Torino, 2020, p. 3 ss.; C. SOTIS, *Il diritto senza codice. Uno studio sul sistema penale europeo vigente*, Giuffrè, Milano, 2007; G. SALCUNI, *L'europeizzazione del diritto penale: problemi e prospettive*, Giuffrè, Milano, 2011; G. GRASSO, R. SICURELLA, *Lezioni di diritto penale europeo*, Giuffrè, Milano, 2007; S. RIONDATO, *Competenza penale della Comunità europea. Problemi di attribuzione attraverso la giurisprudenza*, CEDAM, Padova, 1996; E. MILITELLO, *Recenti novità in tema di diritto penale europeo*, in *Cass. pen.,* 4/2017, p. 1640 ss.; G. SALCUNI, *Culture penalistiche a confronto: diritto penale nazionale vs diritto penale europeo*, in *Arch. pen.*, 2/2011, p. 445 ss.; G. GRASSO, *Il Trattato di Lisbona e le nuove competenze penali dell'Unione*, in M. Bertolino, L. Eusebi, G. Forti (a cura di), *Studi in onore di Mario Romano*, vol. IV, Jovene, Napoli, 2011, p. 2326 ss.; A. MONTAGNA, *Il difficile cammino verso un diritto penale europeo minimo*, in *Cass. pen.*, 2/2007, p. 805 ss.; P. VELTEN, *Diritto penale europeo*, in *Criminalia*, 2006, p. 125 ss.; S. MOCCIA, *La politica criminale del Corpus Juris: dal Corpus Juris al diritto penale europeo?*, in *Ind. pen.*, 3/2001, p. 1425 ss.; A. BERNARDI, *Corpus Juris e formazione di un diritto penale europeo*, in *Riv. it. dir. pubbl. com.*, 2/2001, p. 283 ss.; G. FUGGETTI, *Possibilità e limiti di un diritto penale europeo*, in *Ind. pen.*, 1/1999, p. 445 ss.; S. CRISPINO, *Interpretazione conforme al diritto europeo e internazionale in materia penale*, in *Ars Interpretandi*, 1/2019, p. 171 ss.

[38] Sul punto si veda M. LANZI, *Self-driving cars e responsabilità penale,* cit., p. 281.

dell'UE. I sistemi con rischi limitati dovranno invece solamente seguire alcuni obblighi di trasparenza[39].

Questa nuova legge, rivoluzionaria nell'ambito dell'intelligenza artificiale, porrà le basi per poter regolare anche gli ambiti più specifici, come quello di cui si è trattato nelle pagine precedenti. Grazie ad una base legale definita si potranno tipizzare gli elementi essenziali per fondare, e nel contempo circoscrivere, le indispensabili «posizioni di garanzia» facenti capo a soggetti che possano e debbano essere in grado di controllare adeguatamente le specifiche «fonti di rischio» per cui sono competenti, fino ai possibili esiti «imprevedibili» delle decisioni di comportamenti di guida concretamente prese ed attuate dai veicoli a conduzione automatica[40].

A seconda delle posizioni e funzioni svolte dagli enti ed agenti umani coinvolti, occorre poi stabilire regole cautelari chiare ed espresse, che circoscrivano il concreto perimetro della eventuale responsabilità di ciascuno per gli eventi avversi a titolo di colpa, da adattare alle peculiarità ed agli sviluppi delle tecnologie che vengono o dovrebbero essere applicate.

2. Navi autonome

2.1. Nascita e sviluppo delle navi-drone

Lo sviluppo tecnologico ha interessato anche il comparto marittimo. La timida comparsa delle c.d. navi drone[41] potrebbe un domani incidere sulla navigazione

[39] T. MADIEGA, *Artificial intelligence act*, Briefing 28 giugno 2023, sul sito *web* www.europarl.europa.eu.

[40] Per un approfondimento sulle nuove prospettive si veda R. COMPOSTELLA, *Auto a guida autonoma e diritto penale. Profili di responsabilità individuale e collettiva*, Editoriale Scientifica, Napoli, 2024.

[41] Sul punto si veda L. ANCIS, *Navi pilotate da remoto e profili di sicurezza della navigazione nel trasporto di passeggeri*, in *Dir. trasp*., 2019, p. 428 ss.; P. ZAMPELLA, *Navi autonome e navi pilotate da remoto, spunti per una riflessione*, in *Dir. trasp.* 2019, p. 588 ss.; R. TRANQUILLI LEALI, *La tutela della sicurezza dei passeggeri nel trasporto marittimo tra comandante della nave e pilota da remoto*, in *Dir. trasp.* 2019, p. 471 ss.; S. AHVENJÄRVI, *The Human Element and Autonomous Ships,* in *Transnav,* 10/2010, p. 519 ss.; C. SEVERONI, *Soccorso e mezzi di trasporto autonomi,* in *Dir. trasp.,* 2018, p. 72 ss.

marittima, considerato che potrebbe risultare sempre meno necessaria la presenza di un equipaggio addetto al comando a bordo, grazie a sistemi che consentono il governo delle unità da remoto, le comunicazioni a lunga distanza e un calcolo sempre più preciso della posizione.

Il diffondersi di questo fenomeno porta con sé varie conseguenze. Occorre considerare, in primo luogo, l'impatto negativo in campo sociale e occupazionale: è facilmente intuibile, in proposito, che per la fornitura di alcuni servizi a bordo non sarà più necessaria l'opera dell'uomo; così come è prevedibile che emergeranno molteplici difficoltà nell'individuare di volta in volta la legislazione applicabile e, ove necessario, apportare i relativi adeguamenti.

Tuttavia, nonostante i rischi appena descritti, vanno evidenziati i rilevanti benefici che possono derivare da una navigazione sempre più automatizzata. Le avanzate tecnologie di cui disponiamo, infatti, possono migliorare la sicurezza marittima, contribuendo in misura significativa alla riduzione degli incidenti in mare, attualmente provocati nell'80% dei casi dal fattore umano, come causa unica o unitamente ad altri fattori[42].

Altri vantaggi consistono nell'ottimizzazione delle rotte, nel miglioramento del rapporto tra velocità e consumo di carburante, contribuendo così a ridurre l'impatto ambientale del trasporto marittimo. Pertanto, incentivando l'adozione di queste tecnologie si promuove non solo la sicurezza ma anche la sostenibilità del settore.

Le navi autonome rappresentano dunque una promettente evoluzione nel settore dalla navigazione marittima, ma richiedono un significativo adattamento normativo al fine di regolamentare in modo efficace questa nuova tecnologia. La definizione della responsabilità, la conformità ai trattati internazionali e la protezione dei dati sono solo alcune delle questioni giuridiche che richiedono attenzione.

Così come per i veicoli che circolano su strada, anche in questo caso una delle principali problematiche legate al traffico delle navi autonome riguarda la

[42] M. MUSI, *The phenomenon of «mass»: is it time to rethink the current maritime liability regime?,* in *Riv. Dir. Nav.*, 2/2021, p. 763 ss.; M. R. GRECH – T. J. HORBERRY – T. KOESTER, *Human Factor in the Maritime Domain*, *Boca Raton*, 2008; L. ANCIS, *Navi pilotate da remoto e profili di sicurezza della navigazione nel trasporto di persone*, cit., p. 433 ss.

determinazione della responsabilità in caso di incidenti e danni, soprattutto perché con equipaggi ridotti o assenti, diventa complicato stabilire chi debba essere chiamato a rispondere in caso di collisioni e danni a terzi. Le leggi marittime dovranno affrontare tale questione con l'obiettivo di definire, nella misura più precisa possibile, il soggetto cui debba essere attribuita la colpa: il proprietario, il produttore dei sistemi di automazione, o altri attori coinvolti.

2.2. La normativa di riferimento

Nel diritto marittimo non sono riscontrabili precisi riferimenti a mezzi nautici che navigano privi di un comando a bordo. Negli anni Trenta si paventò l'ipotesi di adibire al traffico commerciale navi definite «senza equipaggio», che in quel momento erano costruzioni manovrate a distanza grazie al collegamento con una «nave madre» munita di equipaggio [43].

Nuove sperimentazioni si ebbero intorno al secondo dopoguerra con le prime navi gestite tramite pannello di controllo, fino ad arrivare ai primi prototipi di *Unmanned Surface Vessel (UMV)*, senza equipaggio e pilotati a distanza[44].

Nelle più recenti accezioni terminologiche le navi che presentano tali caratteristiche vengono definite autonome (anche dette navi drone). Con questa espressione si indicano quelle unità che utilizzano avanzati sistemi di automazione, intelligenza artificiale, sensori e tecnologie di guida autonoma che consentono di operare senza la necessità di un equipaggio a bordo[45].

---

[43] U. LA TORRE, *Navi senza equipaggio e shore control operator*, in *Dir. trasp.*, 2019, p. 487 ss. Per un approfondimento si veda anche S. CRISAFULLI BUSCEMI, *Alcune considerazioni sulla situazione giuridica delle navi manovrate da lontano*, in *Studi in onore di F. Berlingieri*, Pubblicazione dell'Associazione Italiana di Diritto Marittimo, Genova, 1933, p. 191 ss.; E. VAN HOOYDONK, *The law of unmanned merchant shipping - an exploration*, in *JIML*, 20/2014, p. 404 ss.; R. VEAL, M. TSINPLIS RINGBOM*, The navigation of Unmanned ships into the lex maritima,* in *LMLQ*, 2017, p. 303 ss.

[44] G.M. BOI, *«Navi-drone»: primi interrogativi in tema di disciplina giuridica*, in *Riv. Dir. Nav.,* 2017, p. 175 ss.

[45]Per un approfondimento sulle navi unmanned si veda, fra tutti, M. MUSI, *The phenomenon of «mass»: is it time to rethink the current maritime liability regime?,* cit., p. 763 ss.; M.M. COMENALE PINTO,

Queste navi hanno molteplici possibilità di utilizzo in diversi settori marittimi, tra cui il trasporto merci, la navigazione passeggeri, la ricerca oceanografica e la sorveglianza in mare.

Sebbene il loro sviluppo non sia stato rapido come quello dei veicoli autonomi aerei e terrestri[46], anche nell'ambito della navigazione marittima le tecnologie che prevedono una guida autonoma stanno acquisendo un ruolo sempre più importante.

Il crescente successo degli *UMV*, nelle loro varie forme, è dovuto in gran parte alla varietà di usi a cui, da qualche tempo, sono stati destinati, tra i quali possiamo ricordare la mappatura dei fondali, il posizionamento di cavi sottomarini, la manutenzione di piattaforme petrolifere e oleodotti, la ricerca di relitti, lo sviluppo degli studi scientifici, oltre a finalità militari (spionaggio, sminamento, sorveglianza)[47].

Sistemi di bordo anticollisione e relative problematiche giuridiche, in *Studi in onore di Umberto Leanza*, Editoriale Scientifica, Napoli, 2008, p. 1595 ss.; L. ANCIS, *Navi pilotate da remoto e profili di sicurezza della navigazione nel trasporto di passeggeri*, cit., p. 427 ss.; B. GOGARTY, M. HAGGER, *The Laws of Man over Vehicles Unmanned: the Legal Response to Robotic Revolution on Sea, Land and Air*, in *JLawInfoSci*, 19/2008, p. 73 ss.; B. GOGARTY, I. ROBINSON, *Unmanned Vehicles: a (Rebooted) History, Background and Current State of the Art*, in *JLawInfoSci*, 21/2012, p. 1 ss.; G. HALLEVY, *Unmanned Vehicles: Subordination to Criminal Law under the Modern Concept of Criminal Liability. Comment*, in *JLawInfoSci*, 21/2012, p. 200 ss.; R. MCLAUGHLIN, *Unmanned Naval Vehicles at Sea: USVs, UUVs, and the Adequacy of the Law*, in *JLawInfoSci*, 21/2012, p. 100 ss.; G. M. BOI, *«Navi-drone»: primi interrogativi in tema di disciplina giuridica*, cit., p. 175 ss.; U. LA TORRE, *Navi senza equipaggio e shore control operator*, cit., p. 487 ss.; F. SICCARDI, *Le navi autonome. Maritime Autonomous Surface Ships (MASS)*, in *Dir. mar.*, 2019, p. 848 ss.

[46] Con riferimento ai veicoli autonomi terrestri e aerei si veda *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, *on line* sul sito *web* www.sae.org, aggiornato al 30 aprile 2021; D.G. GLEAVE, R. FRISONI, A. DALL'OGLIO, C. NELSON, J. LONG, C. VOLLA, D. RANGHETTI, S. MCMINIMY, *Self Piloted Cars: the Future of Road Transport?, Research for the Transport and Tourism Committee of the EuropeanParliament*, cit.; L. PICOTTI, *Profili di responsabilità penale per la circolazione di veicoli a guida autonoma*, cit.; G. CALABRESI, E. AL MUREDEN, *Driveless cars, Intelligenza artificiale e futuro della mobilità*, cit.; A. BERTOLINI, *Robotsas Products: The Case for a Realistic Analysis of Robotic Application and Liability Rules*, cit., p. 214 ss.; E. AL MUREDEN, *Sicurezza "ragionevole" degli autoveicoli e responsabilità del produttore nell'ordinamento giuridico italiano e negli Stati Uniti*, cit., p. 1505 ss.; K. VAN WEES, K. BROOKHUIS, *Product Liability for ADAS: legal and human factors perspectives*, cit., p. 357 ss.; A. BERTOLINI, E. PALMERINI, *Regulating robotics: A challenge for Europe*, cit., p. 169 ss.; J. MANIKA, *Big Data: the next frontier for innovation, competition and productivity,* cit.; S. STEFANIZZI, *Riflessioni metodologiche sul concetto e sull'uso dei Big Data*, cit., p. 17 ss.; C. SEVERONI, *Prime considerazioni su un possibile inquadramento giuridico e sul regime di responsabilità nella conduzione dei veicoli a guida autonoma*, cit., p. 331 ss..

[47] Forse il settore militare è quello in cui le navi autonome sono più utilizzate. Queste sono già oggi utilizzate per missioni di *intelligence*, sorveglianza e ricognizione grazie all'utilizzo di sensori *radar*, *sonar* e sistemi di *imaging* che consentono di rilevare minacce, raccogliere informazioni e trasmetterle a basi di comando in tempo reale. In particolare, Gli *UMV* sono impiegati per la rilevazione e la

Tuttavia, il loro utilizzo nel trasporto commerciale di merci e passeggeri è ancora agli inizi, anche se alcuni dei primi prototipi sono già stati costruiti e testati, mentre altri sono in fase di realizzazione. La particolare rilevanza del problema e la sua portata mondiale hanno spinto le istituzioni europee e le organizzazioni internazionali ad attivare progetti ad hoc e gruppi di ricerca. La Commissione europea ha promosso e cofinanziato il «*Maritime Unmanned Navigation through Intelligence in Networks*» (MUNIN) *Project*, destinato a sviluppare e verificare un «*concept*» per una nave autonoma, definita come un veicolo guidato principalmente da sistemi di decisione automatizzati a bordo ma controllata da un operatore remoto in una stazione di controllo a terra[48].

A livello internazionale, l'IMO[49] ha inserito nel suo Piano Strategico 2018-2023 l'obiettivo di «Integrare le tecnologie nuove e in progresso nel quadro normativo» allo scopo di studiare gli effetti che esse possono avere nei confronti della sicurezza, l'ambiente, l'agevolazione degli scambi, i costi di spedizione e del personale di bordo e di terra[50].

---

neutralizzazione delle mine marine, senza mettere a rischio l'equipaggio umano. Un altro impiego è quello di individuare e tracciare sottomarini nemici. Il programma *ACTUV* (*Anti-Submarine Warfare Continuous Trail Unmanned Vessel*) è un esempio di progetto volto a costruire navi in grado di seguire sottomarini a grande distanza senza assistenza umana diretta, sviluppato dall'agenzia *DARPA* (*Defense Advanced Research Projects Agency*).

[48] Si veda il sito *web* del progetto, dove si legge «*The project MUNIN – Maritime Unmanned Navigation through Intelligence in Networks – is a collaborative research project, co-funded by the European Commissions under its Seventh Framework Programme. MUNIN aims to develop and verify a concept for an autonomous ship, which is defined as a vessel primarily guided by automated on-board decision systems but controlled by a remote operator in a shore side control station*». Per un approfondimento v. H. C. BURMEISTER, W. BRUHN, Ø. J. RØDSETH, T. PORATHE, *Autonomous Unmanned Merchant Vessel and its Contribution towards the e-Navigation Implementation: The MUNIN Perspective*, in *International Journal of e-Navigation and Maritime Economy*, 1/2014, p. 1 ss. Di interesse altresì il documento redatto in sede CMI, *International Working Group Position Paper on Unmanned Ships and the International Regulatory Framework*, consultabile sul sito *web* www.comitemaritime.org.

[49] L'IMO, o *International Maritime Organization* (Organizzazione Marittima Internazionale), è un'agenzia delle Nazioni Unite fondata nel 1948 e operativa dal 1959, che si occupa di sicurezza in ambito marittimo. L'IMO stabilisce *standard* globali per la sicurezza della navigazione e la prevenzione dell'inquinamento marino causato dalle navi. Le sue convenzioni principali includono la *Convenzione SOLAS* (*Safety of Life at Sea*), che regola la sicurezza della navigazione, e la *MARPOL* (*Marine Pollution*), volta alla prevenzione dell'inquinamento causato dalle navi.

[50] M. MUSI, *The phenomenon of «mass»: is it time to rethink the current maritime liability regime?,* cit., p. 765.

Nel 2017 il Comitato per la sicurezza marittima (MSC) dell'IMO ha così messo all'ordine del giorno uno studio, ancora in corso, volto a verificare se, come ed entro quali limiti i cosiddetti «strumenti IMO» siano in grado di fornire un adeguato quadro normativo per le attività di un «*Maritime Autonomous Surface Ship*» (o «MASS»), definito come «una nave che, in varia misura, può operare indipendentemente dall'interazione umana»[51].

Il Comitato ha chiarito anche quali sono i vari gradi di autonomia delle navi *unmanned*:

- Grado uno, con forte automazione: nave con processi automatizzati e supporto decisionale; l'equipaggio è a bordo per operare e controllare i sistemi e le varie funzioni. Alcune operazioni possono essere automatizzate e talvolta senza supervisione, ma con l'equipaggio pronto a prendere il controllo.
- Grado due, controllo a distanza ma con equipaggio a bordo: la nave è condotta e gestita da un'altra posizione. I marittimi sono a bordo per assumere il controllo, ove si renda necessario, e gestire i sistemi e le funzioni del natante.
- Grado tre, controllate a distanza e prive di equipaggio: la nave è condotta e gestita da un'altra posizione. Non ci sono marittimi a bordo.
- Grado quattro, completamente autonome: il sistema operativo della nave è in grado di prendere decisioni e determinare azioni da solo[52] .

---

[51] IMO, *Press briefing* n. 8 del 25 maggio 2018, sul sito *web* www.imo.org. Sull'argomento v. anche l'ordine del giorno della riunione dell'organismo interno IMO *Maritime SafetyCommitee* (MSC) del 16-25 maggio 2018, sessione n. 99, disponibile sul sito *web* dell'IMO.

[52] R. VEAL, M. TSIMPLIS, A. SERDY, S. QUINN, A. NTOVAS, *Liability for Operation in Unmanned Maritime Vehicles with Differing Levels of Autonomy*, Institute of Maritime Law, Brussels, 2016; S. OTA, *Identification of IMO Regulations relating to Unmanned Operations of Maritime Autonomous Surface Ships – SOLAS Convention and Related Mandatory IMO instruments*, in *Papers of National Maritime Research Institute*, 17/2018, p. 227 ss.; R. VEAL, *Maritime Autonomous Surface Ships: Autonomy, Manning and the IMO*, in *ShipTL*, 2018, p. 1 ss.; M. SHIOKARI, S. OTA, *Considerations on the Regulatory Issues for realization of Maritime Autonomous Surface Ships*, in *J. Physics: Conference Series*, 2019, p. 1 ss.; E. RINGBOM, *Regulating Autonomous Ships – Concepts, Challenges and Precedents*, in *Ocean Dev. Intern. Law*, 2/2019, p. 1 ss.; Z. PIETRZYKOWSKI, J. HAJDUK, *Operations of Maritime Autonomous Surface Ships*, in *Int'l J. Marine Nav. &Safety Sea Transp.*, 13/2019, p. 725 ss.

Allo stato attuale, risulta difficile immaginare l'esistenza di un'unità appartenente all'ultima categoria, completamente autonoma, in grado di elaborare i propri processi decisionali e agire di conseguenza. La navigazione è ben più complessa della guida su strada, e sarebbe impensabile che una nave possa muoversi senza nessun controllo da parte dell'uomo, soprattutto in aree marine particolarmente trafficate, durante le operazioni di attracco o di utilizzo di canali artificiali[53].

Solo nel caso di traffici di linea regolari le direttive dell'armatore potrebbero essere inserite nel sistema di controllo e sarebbe ipotizzabile una conduzione della nave in completa autonomia, adattata alla situazione ambientale e metereologica in corso, ma sarebbe comunque difficile pensare ad una unità con determinazioni e azioni del tutto proprie[54].

Per tale ragione parte della dottrina ritiene preferibile definire gli UMV come unità «*capable of controlled, self propelled movement on the water in the absence of any on board crew*»[55], sottolineando che l'autonomia del veicolo non riguarda il processo decisionale, ma la capacità di muoversi in ambiente acqueo e seguire una rotta a prescindere dalla presenza di personale a bordo.

Attualmente, pertanto, quando si parla di navi autonome ci si riferisce, realisticamente, a quelle che, durante la navigazione e con esclusione delle fasi più critiche, risultino manovrate a distanza oppure siano monitorate da uno *Shore Control Center* (SCC, Centro di controllo a terra), ovvero da un gruppo di persone in grado di assumerne il controllo diretto ogni qual volta necessario.

Questo SCC comprende al suo interno varie figure con ruoli e responsabilità definiti, nonché un soggetto con un ruolo di decisione e coordinamento degli altri operatori, responsabile di ciò che accade nel Centro di Controllo, il *remote controller*.

---

[53] L. ANCIS, *Navi pilotate da remoto e profili di sicurezza della navigazione nel trasporto di passeggeri*, cit., p. 439 ss.

[54] U. LA TORRE, *Navi senza equipaggio*, cit., p. 516 ss.

[55] R.VEAL-H. RINGBOM, *Unmanned ships and the international regulatory framework*, in *Journal of International Maritime Law*, 2017, p. 100 ss.; L. ANCIS, *Navi pilotate da remoto e profili di sicurezza della navigazione nel trasporto di passeggeri*, cit., p. 433 ss.

Tenendo conto dei ruoli della SCC, essa si assume la responsabilità per l'operazione e le conseguenze del funzionamento della nave autonoma[56].

È evidente come l'evoluzione tecnologica in atto stia profondamente modificando la percezione finora acquisita della nozione di nave, essendo gli UMV privi di una caratteristica che, nonostante i notevoli cambiamenti che ha subito negli ultimi due secoli, era sempre stata preservata: la presenza dell'elemento umano. Pertanto, tra gli interrogativi a cui devono rispondere le istituzioni europee vi è anche quello di valutare l'opportunità di assoggettare o meno queste nuove forme di unità al diritto marittimo internazionale, ora applicabile alle navi con equipaggio, o se sia più corretto considerare una nuova nozione di nave, per non dover affrontare le conseguenze di un pericoloso vuoto normativo sostanziale.

2.3. Configurabilità di una responsabilità penale.

In caso di eventi dannosi che siano stati causati da una nave autonoma, soprattutto per quelle con grado di automazione più elevato, occorre chiedersi chi sia responsabile.

Anche qui vale lo stesso discorso svolto nei paragrafi precedenti con riferimento alle *self-driving cars*. La loro autonomia, allo stato attuale, non può essere idonea ad ascrivere una responsabilità penale.

La responsabilità delle «scelte» operate dal sistema di IA sarà quindi da attribuire ad un agente umano, attraverso una ricostruzione dei diversi contributi causali che hanno portato alla condotta posta in essere dal sistema. D'altronde, il fattore umano, seppur ridimensionato, continua a svolgere un ruolo importante nella direzione di operazioni a controllo remoto o nella programmazione dei sistemi di navigazione.

In questo contesto, la sfida più cruciale e complessa è quella dell'identificazione dei soggetti verso i quali deve essere incanalata la responsabilità per il funzionamento

[56] Le procedure operative effettive del SCC sono descritte in un documento intitolato «*MUNIN D.8.8: Final Report: Shore Control Centre*», disponibile sul sito *web*: www.unmanned-ship.org.

di un *UMV* e della relativa disciplina applicabile, per la quale devono essere adottati criteri calibrati sul diverso tipo di figura interessata. I soggetti umani che operano attraverso i sistemi di IA possono essere considerati come autori mediati dei fatti agli stessi riconducibili. In tale contesto occorrerà arginare la tendenza ad una diffusione della responsabilità tra i vari soggetti che hanno avuto un ruolo nell'avvenimento[57].

Anche se viene attivato il sistema di navigazione autonoma, vi è sempre un soggetto umano che deve assumere una posizione di controllo sul natante. È la stessa convenzione SOLAS a richiedere (reg. 14) che «*from the point of view of the safety of life at sea all ship shall be sufficiently and efficiently manned*». Tale soggetto è, spesso, difficilmente individuabile, soprattutto perché l'attuale normativa sulla navigazione marittima e le conseguenti attribuzioni di responsabilità presuppongono la presenza a bordo di un comandante[58].

Mancando, a bordo degli UMV, una figura analoga, occorre fare riferimento a coloro che sono incaricati di controllare e gestire i sistemi autonomi, e quindi il SCC e il *remote controller*. La definizione del ruolo di quest'ultimo non è ancora oggetto di specifiche previsioni normative.

Rimane quindi il dubbio se il *remote controller* possa essere considerato come un comandante vero e proprio, con conseguente applicazione analogica della normativa concernente la formazione, l'addestramento e l'aggiornamento, nonché la forma giuridica con cui lo stesso potrà operare[59]. In alternativa, qualora una simile estensione non sia praticabile, si potrebbe valutare la possibilità di creare una normativa *ad hoc* per questa nuova figura.

In caso di violazione dell'obbligo di sorveglianza, può sorgere una forma di responsabilità colposa omissiva per non aver impedito l'evento dannoso, dal momento

---

[57] C. MINELLI, *La responsabilità "penale" tra persona fisica e corporation*, cit., p. 55 ss.

[58] U. LA TORRE, *Comando e comandante nell'esercizio della navigazione*, Edizioni Scientifiche, Napoli, 1997, p. 8 ss.; E. SPASIANO, *Comandante della nave o dell'aeromobile*, in *Enc. dir. VII*, 1960, p. 688 ss.; U. LA TORRE, *Funzione di comando e sicurezza della navigazione*, in E. Turco Bulgherini, F. Salerno (a cura di), *Infrastrutture e navigazione: nuovi profili della sicurezza marittima ed aerea*, Aracne, Roma, 2013, p. 92 ss.; F.A. QUERCI, *La figura giuridica del comandante di nave e aeromobile*, Giuffrè, Milano, 1964; R. TRANQUILLI LEALI, *Lineamenti della comunità viaggiante nel diritto della navigazione*, Roma, 1982, p. 31 ss.; U. LA TORRE, *Equipaggio, comando e determinazione della rotta nella navigazione marittima*, in *Riv. Dir. Nav.,* 2013, p. 95 ss.

[59] G. BOI, *Navi drone*, cit., p. 187.

che il soggetto preposto al controllo assume un obbligo cosiddetto di protezione, che si configura come un obbligo giuridico di impedire qualunque evento penalmente rilevante che possa derivare dalla navigazione[60]. Può senz'altro condividersi l'opinione per cui una responsabilità di colui che è preposto al controllo del natante sia configurabile in caso di inadempimento dell'obbligo di protezione; a rilevare sarebbe una trascurata o insufficiente supervisione, ovvero una omessa attivazione a fronte di un pericolo[61].

Tuttavia, nonostante il controllo attivo del soggetto a ciò preposto, l'incidente potrebbe verificarsi anche per un malfunzionamento del sistema, per errori nei programmi informatici o per illecite intrusioni da parte di *hacker*[62]. In tali ipotesi, se l'errore non può essere rimproverato direttamente al sistema di IA, non resta che valutare la possibilità di attribuire la responsabilità al proprietario dell'unità o al programmatore del *software*.

In tal caso, tra le cause del danno potrebbe esservi un difetto di programmazione o di costruzione, i quali possono anche interagire *pro quota* (art. 41, commi 1 e 3 c.p.),

---

[60] Per un approfondimento sui reati omissivi impropri, e in particolare sulle posizioni di garanzia v. G. MARINUCCI, E. DOLCINI, G. L. GATTA, *Manuale di Diritto Penale. Parte Generale*, cit., p. 279 ss.; F. MANTOVANI, *Diritto Penale. Parte generale*, XI ed., CEDAM, Padova, 2020, p. 675 ss. In particolare, quanto agli obblighi di protezione nell'ambito del diritto marittimo v. F. BENATTI, *Osservazioni in tema di doveri di protezione*, in *Riv. trim. dir. proc. civ.*, 1960, p. 1342 ss.; C. CASTRONOVO, *Obblighi di protezione e tutela del terzo*, in *Jus*, 1976, p. 123 ss.; S. CICARELLO, *Dovere di protezione e valore della persona*, Giuffrè, Milano, 1988; F. BENATTI, *Doveri di protezione*, in *Dig. civ.,* VII, Utet Giuridica, Torino, 1990, p. 221 ss.; L. LAMBO, *Obblighi di protezione*, CEDAM, Padova, 2007; A. ASQUINI, *La responsabilità del vettore per infortunio del viaggiatore*, in *Riv. dir. comm.*, 2/1919, p. 350 ss.; S. ZUNARELLI-A. ROMAGNOLI, *Contratto di trasporto marittimo di persone*, Giuffrè, Milano, 2012, p. 110 ss.; L. TULLIO, *L'obbligazione di protezione nel trasporto marittimo ed aereo*, in *Dir. trasp.*, 2013, p. 349 ss.

[61] C. MINELLI, *La responsabilità "penale" tra persona fisica e corporation,* cit., p. 58. La tendenza del legislatore a punire di fronte ad un pericolo si spiega in chiave prevalentemente preventiva. In quest'ottica il pericolo è protagonista e viene ricollegato il più delle volte, sul piano del fatto tipico, a una condotta di tipo omissivo e sul piano soggettivo alla colpa. Quest'ultima può derivare da precise posizioni di garanzia: gli obblighi di protezione riguardano la tutela di uno o più beni che fanno capo a singoli soggetti o a una determinata categoria di soggetti nei confronti di una gamma più o meno ampia di pericoli, mentre gli obblighi di controllo hanno per oggetto la neutralizzazione dei pericoli derivanti da una determinata fonte, in funzione di tutela di chiunque possa essere messo a repentaglio da quella fonte di pericolo. Sul punto si veda anche G.P. DEMURO, *Il pericolo e la sua pena: tra proporzionalità e ne bis in idem*, in *Riv. it. dir. e proc. pen.*, 2023, p. 903.

[62] G. BOI, *Navi drone*, cit., p. 195.

nonché fattori ambientali esterni (ad esempio una condizione di scarsa visibilità in cui i sensori non riescono ad operare correttamente).

Una volta attribuita la responsabilità nel caso concreto, occorre valutare quale sia la disciplina applicabile. In tal senso potrebbe rendersi necessario adeguare l'attuale quadro normativo al nuovo fenomeno degli *UMV*, per poi realizzare tutti gli interventi di adattamento e aggiornamento necessari.

2.4. Il nuovo omicidio nautico.

Una volta determinato cosa si intenda per *UMV*, è necessario comprendere se ad esse sia applicabile la disciplina attualmente riferita alle sole unità con equipaggio, e quindi valutare se si tratti o meno di navi in senso giuridico[63].

Sul piano terminologico, dalla definizione contenuta nell'art. 136 cod. nav. si trae che «Per nave s'intende qualsiasi costruzione destinata al trasporto per acqua, anche a scopo di rimorchio, di pesca, di diporto, o ad altro scopo». La giurisprudenza sul punto rapporta la nozione di nave ad ogni «imbarcazione atta al trasporto di più persone, qualunque sia la sua stazza o la sua portata, il mezzo di propulsione utilizzato (remi, vela, motore) e la sua funzione (diporto, ecc.)»[64].

Ai sensi del comma 1 *bis* (inserito dal D.lgs. n. 229 del 2017) dell'articolo 1 del codice della nautica da diporto, le disposizioni di detta normativa si applicano alle unità di cui all'articolo 3 dello stesso codice che navigano in acque marittime e interne, fermo restando quanto previsto dall'art. 3 della legge n. 172 del 2003 (Disposizioni

---

[63] L. ANCIS, *Navi pilotate da remoto e profili di sicurezza della navigazione nel trasporto di passeggeri*, cit., p. 440. Sulla nozione di nave v. M. MUSI, *La nozione di nave*, in *Il diritto marittimo – quaderni*, Bologna, 2020; S. ZUNARELLI – M. M. COMENALE PINTO, *Manuale di diritto della navigazione e dei trasporti. Vol. I*, CEDAM, Padova, 2023; G. RIGHETTI, *Trattato di diritto marittimo*, Giuffrè, Milano, 1987, p. 913 ss.; G. VERMIGLIO, *La nave e l'aeromobile*, in L. Tullio, M. Deiana (a cura di), *Il cinquantenario del Codice della navigazione*, ISDIT, Cagliari, 1993, p. 114 ss.; M. CARRETTA, *La nave*, in A. Antonini (a cura di), *Trattato breve di diritto marittimo*, I, Giuffrè, Milano, 2007, p. 299 ss.

[64] V. Cass. pen., 15 maggio 1987, n. 10391, in *Giur. it.*, 1988, II, 375; Cass. pen., 24 aprile 1963, n. 852 in *DeJure.it*; Cass. pen., 14 dicembre 1971, n. 1588, in *DeJure.it*; Cass. pen. 30 maggio 2019, n. 27225, in *DeJure.it*.

per il riordino e il rilancio della nautica da diporto e del turismo nautico) in relazione alle navi destinate esclusivamente al noleggio per finalità turistiche, nonché quanto previsto dal decreto-legge n. 457 del 1997 (Disposizioni urgenti per lo sviluppo del settore dei trasporti e l'incremento dell'occupazione), istitutivo del registro delle navi adibite alla navigazione internazionale (c.d. Registro internazionale), nel quale sono iscritte, a seguito di specifica autorizzazione del Ministero dei trasporti, le navi adibite esclusivamente a traffici commerciali internazionali. Nessun riferimento è fatto, dunque, alla necessaria presenza di un equipaggio a bordo.

Già con riferimento ai veicoli autonomi che circolano su strada la dottrina si è chiesta quale normativa potesse essere applicata in caso di eventi dannosi dai quali derivasse la morte di un soggetto coinvolto nell'incidente. Un'ipotesi avanzata era quella di ricondurre il fatto nel campo di applicazione dell'articolo 589 *bis* del codice penale, rubricato (prima della recente modifica) «omicidio stradale»[65]. Difatti, il mancato riferimento nel testo del citato articolo alla figura del conducente umano a bordo del veicolo, lasciava aperta la possibilità di interpretare estensivamente la disposizione, facendo rientrare nel concetto di responsabile anche figure non direttamente legate all'incidente, come il proprietario del veicolo o il programmatore del software[66].

[65] Per un approfondimento sulla fattispecie dell'omicidio stradale v. M. MANTOVANI, *In tema di omicidio stradale*, in *Dir. Pen. Cont.*, 9 dicembre 2015; P. PISA, *L'omicidio stradale nell'eclissi giurisprudenziale del dolo eventuale*, in *Dir. pen. e proc.*, 2016, p. 145 ss.; G. LATTANZI, *L'omicidio stradale. Relazione al convegno sul tema "Ipotesi su una nuova figura di reato: l'omicidio stradale – Napoli 7 marzo 2014"*, in *Cass. pen.*, 2014, p. 1988 ss.; D. D'AURIA, *Le modifiche apportate alla materia della circolazione stradale*, in *Dir. pen. e proc.*, 2010, p. 1274 ss.; E. SQUILLACI, *Ombre e (poche) luci nella introduzione dei reati di omicidio e le personali lesioni stradali*, in *Dir. Pen. Cont.*, 18 aprile 2016; *Omicidio stradale e lesioni personali stradali: le linee guida della Procura di Trento*, in *Dir. Pen. Cont.*, 5 aprile 2016; A. MASSARO, *Omicidio stradale e lesioni personali stradali gravi o gravissime: da un diritto penale "frammentario" a un diritto penale "frammentato"*, in *Dir. Pen. Cont.*, 20 maggio 2016, p. 6 ss. Per una casistica giurisprudenziale relativa all'ambito della circolazione stradale v. A. CANEPA, *L'imputazione soggettiva della colpa. Il reato colposo come punto cruciale nel rapporto tra illecito e colpevolezza*, Torino, Giappichelli, 2011, p. 110 ss.; I. GIUGNI, *Causalità della colpa e circolazione stradale tra prassi applicative e dubbi irrisolti*, in *Dir. Pen. Cont.*, 1/2019, p. 6 ss.

[66] Per un approfondimento sul ruolo del conducente e del programmatore v. M. M. COMENALE PINTO – E. G. ROSAFIO, *Responsabilità civile per la circolazione degli autoveicoli a conduzione autonoma. Dal grande fratello al grande conducente*, in *Dir. trasp.*, 2/2019, p. 373 ss.

La disposizione in esame è stata recentemente modificata[67] con l'istituzione della nuova fattispecie di omicidio nautico[68], che abbraccia quelle ipotesi in cui l'evento mortale si verifica non sulle strade ma sulle acque, in relazione alla navigazione in mare, laghi o fiumi.

Prima della riforma un riferimento ad incidenti navali si aveva già nel delitto di naufragio, contemplato nella forma dolosa all'art. 428 c.p. e in quella colposa all'art. 449 c.p. Per naufragio[69] si intende la perdita di una nave per una causa violenta (urto, collisione, esplosione) che ne provochi l'affondamento, lo sfascio, l'arenamento[70]; la giurisprudenza ricomprende nel naufragio anche la semplice inutilizzabilità, cioè l'impossibilità per la nave di galleggiare e navigare regolarmente, non richiedendo la vera e propria perdita del natante.

La modifica dell'art. 589 *bis* c.p. è finalizzata proprio ad ovviare ad un vuoto legislativo, non essendo presente fino ad oggi una normativa *ad hoc* rivolta ai responsabili di eventi mortali avvenuti durante la navigazione[71].

Occorre però chiedersi se questa nuova figura di omicidio nautico possa essere applicata anche nel caso in cui il fatto sia cagionato nell'ambito della navigazione di una nave autonoma.

---

[67] La proposta di legge (A.C. n. 911 d'iniziativa dei senatori Balboni e Liris) è stata approvata in via definitiva dalla Camera il 20 settembre 2023.

[68] G.P. DEMURO, *Uguali ma diversi: sul reato di omicidio stradale o nautico*, in *Sistema Penale*, 21 settembre 2023.

[69] Per una ricostruzione storica, S. FERRARINI, *Note sul concetto di naufragio*, in *Riv. Dir. Nav.*, 1963, p. 90 ss.

[70] S. ARDIZZONE, voce *Naufragio, disastro aviatorio, disastro ferroviario*, in *Dig. disc. pen*., VIII, Utet Giuridica, Torino 1994, p. 224 ss.; S. CORBETTA, *I delitti contro l'incolumità pubblica*, in G. Marinucci, E. Dolcini (a cura di), *Trattato di Diritto penale. Parte speciale*, II, CEDAM, Padova, 2003, p. 365 ss.; A. GARGANI, *Reati contro l'incolumità pubblica,* in C.F. Grosso, T. Padovani, A. Pagliaro (a cura di), *Trattato di Diritto penale. Parte speciale*, IX, Giuffrè, Milano 2008, p. 329 ss.; M. GRIGOLI, voce *Naufragio (dir. nav.)*, in *Enc. dir.,* XXVII, Milano, 1977, p. 559 ss.; F. TRONCONE, *Il delitto di naufragio colposo: una fattispecie di nuovo attuale*, in *Studi Marittimi*, 1996, p. 46 ss.

[71] A. ROIATI, *L'introduzione dell'omicidio stradale e l'inarrestabile ascesa del diritto penale della differenziazione*, in *Dir. Pen. Cont.*, 1° giugno 2016, p. 3 ss.; D. PULITANÒ, *Tensioni vecchie e nuove sul sistema penale*, in *Dir. pen. e proc.*, 2008, p. 1081 ss.

Come già precisato, la legge non fa alcun riferimento alla necessaria presenza di un equipaggio a bordo per definire l'oggetto della normativa riguardante la navigazione.

Inoltre, il testo dell'articolo recita «Chiunque cagioni per colpa la morte di una persona con violazione delle norme sulla disciplina della circolazione stradale o della navigazione marittima o interna è punito con la reclusione da due a sette anni». La dicitura «chiunque cagioni» lascia aperta la strada ad una molteplicità di interpretazioni, in quanto «chiunque» può certamente essere il comandante, ma anche colui che a distanza deve controllare il sistema di navigazione autonoma, o ancora il programmatore del sistema stesso.

Almeno sul piano terminologico, pertanto, sembra che nulla osti all'estensione dell'applicabilità dell'omicidio nautico alle navi *unmanned*.

Ciò che può, invece, creare dubbi di compatibilità è il richiamo alla colpa per violazione delle norme sulla disciplina della navigazione marittima o interna. A tal proposito è utile riportare brevemente le considerazioni svolte con riferimento all'omicidio stradale, che possono valere anche per la fattispecie in esame.

Infatti, la fattispecie ex art 589 *bis* richiede una colpa c.d. specifica, concernente appunto la violazione di norme positive, relative alla navigazione marittima o interna[72].

Occorre, preliminarmente, comprendere quali siano le disposizioni cui la riforma fa riferimento, difficilmente individuabili a causa del fatto che si tratta di normative multilivello. Ciò è esplicitato nella documentazione del Servizio Studi della

[72] Per un approfondimento sulla nozione di colpa specifica v. M. GROTTO, *Principio di colpevolezza, rimproverabilità soggettiva e colpa specifica*, cit., p. 259 ss.; E. PENCO, *Limiti-soglia e responsabilità colposa. Il ruolo incerto delle soglie quantitative, dalla colpa specifica al rischio consentito*, cit., p. 195 ss.; G. AMATO, *Un impianto diretto a considerare solo la colpa specifica*, cit., p. 55 ss.; A.M. BONANNO, *Protocolli, linee guida e colpa specifica*, cit., p. 441 ss.; S. PUGNO, *Accertamento del nesso di causalità e colpa specifica nella circolazione stradale*, cit., p. 2254 ss.; G. MARINUCCI, *La responsabilità colposa: teoria e prassi*, cit.; D. CASTRONUOVO, *La colpa penale*, cit., pp. 345 e 535; T. PADOVANI, *Il grado della colpa*, cit., p. 818 ss.; F. GIUNTA, *Illiceità e colpevolezza nella responsabilità colposa*, cit., p. 334 ss.; D. CASTRONUOVO, *L'evoluzione teorica della colpa penale tra dottrina e giurisprudenza*, cit.; N. MAZZACUVA, *L'apparente prossimità della colpa penale a garantismo e ultima ratio*, cit. p. 41 ss.; S. THOBANI, *Percorsi giurisprudenziali in tema di accertamento dell'elemento soggettivo della P.A.: colpa generica e colpa specifica*, cit., p. 189 ss.

Camera dei deputati sull'introduzione del reato di omicidio nautico e del reato di lesioni personali nautiche. Innanzitutto, deve farsi riferimento alle disposizioni del codice della navigazione (R.D. n. 327 del 1942) e dell'apposito regolamento attuativo (d.P.R. n. 631 del 1949, concernente approvazione del regolamento della navigazione interna), del codice della nautica (D.lgs. n. 171/2005) e del diritto civile (art. 1, c. 2 codice della navigazione).

La violazione di queste regole ben potrebbe integrare una forma di colpa specifica, assimilabile alla fattispecie ex art. 589 *bis* c.p..

Tale discorso ovviamente vale sia per le navi con equipaggio sia per quelle autonome. Quanto a queste ultime, tuttavia, la situazione è complicata dal fatto che manca una esaustiva disciplina *ad hoc*, delle regole cautelari positive, codificate, che tengano in considerazione le specificità della navigazione autonoma. Per tale ragione, ancora più ampia è la sfera di operatività della colpa generica in luogo di quella specifica, e di conseguenza paiono limitate le ipotesi in cui al responsabile di un evento dannoso derivato dalla navigazione di un UMV possa essere ascritto il reato di cui all'art. 589 *bis* c.p.

Ebbene, qualora un incidente dipenda dal mancato funzionamento del sistema e si ritenga responsabile, ad esempio, il produttore del *software*, oppure il *remote controller*, potranno certamente ravvisarsi gli estremi della colpa in capo a questi ultimi, i quali tuttavia non hanno violato una norma della navigazione: piuttosto avranno commesso un errore nella programmazione o nell'installazione del software o nel controllo della nave per negligenza, imprudenza o imperizia. Non si tratterà, dunque, di un'ipotesi di colpa specifica (come quella richiesta dall'art. 589 bis c.p.), quanto piuttosto di colpa generica, per la mancata progettazione di un sistema esente da vizi o da difetti che ne hanno comportato il malfunzionamento o per il mancato controllo sulla navigazione[73].

[73] Quanto alla nozione di colpa generica v. A. ZACCHIA, *L'individuazione della regola cautelare non scritta in tema di colpa generica*, cit., p. 2114 ss.; F. BASILE, *Fisionomia e ruolo dell'agente-modello ai fini dell'accertamento processuale della colpa generica*, cit., p. 94 ss.; G. MARINUCCI, *La responsabilità colposa: teoria e prassi*, cit., p. 5 ss.; D. CASTRONUOVO, *La colpa penale*, cit., p. 345 ss.; T. PADOVANI, *Il grado della colpa*, cit., p. 818 ss; F. GIUNTA, *Illiceità e colpevolezza nella responsabilità colposa*, cit., p. 334 ss.; D. CASTRONUOVO, *L'evoluzione teorica della colpa penale tra dottrina e giurisprudenza*, cit., p. 1597 ss.; N. MAZZACUVA,

In questo ultimo caso, non sarebbe più applicabile la disciplina ex art. 589 *bis*, il quale richiede espressamente la violazione di una norma positiva (colpa specifica), e non anche qualunque violazione di regole di prudenza, perizia e diligenza. Se l'evento dannoso si è verificato per la violazione di una regola cautelare di esperienza, non scritta, dovrà applicarsi l'ordinaria figura dell'omicidio colposo – punito meno gravemente della fattispecie speciale dell'omicidio nautico – eventualmente in concorso con il reato di naufragio colposo[74].

Tuttavia, si potrebbe valutare l'opportunità di interpretare estensivamente le disposizioni che sono a fondamento della colpa specifica, facendovi rientrare anche le ipotesi di comportamenti negligenti, imprudenti e imperiti commessi da chi aveva il controllo del natante.

A tal fine, possiamo prendere in considerazione una normativa internazionale, il c.d. COLREG72 (*Convention on the International Regulations for Preventing Collisions at Sea*)[75], un insieme di regole cautelari stabilite per prevenire collisioni in mare e garantire la navigazione sicura dei natanti.

Il COLREG 72 copre vari aspetti della navigazione e definisce i diritti e le responsabilità delle navi al fine di evitare collisioni. Comprende regole su luci di navigazione, segnali acustici, diritto di precedenza e comportamento generale delle navi quando si trovano in prossimità l'una dell'altra.

A proposito dell'applicabilità delle disposizioni, la Convenzione precisa che nessuna delle norme contenute nell'atto esonera dall'osservanza di «tutte le precauzioni richieste dall'ordinaria esperienza dei naviganti o dalle speciali circostanze del caso» dovendosi discostare dalle norme di colpa specifica contenute nell'atto quando

L'apparente prossimità della colpa penale a garantismo e ultima ratio, in *Reato colposo e modelli di responsabilità*, cit., p. 41 ss.; S. THOBANI, *Percorsi giurisprudenziali in tema di accertamento dell'elemento soggettivo della P.A.: colpa generica e colpa specifica*, cit., p. 189 ss.

[74] Si avrà concorso tra le due norme nell'ipotesi in cui l'incidente sia dovuto a una collisione che provochi la perdita o l'inutilizzabilità della nave.

[75] Si tratta del Regolamento internazionale per prevenire gli abbordi in mare, (Londra, 20 ottobre 1972), recepito in Italia con legge 1085/1977 ed entrato in vigore nel luglio del 1978.

sopravvengano regole di esperienza che meglio si attagliano al caso concreto per evitare incidenti (regola 2 lett. a e b)[76].

Questa previsione sta a significare che colui che conduce la nave deve seguire le disposizioni del COLREG72 salvo qualora, nel caso concreto, questo non comporti un aumento del rischio. In tali ipotesi, il rispetto delle norme codificate integrerebbe la colpa del soggetto, il quale deve invece comportarsi secondo le regole dell'esperienza, come avrebbe fatto l'agente modello[77].

Come sappiamo, quando si parla di regole di esperienza, di regole cautelari non codificate, si fa riferimento alla colpa generica. In questo ultimo caso, come nell'ipotesi sopra richiamata a proposito della responsabilità del produttore del *software* o del *remote controller*, non sarebbe più applicabile la disciplina ex art. 589 *bis*, il quale richiede espressamente la violazione di una norma positiva, ma dovrà applicarsi l'ordinaria figura dell'omicidio colposo, eventualmente in concorso con il reato di naufragio colposo.

A tal proposito si può ricordare un orientamento giurisprudenziale in tema di circolazione stradale, riferito al comma 2 dell'art. 589 c.p. nella sua formulazione ante 2016. Infatti, prima della riforma che ha introdotto il reato di omicidio stradale, le condotte di omicidio commesso nell'ambito della guida di veicoli erano punite come omicidio colposo aggravato ai sensi dell'art. 589 co. 2, il quale prevedeva che «se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale […] la pena è della reclusione da 2 a 7 anni».

La giurisprudenza aveva affermato, al riguardo, che ai fini della sussistenza dell'aggravante di cui all'art. 589, comma 2, c.p., non è necessaria la violazione di una

[76] Regola 2 del COLREG72: «a) Nessuna delle presenti Regole può esonerare una nave, il proprietario, il comandante o l'equipaggio stesso, dalle conseguenze di qualsiasi negligenza nell'applicazione delle Regole stesse ovvero nell'attenersi a tutte le precauzioni richieste dall'ordinaria esperienza dei naviganti o dalle speciali circostanze del caso. b) Nell'interpretazione e nell'applicazione delle presenti Regole si debbono tenere nel debito conto tutti i pericoli della navigazione e i rischi di abbordaggio, incluse le difficoltà in cui una nave può trovarsi, per le quali è necessario discostarsi dalle Regole stesse allo scopo di evitare un immediato pericolo».

[77] G.P. DEMURO, *Uguali ma diversi: sul reato di omicidio stradale o nautico*, cit.

specifica norma del codice stradale, essendo sufficiente l'inosservanza delle regole di generica prudenza, perizia e diligenza[78].

Tali regole, secondo la Cassazione, devono ritenersi parte integrante della disciplina della circolazione stradale, come si desume dal disposto dell'art. 140 C.d.S., il quale impone un generico dovere per gli utenti della strada di comportarsi in modo da non costituire pericolo o intralcio per la circolazione e in modo da salvaguardare la sicurezza stradale[79]. Il predetto articolo pone dunque una generica regola cautelare, la cui violazione integrerebbe colpa generica, ma che, secondo la Cassazione, assume lo stesso valore della violazione di una disposizione specifica[80].

Possiamo dire che la normativa, in un certo senso, positivizzi le regole cautelari. Applicando lo stesso ragionamento alla normativa del COLREG, la stessa potrebbe essere considerata come una norma che positivizza regole cautelari nell'ambito della navigazione, la cui violazione integrerebbe colpa specifica. Secondo questa interpretazione potrebbe applicarsi la disciplina ex art. 589 bis anche alle navi autonome.

Come già precisato, l'automazione è diretta ad elevare il livello complessivo di sicurezza della navigazione ed a ridurre il numero degli incidenti, con l'obiettivo di evitare o limitare considerevolmente quelli causati da errori umani, che ne rappresentano la maggioranza.

È emerso, tuttavia, che la disciplina esistente sia difficilmente applicabile all'ambito di operatività degli UMV, poiché non tutte le disposizioni attuali sono compatibili con le caratteristiche di queste unità[81]. È necessario, dunque, apportare delle modifiche alla normativa prima che tale particolare tipologia di trasporto diventi più diffusa e non solo una semplice sperimentazione.

---

[78] Sez. 4, n. 356665 del 19/6/20007, Di Toro, Rv. 237453.

[79] L'art. 140 CdS, al primo comma prevede che «Gli utenti della strada devono comportarsi in modo da non costituire pericolo o intralcio per la circolazione ed in modo che sia in ogni caso salvaguardata la circolazione stradale».

[80] Sez. 4, n. 18204 del 15/3/2016, Bianchini, Rv. 266641.

[81] G. BOI, *Navi drone*, cit., p. 198. Per un approfondimento si veda anche S. ROSSI, *Il sistema penale della navigazione. Contributo allo studio del diritto penale marittimo*, Editoriale Scientifica, Napoli, 2020.

3. La responsabilità diretta dei sistemi di intelligenza artificiale

3.1. Machina delinquere potest?

Negli ultimi paragrafi sono stati esplorati i confini della possibile responsabilità penale per eventi dannosi causati da sistemi di guida automatizzati, attribuibili agli esseri umani che hanno progettato e impostato le modalità di funzionamento del veicolo intelligente.

Al termine di questa analisi, emerge una questione forse più rilevante e allo stesso tempo più preoccupante riguardo ai rapporti tra intelligenza artificiale e responsabilità: la possibilità che la decisione dannosa del veicolo autonomo non possa essere attribuita, sotto un profilo causale, a violazioni delle normative per la certificazione del sistema di guida autonoma, né a errori o omissioni da parte dei produttori. In altre parole, potrebbe verificarsi che la decisione del veicolo derivi dalla capacità di elaborazione autonoma del *software* di guida, configurandosi come una scelta del veicolo stesso, piuttosto che degli individui che hanno progettato e certificato i criteri di funzionamento[82].

Anche estendendo l'analisi oltre ai confini della guida autonoma, e prendendo in considerazione tutte le modalità di coinvolgimento di un sistema di IA nella commissione di un reato, ci si potrebbe domandare se non si possa già considerare la possibilità che l'IA stessa possa essere vista come il soggetto colpevole del crimine. Nel momento in cui le decisioni, le valutazioni e i bilanciamenti che conducono alla commissione di un reato non sono più esclusivamente opera dell'uomo, ma sono in parte condivisi o addirittura interamente delegati alla macchina, il processo di attribuzione delle responsabilità diventa inevitabilmente più complesso.

---

[82] Sul punto si veda M. LANZI, *Self-driving cars e responsabilità penale,* cit., p. 273. Per un approfondimento si veda anche G. HALLEVY, *I Robot - I, Criminal: When Science Fiction Becomes Reality: Legal Liability of Al Robots Commiting Criminal Offenses*, in *Syracuse Science and Technology Law Reporter*, 22/2010, p. 1 ss.; G. HALLEVY, *The Criminal Liability of Artificial Inteligence Entitis - from Science Fiction to Legal Social Control*, in *Akron Intelectual Property Journal*, 4/2010, p. 171 ss.

La questione centrale è comprendere quale sia il contenuto dell'obbligo di controllo dell'utilizzatore rispetto al comportamento dell'IA e, in caso di errore o danno, fino a che punto egli sia responsabile.

Quando l'IA riduce il ruolo dell'utilizzatore a una semplice sorveglianza passiva, la responsabilità di quest'ultimo potrebbe essere valutata principalmente in relazione al mancato esercizio di un controllo adeguato, ma solo se esiste un obbligo giuridico di sorveglianza. Questo implica che, se la legge impone all'utilizzatore di monitorare e intervenire sulle azioni dell'IA, la sua responsabilità potrebbe derivare dall'omissione di tale obbligo di vigilanza. Tuttavia, se l'utilizzatore mantiene un ruolo attivo nel processo decisionale e operativo, anche con il supporto dell'IA, egli potrebbe essere considerato responsabile direttamente delle azioni eseguite.

In tale contesto si potrebbe ipotizzare un'estensione analogica delle considerazioni svolte da dottrina e giurisprudenza con riferimento al lavoro in *équipe*, dove identificare il responsabile diventa complesso, soprattutto quando il processo decisionale ed esecutivo è frammentato tra diversi individui[83]. In questi casi, la responsabilità è distribuita tra i vari membri, rendendo difficile individuare chi sia effettivamente il

[83] Di tale avviso è F. BASILE, *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione*, cit., p. 14. Per un approfondimento sull'accertamento della responsabilità penale nell'ambito di un lavoro in équipe si veda P. F. POLI, *Attività medica in "équipe": c'è spazio per il principio di affidamento?*, in *Giur. it.*, 5/2021, p. 1204 ss.; B. ROSSI, *La responsabilità del capo dell'equipe medico-chirurgica*, in *Cass. pen.*, 11/2019, p. 3980 ss.; L. RISICATO, *Linee guida e colpa "non lieve" del medico. Il caso delle attività di équipe*, in *Giur. it.*, 8/2014, p. 2065 ss.; A. MASSARO, *Principio di affidamento e "obbligo di vigilanza" sull'operato altrui: riflessioni in materia di attività medico-chirurgica in équipe*, in *Cass. pen.*, 11/2011, p. 3857 ss.; A. MULÈ, *Attività medica di équipe e responsabilità di componenti per omicidio colposo*, in *Foro it.*, 5/2007, p. 308 ss.; L. GIZZI, *Orientamenti giurisprudenziali in tema di responsabilità medica in équipe*, in *Dir. pen. e proc.*, 6/2006, p. 753 ss.; R. BLAIOTTA, *Sulla colpa nel caso di attività svolta in equipe*, in *Cass. pen*, 3/2000, p. 584 ss.; E. BELFIORE, *Profili penali dell'attività medico-chirurgica in equipe. Sezione I. Evoluzione storico-dogmatica della responsabilità per colpa*, in *Arch. pen.*, 9/1986, p. 265 ss.; A. PROVERA, *Responsabilità medica svolta in èquipe*, in *Riv. it. med. leg.*, 3/2011, p. 822 ss.; L. CORNACCHIA, *Responsabilità penale da attività sanitaria in "équipe"*, in *Riv. it. med. leg.*, 3/2013, p. 1219 ss.; A. M. CARELLA, *Responsabilità per colpa professionale di "equipe" medico-chirurgica*, in *Riv. it. med. leg.*, 4/2019, p. 1560 ss.; G. ROCCHI, *L'interruzione del nesso causale tra condotta ed evento e la posizione di garanzia del capo dell'"équipe" chirurgica*, in *Cass. pen.;* 3/2016, p. 907 ss.; G. D'ARCA, *Profili problematici della responsabilità penale del medico per attività in équipe: successione nella posizione di garanzia e principio di affidamento*, in *Riv. it. med. leg.*, 2/2019, p. 671 ss.; A. M. SALERNO, *Responsabilità medica "in équipe": cooperazione colposa, posizione di garanzia degli organi apicali e principio di auto-responsabilità dei singoli cooperanti*, in *Riv. it. med. leg.*, 2/2014, p. 595 ss.

colpevole. Utilizzando questo schema ai fini della nostra analisi, si potrebbe ipotizzare un'*équipe* che vanti tra i suoi membri non solo esseri umani, ma anche sistemi di intelligenza artificiale.

L'idea di attribuire una forma di personalità giuridica alle intelligenze artificiali e di riconoscere loro una responsabilità penale rappresenta un concetto affascinante, ma attualmente rimane un esercizio teorico più che una reale possibilità di riforma del sistema giuridico. Questo accade perché le IA, allo stato attuale, sono ontologicamente incompatibili con i requisiti essenziali della responsabilità penale.

Perché vi sia responsabilità penale, è necessario che l'agente abbia la capacità di essere rimproverato. La sanzione penale presuppone infatti un soggetto consapevole delle proprie azioni, che sia in grado di comprendere cosa è giusto o sbagliato, e che possa essere influenzato dalla punizione. Le IA, anche le più avanzate, non hanno coscienza o volontà autonoma e sono semplicemente strumenti programmati per eseguire compiti definiti dai loro creatori o utilizzatori.

Come abbiamo visto nel corso della trattazione, nell'attuale contesto tecnologico, i sistemi artificiali agiscono sulla base di algoritmi predeterminati, ma restano privi di intenzionalità o consapevolezza. Pertanto, attribuire loro una responsabilità penale significherebbe andare contro i principi basilari del diritto penale, che richiedono la presenza di dolo o colpa, elementi che mal si attagliano alla natura degli agenti artificiali, indipendentemente dal loro grado di sviluppo o di intelligenza algoritmica[84].

La responsabilità attuale ricade sugli esseri umani che creano, controllano e utilizzano questi sistemi, in quanto un'intelligenza artificiale non può comprendere il significato delle proprie azioni, né essere motivata da punizioni o sanzioni.

La Commissione Europea ha valutato in passato la possibilità di attribuire una personalità giuridica per le IA, soprattutto nei casi di danni causati da *robot* autonomi. Il Parlamento europeo, a tal proposito, con la Risoluzione del 16 febbraio 2017[85],

[84] C. CUPELLI, *La sfida del l'intelligenza artificiale al diritto penale*, in *Sistema penale*, 12 aprile 2023.

[85] V. Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)). In particolare, al punto 59, il Parlamento «invita la Commissione a esplorare, esaminare e valutare, nell'ambito della valutazione d'impatto del suo futuro strumento legislativo, le implicazioni di tutte le soluzioni giuridiche possibili, tra cui […] f) l'istituzione di uno *status* giuridico specifico per i *robot* nel lungo termine,

seppur con riferimento alle sole norme di diritto civile, ha proposto alla Commissione Europea l'adozione di un quadro normativo volto a regolare le interazioni tra gli esseri umani e le IA, con un'attenzione particolare ai robot autonomi. Il Parlamento ha suggerito di considerare la possibilità di attribuire una sorta di personalità giuridica ai *robot* avanzati, al fine di chiarire le responsabilità in caso di danni causati da essi. Ciò consentirebbe di stabilire una responsabilità civile specifica per i *robot* autonomi, similmente a quanto avviene per le persone giuridiche.

Il Comitato economico e sociale europeo (CESE), nel suo Parere del 31 agosto 2017[86], ha espresso una chiara opposizione alla proposta del Parlamento. Il CESE ritiene che attribuire una personalità giuridica ai *robot* comporterebbe il rischio che i costruttori o utilizzatori di tali tecnologie si sottraggano alla responsabilità per eventuali danni causati dai *robot*, trasferendo questa responsabilità alla macchina stessa. Precisa, inoltre, che l'attribuzione della responsabilità civile ha anche una funzione di prevenzione, che incoraggia comportamenti corretti. Se detta responsabilità civile non

di modo che almeno i *robot* autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il riconoscimento della personalità elettronica dei *robot* che prendono decisioni autonome o che interagiscono in modo indipendente con terzi».

[86] V. Parere del Comitato economico e sociale europeo su «L'intelligenza artificiale - Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società» (2017/C 288/01). Al punto 3.33. si legge: «Si discute molto sulla questione di chi debba essere ritenuto responsabile se un sistema di IA causa un danno. In particolare, nei casi in cui si tratti di sistemi che apprendono autonomamente e continuano ad apprendere anche dopo la loro messa in funzione. Il Parlamento europeo ha formulato delle raccomandazioni concernenti norme di diritto civile sulla robotica, proponendo di esaminare l'opportunità di introdurre il concetto di «personalità elettronica» per i *robot*, in modo tale che essi possano essere ritenuti civilmente responsabili degli eventuali danni causati. Il CESE è contrario all'introduzione di una forma di personalità giuridica per i *robot* o per l'IA (o i sistemi di IA), in quanto essa comporterebbe un rischio inaccettabile di azzardo morale. Dal diritto in materia di responsabilità civile deriva una funzione preventiva di correzione del comportamento, la quale potrebbe venir meno una volta che la responsabilità civile non ricade più sul costruttore perché è trasferita al *robot* (o al sistema di IA). Inoltre, vi è il rischio di un uso inappropriato e di abuso di uno status giuridico di questo tipo. In questo contesto, il confronto con la responsabilità limitata delle società è fuori luogo, in quanto è sempre la persona fisica a essere responsabile in ultima istanza. A tale riguardo, si dovrebbe esaminare in che misura la normativa nazionale e dell'UE vigente e la giurisprudenza in materia di responsabilità (per danno da prodotti difettosi e di rischio) e colpa propria sia sufficiente a rispondere a tale questione e, in caso contrario, quali soluzioni si impongano sul piano giuridico».

ricadesse più sui costruttori o utilizzatori, ma fosse trasferita ai *robot*, questa funzione correttiva potrebbe essere compromessa.

3.2. Tesi dottrinarie al riguardo

È evidente il pericolo che uno *status* giuridico attribuito ai *robot* o ai sistemi di IA possa essere utilizzato in maniera impropria o abusato. Il CESE sottolinea che il confronto con la responsabilità limitata delle società non è adeguato, poiché, anche nel caso delle società, sono sempre le persone fisiche a rispondere delle azioni.

Sul punto, assume particolare interesse la posizione di Gabriel Hallevy[87], che rappresenta una delle teorie più innovative e discusse sul tema della responsabilità penale delle intelligenze artificiali. Hallevy, nel suo lavoro[88], propone tre modelli di responsabilità che potrebbero essere applicati ai sistemi di IA:

Nel primo modello, chiamato *Perpetration through another*, un essere umano (programmatore o utente) utilizza l'intelligenza artificiale come strumento per commettere un reato. Questo schema si rifà a concetti già presenti nel diritto penale, dove una persona commette un crimine attraverso un'altra o attraverso un oggetto, in questo caso attraverso l'IA.

Il secondo modello, *Natural probable consequence*, presuppone che il programmatore o l'utente non abbia pianificato direttamente la commissione di un reato, ma che l'IA lo commetta comunque in modo autonomo. Anche se i soggetti umani non sono direttamente coinvolti nella commissione del crimine, possono essere considerati complici, poiché il reato è una conseguenza probabile e naturale dell'uso del sistema.

Infine, l'ultimo modello è quello in cui l'IA è ritenuta responsabile direttamente per il reato, senza che ci sia una connessione diretta con il programmatore o l'utente.

---

[87] Gabriel Hallevy (nato nel 1973) è un professore di diritto penale israeliano. È conosciuto principalmente per i suoi scritti sul rapporto dell'intelligenza artificiale con la responsabilità penale.

[88] G. HALLEVY, *The Basic Models of Criminal Liability of AI Systems and Outer Circles*, presentato presso *FOI, the Swedish Defense Research Agency*, Stoccolma, 11 giugno 2019.

Questo modello implicherebbe il riconoscimento della personalità giuridica penale dell'IA.

Hallevy suggerisce che una combinazione di questi tre modelli potrebbe rivelarsi utile, creando una situazione in cui sia l'IA che gli esseri umani coinvolti direttamente o indirettamente siano soggetti alla responsabilità penale. Questo approccio, secondo Hallevy, avrebbe il vantaggio di garantire che tutti gli attori, umani o artificiali, siano subordinati al diritto penale, rafforzando così la protezione dei beni giuridici tutelati[89].

Tuttavia, la discussione sull'attribuzione di una forma di personalità giuridica all'IA pone sfide significative. Implica un'analisi approfondita delle situazioni concrete, degli interessi sociali da proteggere, e delle potenziali implicazioni per i diritti e le libertà degli individui, nonché per i beni tutelati dal sistema penale.

Invero, alla base della personalità giuridica (anche nel caso degli enti) vi sono sempre le persone che la compongono, a cui sono riconducibili gli interessi e le prospettive dell'entità stessa.

Un sistema di IA, anche se dovesse essere in parte personificato attraverso l'attribuzione di responsabilità per eventuali danni che contribuisce a causare, rimarrebbe comunque un bene. L'attribuzione di personalità giuridica o autonomia patrimoniale non implicherebbe necessariamente l'acquisizione dello *status* o della dignità di persona.

È possibile infatti che un'entità possa avere una certa indipendenza legale o finanziaria senza per questo essere equiparata ad un essere umano e, di conseguenza, essere titolare dei relativi diritti e obblighi[90]. Forse solo quando l'intelligenza e la

---

[89] A pagina 16 del contributo di Hallevy (citato nella nota precedente) si legge «*Coordination of all three liability models creates an opaque net of criminal liability. The combined and coordinated application of these three models reveals a new legal situation in the specific context of AI systems and criminal law. As a result, when AI systems and human entities are involved, directly or indirectly, in a perpetration of a specific offense, it would be much more difficult to evade criminal liability. The social benefit of such a legal policy is of a very high value. All entities, human, legal or AI, are subordinated to the criminal law. If the clearest purpose of the imposition of criminal liability is the application of the legal social control in the specific society, then the coordinated application of all three models is necessary in the very context of AI systems involvement within the commission of offenses*».

[90] Sul punto si veda l'opinion di U. RUFFOLO, *Intelligenza Artificiale, "machine learning" e responsabilità da algoritmo,* cit., p. 1702. L'autore afferma che «Non è necessario, per responsabilizzarla, che la macchina quale "corpo" abbia un "cervello" che "senta" come quello umano. Non è, in altri termini, indispensabile la transizione da bene a persona (non lo era neppure per lo schiavo quando dotato di

coscienza artificiali raggiungeranno un livello tale da poter essere considerate una persona a tutti gli effetti, sarà necessario superare i pregiudizi e i modelli strettamente antropocentrici. Sarà, allora, importante ridefinire cosa significhi essere una persona, ampliandone il concetto fino al punto di includere nuove forme di esistenza, anche non biologiche.

Allo stato attuale, tuttavia, risulta difficile individuare una giustificazione politico-criminale per l'imposizione di una sanzione punitiva su una macchina, per quanto sofisticata possa essere. Se essa venisse considerata pericolosa, l'autorità pubblica dovrebbe, seguendo la normativa nazionale sulla tutela del consumatore, richiederne la modifica, il ritiro dal mercato o, nei casi più gravi, la disattivazione o distruzione. Questo approccio, considerando le macchine come semplici «prodotti» e non come agenti punibili, semplifica l'applicazione di tali misure, anche dal punto di vista procedurale.

Escludendo la possibilità di attribuire responsabilità penale alle macchine intelligenti, si creerebbero, tuttavia, delle situazioni in cui nessun soggetto, umano o artificiale, sarebbe penalmente responsabile per un determinato evento. Questo scenario potrebbe generare una preoccupazione sociale legata a potenziali lacune nella protezione di interessi fondamentali, e potrebbe persino mettere in discussione il futuro delle auto a guida autonoma. Infatti, l'impossibilità di attribuire la responsabilità per determinate categorie di eventi dannosi potrebbe essere percepita come un rischio inaccettabile. In tale contesto, l'unica misura precauzionale efficace sarebbe imporre un divieto totale di svolgere tali attività[91].

Alcune riflessioni renderebbero, tuttavia, infondata una tale preoccupazione. Essa, infatti, deriva da una concezione del diritto penale come unico strumento di

un qualche "*peculio*"). Si può essere "responsabili", e titolari di risorse patrimoniali, anche senza avere personalità giuridica, e comunque senza dover necessariamente ricevere la equiparazione allo *status* della persona umana. E si può essere responsabili anche quando si sia enti ai quali sia irriferibile il concetto di "colpa", essendo questa (non solo sempre più oggettiva, ma) ormai ridotta ad uno tra i tanti criteri di attribuzione della responsabilità; e non l'unico, e neppure il preminente».

[91] A. CAPELLINI, *Profili penalistici delle self-driving cars*, in *Dir. pen. cont.*, 2/2019, p. 340.

protezione, in cui l'assenza di responsabilità per qualsiasi evento dannoso viene percepita come un possibile vuoto di tutela[92].

In queste circostanze, potrebbe risultare dubbio che il rimprovero penale abbia un valore preventivo generale, poiché è possibile che né i produttori né i conducenti di smart car siano in grado di modificare i propri comportamenti in risposta alla minaccia di una sanzione. Analogamente, l'efficacia preventiva specifica potrebbe essere messa in discussione, dato che gli agenti umani coinvolti potrebbero non aver manifestato un comportamento colpevole tale da richiedere rieducazione o una correzione delle loro future scelte di azione.

Sarebbe opportuno considerare la possibilità che, anziché ricorrere a una risposta sanzionatoria penale, che potrebbe rivelarsi inefficace, possano risultare più adeguati a garantire la tutela delle vittime di eventi lesivi «senza responsabili» gli strumenti risarcitori attualmente in fase di sviluppo a livello europeo. Secondo la proposta della Commissione, questi strumenti prevederebbero un robusto sistema di assicurazione obbligatoria e una presunzione di causalità tra il difetto del robot e il danno, riducendo così significativamente l'onere probatorio per la parte lesa. L'introduzione di un sistema risarcitorio adeguato per i danni «incolpevoli» causati dall'intelligenza artificiale potrebbe, quindi, ridurre l'interesse per una reazione punitiva da parte dello Stato in tali casi.

Non è affatto improbabile che una normativa transitoria futura, riguardante i primi periodi di introduzione nel mercato dei veicoli autonomi, continui a richiedere la presenza di un operatore umano esperto e vigile a bordo del mezzo intelligente.

Questa misura potrebbe risultare valida e appropriata se ben progettata e implementata. In tale contesto, una definizione chiara delle responsabilità relative alla supervisione umana del veicolo autonomo, insieme a una limitazione della responsabilità a specifiche forme di colpa, potrebbe evitare che l'operatore diventi un capro

[92] Per un approfondimento sul diritto penale come *ultima ratio* si veda A. CADOPPI, *Il "reato penale". Teorie e strategie di riduzione della criminalizzazione*, Edizioni Scientifiche Italiane, Napoli, p. 39 ss.; M. DONINI, *Il diritto penale come etica pubblica. Considerazioni del politico quale "tipo d'autore"*, Mucchi Editore, Modena, 2014; M. MANTOVANI, *Contributo ad uno studio sul disvalore di azione nel sistema penale vigente*, Bologna University Press, 2014.

espiatorio per le decisioni dannose dell'intelligenza artificiale che non possono essere attribuite ad altri soggetti. I sistemi di bordo potrebbero, infatti, accertare se l'operatore stesse monitorando adeguatamente il funzionamento del veicolo al momento dell'incidente, e, in tal caso, escludere eventuali violazioni delle norme di cautela che potrebbero comportare una responsabilità penale.

Conclusioni

Durante i mesi della pandemia, l'adozione estesa di strumenti digitali, anche all'interno delle istituzioni pubbliche, ha messo in luce in modo definitivo i benefici che possono derivare da un utilizzo consapevole della tecnologia. Questo periodo ha permesso a milioni di persone di acquisire familiarità con nuovi strumenti, rendendoli di uso comune su vasta scala e aprendo prospettive che sarebbe imprudente abbandonare per il benessere della collettività. L'integrazione di nuove modalità operative, processi ed esperienze appare, pertanto, ormai non solo opportuna, ma necessaria.

La precedente analisi ha evidenziato che dall'utilizzo della tecnologia possono derivare rischi significativi, tra i quali preme sottolineare la possibilità di ingiustificate violazioni di diritti e libertà individuali.

Passi avanti nella regolamentazione del settore sono stati fatti grazie all'*AI Act*, che ha introdotto un approccio basato sul rischio, evitando eccessi regolatori che possano soffocare l'innovazione. Tuttavia, è emerso che l'IA presenta spesso livelli di imprevedibilità e opacità tali da rendere difficile una valutazione *ex ante* delle conseguenze delle sue azioni.

In parallelo, il GDPR ha offerto un primo tentativo di affrontare la questione del processo decisionale automatizzato, garantendo un certo grado di supervisione umana sulle decisioni che riguardano dati personali. Ma la realtà operativa dimostra che il mero controllo umano spesso si traduce in una supervisione formale e inefficace, specie nei contesti ad alto contenuto tecnologico.

Invero, molti dei sistemi utilizzati nei contesti giudiziari si basano su reti neurali e altri modelli di *machine learning*, che sono progettati per apprendere in modo autonomo dai dati a loro disposizione. Tuttavia, è stato evidenziato che il funzionamento interno di questi sistemi è spesso oscuro, e questa mancanza di trasparenza rende estremamente difficile valutare la validità delle decisioni prese dall'algoritmo.

È emersa, inoltre, la necessità di regolamentare e moderare i contenuti diffusi su tali piattaforme, ma le modalità con cui le società che gestiscono i *social media* hanno affrontato la questione sono spesso risultate poco trasparenti e incoerenti. Questo scenario ha messo in evidenza un problema ancora più grande: la concentrazione di un potere sostanzialmente censorio nelle mani di pochi operatori privati di enormi dimensioni, gli *Internet Service Provider*, potere che risulta estremamente difficile da sottoporre al controllo pubblico.

Resta, pertanto, aperto un tema controverso e di non facile soluzione: riuscire a coniugare l'evoluzione tecnologica con la protezione dei diritti fondamentali, quali il diritto alla non discriminazione, la riservatezza, e la dignità personale.

Un aspetto particolarmente problematico è quello del *bias* algoritmico, discusso nel Capitolo 2, in quanto le discriminazioni derivanti da scelte dei sistemi di IA influiscono negativamente sui diritti fondamentali degli individui, come la libertà personale e l'uguaglianza. Gli algoritmi possono perpetuare e ampliare pregiudizi preesistenti, causando così gravi conseguenze giuridiche e sociali. La sfida normativa è quella di assicurare che tali sistemi rispettino i principi di non discriminazione e che siano progettati in modo trasparente, affinché possano essere soggetti a verifiche esterne indipendenti.

Una delle principali soluzioni proposte per mitigare il rischio di discriminazione algoritmica è quella di assicurare che il processo decisionale automatizzato sia sempre soggetto a una supervisione umana. Questo principio, noto come *human-in-the-loop*, prevede che, anche nei casi in cui un algoritmo sia utilizzato per supportare un processo decisionale, la scelta finale debba sempre essere presa da un essere umano. Il *General Data Protection Regulation* (GDPR), ad esempio, stabilisce un diritto per gli individui a non essere sottoposti a decisioni interamente automatizzate, che abbiano un impatto significativo sulla loro vita. Questo diritto, tuttavia, è soggetto a importanti eccezioni, come il consenso dell'interessato o la necessità dell'automazione per l'esecuzione di un contratto.

La questione del controllo umano è di fondamentale importanza nel contesto del diritto penale. In molti casi, la decisione di infliggere una pena, di concedere una

misura alternativa alla detenzione o di determinare il rischio di recidiva di un detenuto può avere conseguenze molto gravi per l'individuo coinvolto. In tali contesti, è essenziale che il giudice o l'autorità competente mantengano il controllo sul processo decisionale, valutando criticamente i risultati prodotti dall'algoritmo. Tuttavia, questa soluzione non è esente da contestazioni. In molti casi, infatti, i giudici e gli operatori del sistema penale non hanno le competenze tecniche necessarie per comprendere a fondo il funzionamento degli algoritmi che utilizzano. Questo può portare a un affidamento eccessivo sulla tecnologia, che, come già visto, può non essere sempre imparziale.

Per affrontare questo problema, si è ipotizzata anche l'adozione di modelli di IA c.d. *Explainable* (*XAI*)[1], che consentano agli operatori umani di comprendere meglio il processo decisionale dell'algoritmo. Soprattutto nel contesto della giustizia penale, l'impiego di tecnologie intelligenti solleva preoccupazioni specifiche. Sebbene gli algoritmi possano contribuire a migliorare l'efficienza dei procedimenti, il rischio che le decisioni adottate da macchine non siano sempre spiegabili o trasparenti rappresenta una violazione del diritto alla difesa. Di conseguenza, in futuro, il diritto alla spiegazione degli algoritmi potrebbe diventare fondamentale per coloro che sono soggetti a decisioni automatizzate. Questo diritto garantirà che gli individui possano comprendere e contestare le decisioni prese dai sistemi intelligenti, prevenendo così l'adozione di misure potenzialmente ingiuste o arbitrarie.

Tuttavia, anche questo approccio ha i suoi limiti. La spiegabilità di un algoritmo richiede compromessi tecnici che potrebbero ridurne l'efficacia e la precisione. Inoltre, un modello di IA più comprensibile per l'essere umano potrebbe non essere

[1] I sistemi di *AI Explainable* (*XAI*, o Intelligenza Artificiale Esplicabile) sono una classe di tecnologie di intelligenza artificiale progettate per rendere comprensibile agli esseri umani il funzionamento interno dei modelli di IA. L'obiettivo della *XAI* è fornire spiegazioni dettagliate e trasparenti su come e perché l'algoritmo è giunto a una determinata decisione o risultato, riducendo così l'opacità tipica di molte tecniche di IA. Il concetto di *XAI* è emerso in modo più chiaro a partire dalla metà degli anni 2010, quando l'integrazione di sistemi di IA in settori cruciali come la sanità, la giustizia e la finanza ha evidenziato la necessità di giustificare e spiegare le decisioni prese da tali sistemi. Uno dei progetti pionieristici è stato lanciato dall'agenzia *DARPA* (*Defense Advanced Research Projects Agency*) degli Stati Uniti nel 2016, consultabile sul sito *web* www.darpa.mil/program/explainable-artificial-intelligence.

altrettanto efficiente nel trattare grandi quantità di dati complessi, riducendo così i benefici che la tecnologia può garantire in termini di velocità ed efficienza.

La necessità di un controllo pone anche un altro problema: fino a che punto l'intervento dell'uomo è realmente efficace nel prevenire decisioni discriminatorie? Come abbiamo visto nel corso del lavoro, quando gli esseri umani sono affiancati da sistemi automatizzati tendono a fidarsi eccessivamente della macchina, riducendo la propria attenzione e capacità critica. Questo fenomeno, noto come *automation bias*, può portare a una diminuzione delle competenze umane necessarie per valutare correttamente le decisioni prodotte dall'algoritmo, aumentando il rischio che le discriminazioni passino inosservate.

Nella prima parte del lavoro, dunque, si è cercato di comprendere se sia possibile evitare che i sistemi di intelligenza artificiale cagionino danni e commettano violazioni dei diritti individuali. Nel caso le misure approntate a tal fine si rivelino fallaci e inefficaci, è necessario valutare quali siano le conseguenze, anche in termini di responsabilità penale.

È stato evidenziato che il sistema penalistico è costruito su presupposti che mal si adattano alle innovazioni introdotte dalle tecnologie intelligenti. La responsabilità penale, fondata sul concetto di dolo o colpa, richiede un soggetto capace di volontà e discernimento, caratteristiche che allo stato attuale mancano nei sistemi di IA, anche quelli più avanzati. Tuttavia, la crescente autonomia delle macchine solleva il problema del cosiddetto *responsibility gap*, ossia un vuoto di responsabilità penale che rischia di emergere nei casi in cui si riveli difficile attribuire con certezza una determinata condotta illecita.

Taluni hanno ipotizzato una revisione del concetto stesso di colpa, che prenda in considerazione non solo il comportamento umano, ma anche la condotta della macchina stessa. Come si è visto, ad esempio, i veicoli autonomi introducono un grado di autonomia tale da porre seri dubbi circa la possibilità di imputare ad altri la responsabilità penale in caso di incidenti. Con l'aumentare dei livelli di automazione diventa sempre più difficile sostenere che i proprietari o i produttori del veicolo

abbiano un controllo effettivo sul suo comportamento, e secondo alcuni si potrà addirittura ritenere colpevole il *software* stesso, qualificandolo come soggetto di diritto.

Tuttavia, questo passaggio non è privo di rischi: l'attribuzione di una personalità giuridica ai sistemi di IA potrebbe sollevare problematiche etiche e giuridiche di difficile risoluzione, nonché incentivare atteggiamenti di deresponsabilizzazione da parte di chi progetta e utilizza queste tecnologie. Inoltre, l'autonomia dei sistemi in esame, almeno allo stato attuale, non può essere paragonata a quella dell'uomo, che rappresenta un elemento centrale nel concetto di colpevolezza nel diritto penale.

La coscienza umana, invero, consente agli individui di distinguere tra ciò che è giusto e ciò che è sbagliato, e di agire di conseguenza. Questa capacità di valutazione morale è alla base della responsabilità penale, in quanto permette di attribuire una colpa all'individuo che ha violato la legge. Al contrario, un sistema di IA, per quanto sofisticato, non riesce a distinguere tra bene e male. Le decisioni prese dall'algoritmo non sono il frutto di una valutazione etica, ma di un calcolo statistico basato su dati precedenti. Di conseguenza, non è possibile attribuire una responsabilità morale a un sistema di IA.

Attualmente la soluzione più realistica e realizzabile è quella di considerare l'intelligenza artificiale come un semplice strumento nelle mani dell'operatore umano, che rimane responsabile delle decisioni prese con l'ausilio della tecnologia[2]. Tuttavia, questa impostazione non tiene conto dell'autonomia decisionale dei sistemi di IA più avanzati, che possono adottare scelte basate su parametri e dati che l'operatore umano non è in grado di controllare o comprendere pienamente.

Un altro approccio potrebbe essere quello di estendere la responsabilità ai produttori di *software*, imponendo loro obblighi più stringenti in materia di sicurezza e trasparenza degli algoritmi. In questo contesto, la responsabilità per prodotto difettoso[3] potrebbe rappresentare un punto di partenza utile, ma sarà necessario adattare

[2] Affronta tale tematica C. PIERGALLINI, *Danno da prodotto e responsabilità penale. Profili dommatici e politico-criminali*, cit.; *Intelligenza artificiale: da "mezzo" ad "autore" del reato?*, cit., p. 1746 ss.

[3] Sul punto si può far riferimento alle già citate considerazioni di A.L. BITETTO, *In tema di responsabilità per danno da prodotto difettoso*, cit., p. 441 ss.

le norme attuali alle peculiarità dei veicoli autonomi, prendendo in considerazione non solo i difetti di fabbricazione, ma anche eventuali falle nei sistemi di apprendimento automatico e nelle decisioni algoritmiche. Tuttavia, questa soluzione solleva problemi di equità: fino a che punto è giusto ritenere il produttore di un algoritmo responsabile di ogni possibile errore commesso dal sistema, soprattutto quando la tecnologia viene utilizzata in contesti non previsti o, comunque, non facilmente ipotizzabili?

Il quadro normativo attuale, come dimostrato dall'analisi della disciplina europea e delle esperienze legislative di altri Paesi, non è ancora adeguato a rispondere alle sfide poste dai veicoli autonomi di livello 4 e 5, come descritti nel terzo capitolo del presente lavoro. Il futuro della regolamentazione in questo settore dipenderà dalla capacità dei legislatori di definire chiaramente le posizioni di garanzia e di individuare misure di prevenzione efficaci.

Le riflessioni condotte nel corso della tesi convergono verso una conclusione comune: l'intelligenza artificiale, nei suoi vari ambiti di applicazione, non può essere trattata esclusivamente come un problema tecnico-giuridico. Essa pone infatti questioni di ordine etico, sociale e filosofico che richiedono una regolamentazione multidisciplinare, capace di coniugare tutela dei diritti fondamentali, promozione dell'innovazione e gestione dei rischi.

La strada verso una regolamentazione efficace dell'intelligenza artificiale è ancora lunga e complessa, ma a parere di chi scrive alcuni elementi emergono con chiarezza. In primo luogo, è fondamentale che i legislatori adottino un approccio flessibile, capace di adattarsi rapidamente ai cambiamenti tecnologici. In secondo luogo, è essenziale che la regolamentazione non si limiti a intervenire a valle del processo decisionale, ma che miri a prevenire le conseguenze negative attraverso un controllo rigoroso dei dati, degli algoritmi e dei sistemi di IA in fase di sviluppo.

Dal lavoro svolto emerge che l'intelligenza artificiale rappresenta una sfida senza precedenti per il diritto penale, ma anche un'opportunità per ripensare alcuni dei concetti fondamentali della responsabilità e della giustizia. Con una regolamentazione

adeguata e una riflessione interdisciplinare sarà possibile coniugare innovazione e tutela dei diritti fondamentali.

L'evoluzione normativa sarà decisiva per affrontare le sfide sollevate dall'IA. È chiaro che il diritto dovrà continuare a evolversi per rispondere adeguatamente ai rischi che l'uso di sistemi di IA comporta, soprattutto in settori delicati come la sanità, la giustizia e la mobilità. Una delle principali questioni da affrontare è quella del principio di precauzione, il quale richiede che si adottino misure di tutela quando vi è incertezza sui rischi posti da nuove tecnologie. Questo principio, già fondamentale in ambito ambientale e sanitario, potrebbe rappresentare una guida efficace anche nell'applicazione dell'IA.

Il nodo centrale di questo dibattito sarà probabilmente il concetto di rischio consentito[4] e lo spazio che si deciderà di riservargli. Quando i sistemi intelligenti diverranno così diffusi da essere universalmente riconosciuti come portatori di vantaggi significativi per la società, sarà più semplice strutturare normative cautelari adeguate e affrontare il problema dell'imputazione della responsabilità per i danni causati dall'IA.

Questo percorso potrebbe seguire l'esempio di quanto avvenuto in passato con la diffusione dei veicoli a motore, considerati di indubbia utilità sociale, unita ad un'alta attitudine a provocare danni, i cui costi sociali gravano su chi trae beneficio dall'utilizzo di un bene intrinsecamente pericoloso.

Il futuro regolamentare dovrà orientarsi verso la minimizzazione del rischio, attribuendo la responsabilità a chi beneficia dell'uso dell'IA, secondo il principio *cuius commoda, eius et incommoda*. Ciò significa che, se il comportamento deviante dell'IA è prevedibile ed evitabile, il produttore dovrà essere ritenuto responsabile. Al contrario, se il danno è inevitabile e il sistema ha agito in modo imprevisto, il soggetto danneggiato dovrà accollarsi il costo dell'evento lesivo.

[4] Tra i vari autori che trattano l'argomento, quelli che si ritiene di citare un'ultima volta sono C. BRUSCO, *Rischio e pericolo, rischio consentito e principio di precauzione*, cit., p. 384 ss.; E. PENCO, *Limiti-soglia e responsabilità colposa. Il ruolo incerto delle soglie quantitative, dalla colpa specifica al rischio consentito*, cit., p. 195 ss.

Non è ancora il tempo di trarre conclusioni definitive sulla soggettività giuridica delle IA e sulla loro responsabilità. È piuttosto il momento di continuare a porre domande, formulare ipotesi e comprendere come il diritto penale possa affrontare e contribuire allo sviluppo di questi delicati e complessi temi.

Bibliografia

A. S. AGRÒ, *L'eguaglianza in transizione, in Il principio di ragionevolezza nella giurisprudenza della Corte costituzionale – Riferimenti comparatistici*, Giuffrè, Milano, 1994, p. 199 ss.

A. ALAIMO, *Il Regolamento sull'Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico*?, in *federalismi.it*, 25/2023, p. 133 ss.

M. ALESCI, *Rilievi sul delitto di diffamazione e sul valore scriminante della critica*, in *Cass. pen.*, 10/2019, p. 3523 ss.

L. ALESIANI, *I reati di opinione: una rilettura in chiave costituzionale*, Giuffrè, Milano, 2006.

L. ALGERI, *Intelligenza artificiale e polizia predittiva,* in *Dir. pen. e proc.,* 6/2021.

M. R. ALLEGRI, *Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, in *Inf. dir.*, 2/2021, p. 7 ss.

E. AL MUREDEN, *Sicurezza "ragionevole" degli autoveicoli e responsabilità del produttore nell'ordinamento giuridico italiano e negli Stati Uniti*, in *Contr. impr.*, 6/2012, p. 1505 ss.

G. ALPA, *Alle origini dei diritti della personalità*, in *Riv. trim. dir. proc. civ.*, 3/2021, p. 671 ss.

G. AMATO, *Un impianto diretto a considerare solo la colpa specifica*, in *Guida dir.*, 16/2016, p. 55 ss.

A. AMBROSI, *Libertà di pensiero e manifestazione di opinioni razziste e xenofobe*, in *Quad. cost.*, 3/2008, p. 519 ss.

F. AMIGONI, V. SCHIAFFONATI, M. SOMALVICO, voce *Intelligenza Artificiale*, in *Enc. Treccani*, 2008.

E. AMODIO, *Il processo come gioco tra letteratura e diritto vivente*, in *Riv. it. dir. e proc. pen.*, 4/2020, p. 1663 ss.

L. ANCIS, *Navi pilotate da remoto e profili di sicurezza della navigazione nel trasporto di passeggeri*, in *Dir. trasp.*, 2019, p. 428 ss.

E. ANDOLINA, *La sentenza della Corte di giustizia UE nel caso "H.K. c. Prokuratuur": un punto di non ritorno nella lunga "querelle" in materia di "data retention"?*, in *Proc. pen. e giust.*, 5/2021, p. 1204 ss.

G. ANDREAZZA, *Cronaca giornalistica e trattamento dei dati personali: le condizioni di esonero dal consenso dell'interessato*, in *Cass. pen.*, 12/2009, p. 4864 ss.

P. ANNICCHINO, *(In)sicurezza dei dati, contromisure e attività di contrasto alla criminalità informatica*, in *Dir. pen. e proc.*, 9/2022, p. 1155 ss.

V. ANGIOLINI, *Manifestazione del pensiero e "libertà altrui"*, in *Giur. cost.*, 6/1995, p. 4585 ss.

F. ANGIONI, *Il pericolo concreto come elemento della fattispecie penale*, Giuffrè, Milano, 1994.

I. ANRÒ, *"Online hate speech": la prospettiva dell'Unione europea tra regolamentazione della condotta dei prestatori di servizi intermediari e ricorso al diritto penale*, in *Osservatorio sulle fonti*, 1/2023, p. 13 ss.

F. ANTOLISEI, *Manuale di diritto penale. Parte generale*, Giuffrè, Milano, 2000.

E. ANTONINI, *Il trattamento illecito di dati personali nel codice della privacy: i nuovi confini della tutela penale*, in *Dir. pen. e proc.*, 3/2005, p. 340 ss.

S. ARDIZZONE, voce *Naufragio, disastro aviatorio, disastro ferroviario*, in *Dig. disc. pen.*, VIII, Utet Giuridica, Torino 1994, p. 224 ss.

S. ARDUINI, *La "scatola nera" della decisione giudiziaria: tra giudizio umano e giudizio algoritmico*, in *BioLaw Journal*, 2/2021, p. 453 ss.

K.D. ASGLEY, *Artificiale Intelligence and Legal Analytics, New Tools for Law Practice in the Digital Age*, Cambridge University Press, Cambridge, 2017.

C. ASPRELLA, *L'"Oversight Board", la "Corte d'appello" di Facebook, e i nuovi "confini" della giurisdizione*, in *Judicium*, 3/2023, p. 241 ss.

A. ASQUINI, *La responsabilità del vettore per infortunio del viaggiatore*, in *Riv. dir. comm.*, 1919, II, p. 350 ss.

S. ATERNO, A. CISTERNA, *Il legislatore interviene ancora sul Data retention, ma non è finita - Decreto legislativo 30 maggio 2008, 109*, in *Dir. pen. e proc.*, 3/2009, p. 282 ss.

V. ATTILI, *L'agente-modello "nell'era della complessità": tramonto, eclissi o trasfigurazione?*, in *Riv. it. dir. e proc. pen.*, 2006, p. 1289 ss.

L. AULINO, *Consenso al trattamento dei dati e carenza di consapevolezza: il "legal design" come un rimedio "ex ante"*, in *Dir. inform.*, 2/2020, p. 303 ss.

G. AVANZINI, *Decisioni amministrative e algoritmi informativi, predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Editoriale Scientifica, Napoli, 2019.

- *Intelligenza artificiale, machine learning e istruttoria procedimentale: vantaggi limiti ed esigenze di una corretta Data governance*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Volume 2, Quaderni ASTRID, Bologna, 2022, p. 80.

G. M. BACCARI, C. CONTI, *La corsa tecnologica tra Costituzione, codice di rito e norme sulla "privacy": uno sguardo d'insieme*, in *Dir. pen. e proc.*, 6/2021, p. 711 ss.

G.M. BACCARI, M. MARRAFFINO, *Le prospettive di utilizzo delle "chatbot" nel procedimento penale*, in *Dir. pen. e proc.*, 8/2021, p. 1008 ss.

B. BALDINI, *Città intelligenti, decisioni "biased" e rischi di esclusione*, in *federalismi.it*, 10/2024.

F. BALLAGUER CALLEJON, *"Social network", società tecnologiche e democrazia*, in *Nomos*, 3/2019, p. 4 ss.

M. BARBERA, *Discriminazioni algoritmiche e forme di discriminazione*, in *Labour & Law Issues*, 1/2021.

P. BARILE, *Libertà di manifestazione del pensiero*, Giuffrè, Milano, 1975.

B. BARRAUD, *Éthique de l'intelligence artificielle*, in *Le droit d'aujourd'hui*, L'Harmattan, Parigi, 2022.

R. BARTOLI, *Danno da prodotto e responsabilità penale*, in *Riv. it. dir. e proc. pen*, 4/2004, p. 1163 ss.

- *Brevi considerazioni sulla responsabilità penale dell' "Internet Service Provider"*, in *Dir. pen. e proc*, 5/2013, p. 600 ss.

F. BASILE, *La roboetica. Una nuova scienza?*, in *L'Arco di Giano*, 2008, p. 11 ss.

- *Fisionomia e ruolo dell'agente-modello ai fini dell'accertamento processuale della colpa generica*, in G. A. De Francesco, C. Piemontese, E. Venafro (a cura di), *La prova dei fatti psichici,* Giappichelli, Torino 2010, p. 94 ss.

- *I delitti contro il sentimento religioso: tra incriminazione dell'opinione e tutela della libertà di manifestazione del pensiero*, in *MediaLaws*, 2/2018, p. 12 ss.

- *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione,* in F. Basile, M. Caterini, S. Romano (a cura di), *Il sistema penale ai confini delle hard sciences. Percorsi epistemologici tra neuroscienze e intelligenza artificiale*, Pacini Editore, Pisa, 2021, p. 3 ss.

M. BASSINI, G. E. VIGEVANI, *Primi appunti su "fake news" e dintorni*, in *MediaLaws*, 1/2017.

E. BATTELLI, *Giustizia predittiva, decisione robotica e ruolo del giudice*, in *Giust. civ.*, 2/2020, p. 281 ss.

V. BATTISTELLA, *Spunti di riflessione sulla conduzione dei veicoli altamente automatizzati nella circolazione stradale in una prospettiva de iure condendo*, in *Dir. trasp.*, 2021, p. 953 ss.

O. BAZINA, *Human rights and biometric data protection. Social credit system*, in *European Studies Quarterly*, 2020.

S. BECK, *Google Cars, Software Agents, Autonomous Weapons Systems. New Challenges for Criminal Law*, in E. Hilgendorf E U. Seidel (eds.), *Robotics, Autonomics and the Law (Nomos)*, 2017, pp. 227-251.

E. BELFIORE, *Profili penali dell'attività medico-chirurgica in equipe. Sezione I. Evoluzione storico-dogmatica della responsabilità per colpa*, in *Arch. pen.*, 9/1986, p. 265 ss.

P. BENANTI, *Human in the loop. Decisioni umane e intelligenze artificiali*, Mondadori, Milano, 2022.

F. BENATTI, *Osservazioni in tema di doveri di protezione*, in *Riv. trim. dir. proc. civ.*, 1960, p. 1342 ss.

- *Doveri di protezione*, in *Dig. civ.,* VII, 1990, Utet Giuridica, Torino, p. 221 ss.

V. BERLINGÒ, *Per una rilettura dei servizi di "Vessel Traffic Service" (VTS) e di pilotaggio alla luce delle implicazioni giuridiche del metodo matematico dell'HITL ("Human in the Loop")*, in *Dir. mar.*, 4/2022, p. 694 ss.

A. BERNARDI, *La responsabilità da prodotto nel sistema italiano: profili sanzionatori*, in *Riv. trim. dir. pen. econ.*, 2003.

- *Corpus Juris e formazione di un diritto penale europeo*, in *Riv. it. dir. pubbl. com.*, 2/2001, p. 283 ss.

R. BERTOLESI, *Intelligenza artificiale e responsabilità penale per danno da prodotto*, Università degli Studi di Milano, Tesi dottorale, A.A. 2018/2019.

A. BERTOLINI, *Robots as Products: The Case for a Realistic Analysis of Robotic Application and Liability Rules*, in *Law, Innovation and Technology*, 2013, p. 214.

A. BERTOLINI, E. PALMERINI, *Regulating robotics: A challenge for Europe,* in *EU Parliament, Workshop on Upcoming issues of EU law for the IURI Committee*, in *Publications Office of the EU Parliament, Bruxelles*, 2014, p. 169 ss.

M. BETZU, *Comunicazione, manifestazione del pensiero e tecnologie polifunzionali*, in *Quad. cost.*, 3/2006, p. 511 ss.

A. BEVERE, A. CERRI, *Il diritto di informazione e i diritti della persona*, Giuffrè, Milano, 1995.

M. BIASI, A. LOMBARDI, *Processo del lavoro e giustizia predittiva: prime riflessioni*, in *Riv. it. dir. lav.*, 3/2023, 1, p. 361 ss.

F. BICO, A. SORGATO, *Diffamazione. Aspetti pratici e nuove problematiche*, Giappichelli, Torino, 2007.

C. BISHOP, *Pattern Recognition and Machine Learning,* Springer, Berlino, 2006.

A.L. BITETTO, *In tema di responsabilità per danno da prodotto difettoso*, in *Foro it.*, 10/2009, 4, p. 441 ss.

C. BJOLA, *Diplomacy in the Age of Artificial Intelligence, in Intelligence artificielle, défise et perspectives*, Bruylant, Bruxelles, 2021, p. 61 ss.

R. BLAIOTTA, *Sulla colpa nel caso di attività svolta in equipe*, in *Cass. pen*, 3/2000, p. 584 ss.

N. BOBBIO, *Eguaglianza e libertà*, Einaudi, Torino, 1995.

G.M. BOI, *«Navi-drone»: primi interrogativi in tema di disciplina giuridica*, in *Riv. Dir. Nav.,* 2017, p. 175 ss.

V. S. BONAMINI PEPOLI, *Profili di contrasto al "cybercrime" "in iure condito" e "de iure condendo"*, in *Inf. dir.*, 2/2022, p. 109 ss.

A. M, BONANNO, *Protocolli, linee guida e colpa specifica*, in *Ind. pen.*, 1/2006, p. 441 ss.

A. BONFANTI, *"Big data" e polizia predittiva: riflessioni in tema di protezione del diritto alla "privacy" e dei dati personali*, in *MediaLaws*, 3/2018.

P. BONINI, *L'autoregolamentazione dei principali "Social Network". Una prima ricognizione delle regole sui contenuti politici*, in *federalismi.it*, 11/2020, p. 265 ss.

J. BONNEFON, A. SHARIFF, I. RAHWAN, *The social dilemma of autonomous vehicles*, in *Science*, Vol. 352, 24 giugno 2016, p. 1573 ss.

R. BORSARI, *Intelligenza Artificiale e responsabilità penale: prime considerazioni*, in *MediaLaws*, 3/2019, p. 262 ss.

Y. BOSHMAF, I. MUSLUKHOV, K. BEZNOSOV, M. RIPEANU, *The socialbot network: when bots socialize for fame and money*, in *Proceedings of the 27th annual computer security applications conference*, 2011, p. 93 ss.

R. BOTSMAN, *Who can you trust? How technology brought us together and why it might drive us apart*, New York, 2017.

G. BOTTO, *Giustizia predittiva e sentenza in forma semplificata: alcuni spunti per una (razionale) applicazione dell'intelligenza artificiale nel processo amministrativo*, in *Diritto e processo amministrativo*, 2/2023, p. 493 ss.

S. BRASCHI, *Il ruolo delle reti sociali nel contrasto ai reati commessi all'interno del web. Tendenze evolutive e prospettive di sviluppo*, in *MediaLaws*, 2/2021, p. 100 ss.

- Il nuovo Regolamento sui servizi digitali: quale futuro per la responsabilità degli "Internet Service Provider"?, in *Dir. pen. e proc.*, 3/2023, p. 367 ss.

C. BRUSCO, *Rischio e pericolo, rischio consentito e principio di precauzione, La c.d. "flessibilizzazione delle categorie del reato"*, in *Criminalia*, 2012, p. 391 ss.

L. BRUSCO, *Il dilemma morale del carrello. Una vivace ricostruzione storica*, in *Diritto & questioni pubbliche*, 1/2016, p. 16 ss.

M. E. BUCALO, *La libertà di espressione nell'era dei "social network" fra "content moderation" e necessità di una regolazione flessibile*, in *Dir. pubbl. comp. eur.*, 1/2023, p. 143 ss.

A. BURATTI, *Framing the Facebook Oversight Board: Rough Justice in the Wild Web?*, in *MediaLaws*, 2/2022, p. 31 ss.

H. C. BURMEISTER, W. BRUHN, Ø. J. RØDSETH, T. PORATHE, *Autonomous Unmanned Merchant Vessel and its Contribution towards the e-Navigation Implementation: The MUNIN Perspective*, in *International Journal of e-Navigation and Maritime Economy*, 1/2014.

N. BUSTO, *Carta europea sulla robotica: una proposta di roboethics per le self driving car*, in *Ciberspazio e dir.*, 2017, p. 289 ss.

A. CADOPPI, *Il "reato penale". Teorie e strategie di riduzione della criminalizzazione*, Edizioni Scientifiche Italiane, Napoli, 2022.

G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *MediaLaws*, 2/2018, p. 5 ss.

S. CAGLI, *La rilevanza del consenso nella disciplina del trattamento dei dati personali*, in *Ind. pen.*, 2/2001, p. 855 ss.

G. CALABRESI, E. AL MUREDEN, *Driveless cars, Intelligenza artificiale e futuro della mobilità*, Il Mulino, Bologna, 2021.

R. CALCAGNO, *Nuove disposizioni per il contrasto ai fenomeni di criminalità informatica*, in *Dir. pen. e proc.*, 8/2012, p. 934 ss.

C. R. CALDERONE, *Libertà di manifestazione del pensiero e limiti*, in *Cass. pen.*, 1/1985, p. 54 ss.

L. CALIFANO, *La libertà di manifestazione del pensiero... in rete; nuove frontiere di esercizio di un diritto antico. "Fake news", "hate speech" e profili di responsabilità dei "social network"*, in *federalismi.it*, 26/2021.

- *Chat GPT e Meta ["Meta Platforms Ireland Limited" - MPIL] EDI ["Election day information"]: spunti problematici su profili regolatori e ruolo delle autorità di controllo di protezione dati*, in *federalismi.it*, 10/2023, pp. 4-15.

R. CALVANO, *L'istruzione, il Covid-19 e le diseguaglianze*, in *Costituzionalismo.it*, 3/2020, 3, p. 57 ss.

M. CAMERON, *Realising the potential of Driverless Vehicles*, Createspace independent publishing, Wellington, 2018.

A. CANEPA, *L'imputazione soggettiva della colpa. Il reato colposo come punto cruciale nel rapporto tra illecito e colpevolezza*, Torino, Giappichelli, 2011.

G. CANZIO, *Il dubbio e la legge*, in *Dir. pen. cont.*, 20 luglio 2018.

M. CAPPELLI, voce *Macchina di Turing*, in *Enc. della Scienza e della Tecnica*, 2008.

A. CAPPELLINI, *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale*, in *Criminalia*, 2018, p. 499 ss.

- *Profili penalistici delle self-driving cars*, in *Dir. pen. cont.*, 2/2019, p. 340 ss.

- *Reati colposi e tecnologie dell'Intelligenza artificiale*, in G. Balbi, A. Esposito, S. Manacorda, F. De Simone (a cura di), *Diritto penale e intelligenza artificiale. Nuovi Scenari*, Giappichelli, Torino, 2023, pp. 19-32.

R. CAPPITELLI, *La sostituzione di persona nel diritto penale italiano*, in *Cass. pen.*, 10/2005, p. 2994 ss.

F. CAPRIOLI, *L'accertamento della responsabilità penale "oltre ogni ragionevole dubbio"*, in *Riv. it. dir. e proc. pen.*, 1/2009, p. 51 ss.

A. CAPROTTI, *L'effettività del principio di non discriminazione sul luogo di lavoro: un discorso in continua evoluzione*, in *DPCE online*, 4/2018, p. 1159 ss.

G. CARAPEZZA FIGLIA, *Decisioni algoritmiche tra diritto alla spiegazione e divieto di discriminare*, in *Persona e Mercato*, 4/2023, p. 638 ss.

A. M. CARELLA, *Responsabilità per colpa professionale di "equipe" medico-chirurgica*, in *Riv. it. med. leg.*, 4/2019, p. 1560 ss.

G. CARLIZZI, *I due principi costituzionali del giudizio probatorio penale. Repliche a G. Tuzet, "Libero convincimento e ragionevole dubbio secondo Gaetano Carlizzi"*, in *Diritto & questioni pubbliche*, 2/2019, p. 14 ss.

- *La regola del ragionevole dubbio nel processo penale, con particolare riguardo al giudizio di cassazione*, in *Foro it.*, 3/2021, 2, p. 209 ss.

E. CARLONI, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm.*, 2/2020, p. 273 ss.

M. CARRETTA, *La nave*, in A. Antonini (a cura di), *Trattato breve di diritto marittimo*, I, Giuffrè, Milano, 2007, p. 299 ss.

D. CARUSI, *Principio di eguaglianza, diritto singolare e privilegio*, Edizioni Scientifiche Italiane, Napoli, 1998.

T. CASADEI, *La libertà d'espressione e i suoi dilemmi*, in *Notizie di Politeia*, 138/2020, p. 90 ss.

T. CASADEI, G. ZANETTI, *Tra dilemmi etici e potenzialità concrete: le sfide dell'autonomous driving*, in S. Scagliarini (a cura di), *Smart roads e driverless cars: tra diritto, tecnologie, etica pubblica*, Giappichelli, Torino, 2019, p. 41 ss.

G. CASCONE, *La Corte di Giustizia dell'Unione europea definisce le condizioni per la legittimità delle normative nazionali in materia di acquisizione dei tabulati. Le ripercussioni sull'ordinamento italiano della sentenza del 2 marzo 2021 (C-746/18) nel caso H.P.*, in *Cass. pen.*, 2/2022, p. 419 ss.

C. CASONATO, *Unlocking the Synergy: Artificial Intelligence and (old and new) Human Rights*, in *BioLaw Journal*, 3/2023, p. 233 ss.

G. CASSANO, B. TASSONE, *Responsabilità dell'Internet "service provider", diritti di proprietà intellettuale e danni punitivi*, in *Foro it.*, 9/2022, 1, p. 2840 ss.

L. CASTELLETTI, G. RIVELLINI, E. STRATICÒ, *Efficacia predittiva degli strumenti di Violence Risk Assessment e possibili ambiti applicativi nella psichiatria forense e generale italiana*, in *Journal of Psychopathology*, 2014, p. 153 ss.

C. CASTELLI, D. PIANA, *Giustizia predittiva. La qualità della giustizia in due tempi,* in *Quest. giust.*, 4/2018.

C. CASTETS-RENARD, J. EYNARD, *Un droit de l'intelligence artificielle, Entre règles sectorielles et régime général, perspectives compares*, Bruylant, Bruxelles, 2023.

C. CASTRONOVO, *Obblighi di protezione e tutela del terzo*, in *Jus*, 1976, p. 123 ss.

D. CASTRONUOVO, *Responsabilità da prodotto e struttura del fatto colposo*, in *Riv. it. dir. e proc. pen.*, 2005, p. 301 ss.

- *La colpa penale*, Giuffrè, Milano, 2009.

- *L'evoluzione teorica della colpa penale tra dottrina e giurisprudenza*, in *Riv. it. dir. e proc. pen.*, 2011, p. 1597 ss.

- *Principio di precauzione e diritto penale: paradigmi dell'incertezza nella struttura del reato*, Aracne, Roma, 2012.

M. CATERINI, *Il giudice penale "robot"*, in *Leg. pen.*, 12/2020.

A. CAVALIERE, *La discussione intorno alla punibilità del negazionismo, i principi di offensività e libera manifestazione del pensiero e la funzione della pena*, in *Riv. it. dir. e proc. pen.*, 2/2016, p. 999 ss.

V. CAVANNA, *Nuovi poteri, vecchi problemi. Il costituzionalismo alla prova del digitale*, in *Dir. pubbl. comp. eur.*, 1/2023, p. 223 ss.

F. CENTONZE, *La normalità dei disastri tecnologici. Il problema del congedo dal diritto penale*, Giuffrè, Milano, 2004, p. 400 ss.

F. CENTORAME, *La disciplina delle intercettazioni (ancora) nel mirino legislativo: chiose a margine della l. 9 ottobre 2023, n. 137*, in *Proc. pen. e giust.*, 2/2024, p. 478 ss.

M. CERASE, *Riforma della diffamazione: rintocchi della giurisprudenza e auspici legislativi*, in *Cass. pen.*, 11/2020, p. 4120 ss.

D. CERINI, *Dal Decreto Smart Roads in avanti ridisegnare responsabilità e soluzioni assicurative*, in *Danno resp.*, 2018, p. 401 ss.

A. CERRI, *Libertà di pensiero: manifestazione, diffusione, mezzi*, in *Giur. cost.*, 5-6/1972, p. 2877 ss.

- *Appunti sul sindacato di costituzionalità relativo al principio di eguaglianza*, in *Giur. cost.*, 3-6/1973, p. 860 ss.

- *L'eguaglianza*, Laterza, Bari, 2005.

Y. CHEN, A. S. CHEUNG, *The trasparent self under big data profiling: privacy and chinese legislation on the social credit system*, in *The journal of comparative law*, 12/2017, p. 356 ss.;

S. CHIARLONI, *Giurisprudenza e dottrina nell'era della rivoluzione informatica (note sui sistemi di documentazione)*, in *Riv. dir. proc.*, 2/1992, p. 590 ss.

M. CHIAROLLA, *La diffamazione a mezzo stampa. Analisi critica della normativa tra diritto di cronaca, diffamazione, privac*y, Experta, Forlì, 2004.

- *Trattamento dei dati personali su Internet ed illecito penale*, in *Foro it.*, 1/2006, 2, p. 46 ss.

D. CHINDEMI, *Diffamazione a mezzo stampa (radio-televisione-Internet)*, Giuffrè, Milano, 2006.

S. CICARELLO, *Dovere di protezione e valore della persona*, Giuffrè, Milano, 1988.

I. CIOLLI, *La salute come diritto in movimento. Eguaglianza, universalismo ed equità nel sistema sanitario nazionale, oggi*, in *BioLaw Journal*, 2/2019, p. 13 ss.

R. L. CLARK, R. G. HAMMOND, M. SANDLER MORRILL, C. KHALAF, *Nudging retirement savings: a field experiment on supplemental plans*, Working Paper 23679 – National Bureau of Economic Research, Cambridge (USA), 2017.

M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini,* in F. Basile, M. Caterini, S. Romano (a cura di), *Il sistema penale ai confini delle hard sciences. Percorsi epistemologici tra neuroscienze e intelligenza artificiale*, Pacini Editore, Pisa, 2021, p. 122 ss.

C. COLAPIETRO, *Libera manifestazione del pensiero, fake news e privacy, oggi*, in *dirittifondamentali.it*, 2/2022, p. 422 ss.

C. COLAPIETRO, A. MORETTI, *L'intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, in *BioLaw Journal*, 3/2020, p. 365 ss.

C. COLOMBO, *Il cyberbullismo. Una particolare tipologia di devianza*, in *Ind. pen.*, 3/2019, p. 441 ss.

D. COLOMBO, *Valutare per rieducare. Alternative al carcere e "risk assessment tools"*, in *Dir. pen. cont.*, 1/2024, p. 262 ss.

E. COLOMBO, *"Data retention" e Corte di giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della Direttiva 2006/24/CE*, in *Cass. pen.*, 7-8/2014, p. 2705 ss.

M.M. COMENALE PINTO, *Sistemi di bordo anticollisione e relative problematiche giuridiche*, in *Studi in onore di Umberto Leanza*, Editoriale Scientifica, Napoli, 2008, p. 1595 ss.

M. M. COMENALE PINTO – E. G. ROSAFIO, *Responsabilità civile per la circolazione degli autoveicoli a conduzione autonoma. Dal grande fratello al grande conducente*, in *Dir. trasp.*, 2/2019, p. 373 ss.

R. COMPOSTELLA, *Auto a guida autonoma e diritto penale. Profili di responsabilità individuale e collettiva*, Editoriale Scientifica, Napoli, 2024.

F. CONSORTE, *Tutela penale e principio di precauzione. Profili attuali, problematicità, possibili sviluppi*, Giappichelli, Torino, 2013, p. 20 ss.

F. CONSULICH, *Flash Offenders. Le prospettive di accountability penale nel contrasto alle intelligenze artificiali devianti*, in *Riv. it. dir. e proc. pen.*, 2022, p. 1015 ss.

G. CONTISSA, F. GALLI, F. GODANO, G. SARTOR, *Il regolamento europeo sull'IA*, in *Riv. di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale*, Vol. 14/2, 2021, p. 387 ss.

S. CORBETTA, *I delitti contro l'incolumità pubblica*, in G. Marinucci, E. Dolcini (a cura di), *Trattato di Diritto penale. Parte speciale*, II, 1, CEDAM, Padova, 2003, p. 365 ss.

R. CORDESCHI, *L'Intelligenza Artificiale* in *La Scienza*, 2005, originariamente pubblicata in E. Bellone, C. Mangione (a cura di), *Storia del pensiero filosofico e scientifico. Il Novecento*, vol. 8, III, Milano, 1996, p. 145 ss.

E. CORN, *Il principio di precauzione nel diritto penale. Studio sui limiti all'anticipazione della tutela penale*, Giappichelli, Torino, 2013.

L. CORNACCHIA, *Responsabilità penale da attività sanitaria in "équipe"*, in *Riv. it. med. leg.*, 3/2013, p. 1219 ss.

F. CORONA, *La decisione del giudice tra precedente giudiziale e predizione artificiale*, in *Democrazia e Diritti Sociali*, 1/2023, p. 83 ss.

G. CORRIAS LUCENTE, *Internet e libertà di manifestazione del pensiero*, in *Dir. inform.*, 4-5/2000, p. 597 ss.

- *La nuova normativa penale a tutela dei dati personali*, in F. Cardarelli, S. Sica, V. Zeno Zencovich, *Il codice dei dati personali. Temi e problemi*, Giuffrè, Milano, 2004.

F. COSTANTINI, *Il problema della sicurezza tra informatica e diritto: una prospettiva emergente dalle "smart cars"*, in *Inf. dir.*, 2016, p. 95 ss.

F. COSTANTINO, *Algoritmi, intelligenza artificiale e giudice amministrativo*, in *Giur. it.*, 6/2022, p. 1527 ss.

P. COSTANZO, *Libertà di manifestazione del pensiero e pubblicazione in internet*, in *Dir. inform.*, 2/1998, p. 372 ss.

C. COULON, *Révision de la Convention de Vienne sur la circulation routière: les voiture autonomes (pas tout à fait) sur la ligne de départ*, in *Resp. civ. et assurance*, alerte 17, 6/2016, p. 57 ss.

S. CRESCI, R. DI PIETRO, M. PETROCCHI, A. SPOGNARDI, M. TESCONI, *The paradigm-shift of social spambots: Evidence, theories, and tools for the arms race*, in *Proceedings of the 26th international conference on world wide web companion*, 2017, p. 963 ss.

E. CRIPPA, *Riconoscimento facciale e vita privata*, in *Riv. it. dir. e proc. pen.*, 4/2023, p. 1660 ss.

S. CRISAFULLI BUSCEMI, *Alcune considerazioni sulla situazione giuridica delle navi manovrate da lontano*, in *Studi in onore di F. Berlingieri*, Pubblicazione dell'Associazione Italiana di Diritto Marittimo, Genova, 1933, p. 191 ss.

C. CUPELLI, *La sfida dell'intelligenza artificiale al diritto penale*, in *Sistema penale*, 12 aprile 2023.

A. D'ADDA, *La Corte di Cassazione riafferma il proprio orientamento in tema di diritto all'identità personale*, in *Resp. civ. prev.*, 2-3/1997, p. 474 ss.

G. D'ALFONSO, *Verso una maggiore responsabilizzazione dell'"hosting provider" tra interpretazione evolutiva della disciplina vigente, innovazioni legislative e prospettive "de jure condendo"*, in *federalismi.it*, 2/2020, p. 108 ss.

J. DANAHER, *Robots, Law and the Retribution Gap*, in *Ethics and Information Technology*, 2016, p. 299 ss.

G. D'ARCA, *Profili problematici della responsabilità penale del medico per attività in équipe: successione nella posizione di garanzia e principio di affidamento*, in *Riv. it. med. leg.*, 2/2019, p. 671 ss.

D. D'AURIA, *Le modifiche apportate alla materia della circolazione stradale*, in *Dir. pen. e proc.*, 2010, p. 1274 ss.

S. DEL CORSO, *La Protezione dei dati personali. Commentario sistematico al d.lgs. 30 giugno 2003, n. 196*, Padova 2007, sub art. 167.

A. DE LIA, *Il principio di uguaglianza ed il diritto penale sostanziale: una sintetica analisi del rapporto*, in *federalismi.it*, 23/2017, p. 15 ss.

M. DELLACASA, *"Punitive damages", risarcimento del danno, sanzioni civili: un punto di vista sulla funzione deterrente della responsabilità aquiliana,* in *Contr. impr.*, 4/2017, p. 1142 ss.

P. DELL'ANNO, *Obbligo di motivazione e "ragionevole dubbio"*, in *Proc. pen. e giust.*, 3/2017, p. 16 ss.

J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. e proc. pen.*, 3/2022, p. 1057 ss.

J. DELLA VALENTINA, *L'insostenibile leggerezza del principio di prevedibilità di fronte al "diritto penale europeo"*, in *Dir. pen. cont.*, 3/2023, p. 76 ss.

E. DELLA VALLE, *Il giudice tributario robot*, in *Riv. dir. trib.*, 2022, p. 15 ss.

M. DELL'UTRI, *La giustizia predittiva. Introduzione*, in *Giur. it.*, 7/2022, p. 1759 ss.

R. DE MEO, *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Dir. inform.*, 3/2013, p. 587 ss.

G. DE MINICO, *Too many rules or zero rules for the ChatGPT?*, in *BioLaw Journal*, 2/2023, p. 491 ss.

G.P. DEMURO, *Il pericolo e la sua pena: tra proporzionalità e ne bis in idem*, in *Riv. it. dir. e proc. pen.*, 2023, p. 903.

- *Uguali ma diversi: sul reato di omicidio stradale o nautico*, in *Sistema Penale*, 21 settembre 2023.

F. DE SIMONE *'Fake news', 'post truth', 'hate speech': nuovi fenomeni sociali alla prova del diritto penale*, in *Arch. pen.*, 1/2018, p. 4 ss.

M. F. DE TULLIO, *Uguaglianza sostanziale e nuove dimensioni della partecipazione politica*, Editoriale Scientifica, Napoli, 2020.

A. DEVEREAUX, L. PENG, *Give us a little social credit: to design or to discover personal ratings in the era of Big Data*, in *Journal of Institutional Economics*, 16/2020, p. 369 ss.

I. P. DI CIOMMO, *La prospettiva del controllo nell'era dell'Intelligenza Artificiale: alcune osservazioni sul modello "Human In The Loop"*, in *federalismi.it*, 9/2023, p. 68 ss.

M. DI FLORIO, *Istigazione all'odio razziale e algoritmi di pericolosità*, in *Giur. it.*, 6/2022, p. 1477 ss.

- *"Calculate criminal law"? Criticità nell'uso degli algoritmi di pericolosità sociale*, in *Leg. pen.*, 1/2023, p. 327 ss.

F.P. DI FRESCO, *In tema di diffamazione telematica*, in *Foro it.*, 9/2007, 2, p. 486 ss.

O. DI GIOVINE, *Il judge-bot e le sequenze giuridiche in materia penale (intelligenza artificiale e stabilizzazione giurisprudenziale)*, relazione al convegno su *Il principio di legalità fra legislatore e giudice*, Università di Foggia, 25 settembre 2019, in *Cass. pen.*, 3/2020, p. 953 ss.

G. DODARO, *Uguaglianza e diritto penale. Uno studio sulla giurisprudenza costituzionale*, Giuffrè, Milano, 2012.

M. DOGLIOTTI, *Il diritto all'identità personale approda in Cassazione*, in *Giust. civ.*, 1/1985, p. 3049 ss.

P. DOMINGOS, *L'algoritmo definitivo: la macchina che impara da sola e il futuro del nostro mondo*, Bollati Boringhieri, Torino, 2016, p. 7 ss.

F. DONATI, *"Fake news" e libertà di informazione*, in *MediaLaws*, 2/2018, p. 36 ss.

- *Impieghi dell'Intelligenza artificiale a servizio della giustizia. Tra rischi e opportunità*, in *AI Anthology*, *Profili giuridici, economici e sociali dell'intelligenza artificiale*, Il Mulino, Bologna, 2022, p. 179 ss.

M. DONINI, *Il volto attuale dell'illecito penale. La democrazia penale tra differenziazione e sussidiarietà*, Giuffrè, Milano, 2004.

- *Il diritto penale come etica pubblica. Considerazioni sul politico quale "tipo d'autore"*, Mucchi Editore, Modena, 2014.

P. DUNN, *Moderazione automatizzata e discriminazione algoritmica: il caso dell'"hate speech"*, in *Inf. dir.*, 1/2022, 2, p. 133 ss.

M. DURANTE, *Potere computazionale. L'impatto delle ITC*, in *Diritto, società, sapere*, Meltemi, Milano, 2019.

E.F.D. ENGELHARD, R.W. DE BRUIN, *Liability for damage caused by autonomous vehicles*, Eleven International Publishing, L'Aia, 2019.

C. EQUIZI, *Libertà di manifestazione del pensiero e piattaforme online*, in *dirittifondamentali.it*, 3/2021, p. 550 ss.

C. ESPOSITO, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Giuffrè, Milano, 1958.

G. M. ESPOSITO, *Al confine tra algoritmo e discrezionalità. Il pilota automatico tra procedimento e processo*, in *Diritto e processo amministrativo*, 1/2019, p. 39 ss.

EUROPOL INNOVATION LAB, *The criminal use of ChatGPT – a cautionary tale about large language models*, 2023.

L. EUSEBI, *Quale diritto penale nel futuro europeo?*, in *Criminalia*, 2020, p. 87 ss.

G. FABRI, *Sul reato di diffamazione*, in *Foro it.*, 10/2023, 2, p. 551 ss.

N. FAIOLA, *"Data retention" ed accesso ai dati per scopi securitari: condizioni e limiti alla luce della giurisprudenza della Corte di giustizia dell'Unione europea*, in *Dir. Un. eur.*, 1/2023, p. 77 ss.

P. FALLETTA, *Controlli e responsabilità dei "social network" sui discorsi d'odio "online"*, in *MediaLaws*, 1/2020, p. 146 ss.

P. FALLETTA, A. MARSANO, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR*, in *Inf. dir.*, 1/2024, p. 119 ss.

E. FALLETTI, *Uso di algoritmi predittivi con scopo investigativo e violazione costituzionale del "Persönlichkeitsrecht"*, in *Foro it.*, 6/2023, 4, p. 298 ss.

- *Alcune riflessioni sull'applicabilità dell'art. 22 GDPR ["General Data Protection Regulation" - Regolamento generale sulla protezione dei dati] in materia di "scoring" creditizio*, in *Dir. inform.*, 1/2024, p. 110 ss.

A. FALLONE, *Appello dell'assoluzione, motivazione rafforzata, principio dell'oltre ogni ragionevole dubbio, rinnovazione dibattimentale: la giurisprudenza italiana e della Corte di Strasburgo*, in *Cass. pen.*, 2/2015, p. 820 ss.

F. FARRI, *Questioni in tema di giustizia predittiva in materia tributaria*, in *Il processo*, 3/2023, p. 841 ss.

M. FASAN, *Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico*, in *BioLaw Journal*, 1/2019, p. 6 ss.

L. FERRAJOLI, *Sul significato del principio di uguaglianza. Una replica*, in *Notizie di Politeia*, 133/2019, p. 259 ss.

E. FERRARA, O. VAROL, C. DAVIS, F. MENCZER, A. FLAMMINI, *The rise of social bots*, in *Communications of the ACM*, 2021.

S. FERRARINI, *Note sul concetto di naufragio*, in *Riv. Dir. Nav.*, 1963, p. 90 ss.

F. FERREIRA, *La questione della compatibilità dei sistemi automatizzati di filtraggio con la libertà di manifestazione del pensiero alla luce della sentenza CGUE, C-401/2019*, in *dirittifondamentali.it*, 3/2023, p. 383 ss.

G. FIANDACA, *La tipizzazione del pericolo*, in *Beni e tecniche di tutela penale,* Franco Angeli, Milano, 1984.

- *L'offensività è un principio codificabile?*, in *Foro it.*, 2001, V, p. 1 ss.

G. FIANDACA, E. MUSCO, *Diritto penale. Parte generale*, Zanichelli, Bologna, 2010.

G. FIORINELLI, *L'attuale ruolo del provider nella società digitale: modelli di responsabilità penale*, in *Leg. pen.*, 4/2022, p. 258 ss.

- *Il concorrente virtuale: la prevenzione dell'uso di ChatGPT per finalità criminali tra etero- e auto-regolazione*, in *Riv. it. med. leg.*, 2/2023, p. 361 ss.

S. FLAMINIO, *Lotta alle "fake news": dallo stato dell'arte a una prospettiva di regolamentazione per il vivere digitale a margine del "Digital Services Act"*, in *Inf. dir.*, 2/2022, p. 75 ss.

L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta cambiando il mondo*, Raffello Cortina editore, Milano, 2017.

- *Semantic Capital: Its Nature, Value and Curation*, in *Philosophy and Technology*, 2/2018, p. 481.

- *What the Near Future of Artificial Intelligence Could Be*, in *Philosophy & Technology*, 32/2019, p. 11 ss.

L. FOFFANI, *Responsabilità per il prodotto e diritto comunitario: verso un nuovo diritto penale del rischio? Note comparatistiche sugli ordinamenti italiano e spagnolo*, in Donini, Castronuovo (a cura di), *La riforma dei reati contro la salute pubblica*, CEDAM, Padova, 2007, p. 152.

C. FONTANA, *Definizioni e lineamenti tecnici essenziali dell'intelligenza artificiale: cenni al quadro regolamentare e ai principali problemi giuridici*, in G.C. Ferroni, C. Fontana, E.C. Raffiotta (a cura di), *AI Anthology, Profili giuridici, economici e sociali dell'intelligenza artificiale*, Il Mulino, Bologna, 2022, p. 65 ss.

G. FORMICI, *La "data retention saga" al capolinea? Le ultime pronunce della CGUE in materia di conservazione dei metadati per scopi securitari, tra conferme e nuove aperture*, in *DPCE online*, 1/2021, p. 1361 ss.

- *Le Conclusioni dell'Avvocato Generale nel rinvio pregiudiziale C-178/22 promosso dal Tribunale di Bolzano: "quo vadis, data retention"?*, in *MediaLaws*, 2/2023, p. 158 ss.

G. FORNASARI, *Dilemma etico del male minore e ticking bomb scenario. Riflessioni penalistiche (e non) sulle strategie di legittimazione della tortura*, Edizioni Scientifiche, Napoli, 2020.

G. FORTI, *Colpa ed evento nel diritto penale*, Giuffrè, Milano, 1990.

- *"Accesso" alle informazioni sul rischio e responsabilità: una lettura del principio di precauzione*, in *Criminalia*, 2006, p. 205 ss.

- voce *Colpa (dir. pen.)*, in *Diz. dir. pubbl. Cassese*, Vol. II, Milano, 2006, p. 950 ss.

S. FRANKLIN, A. GRAESSER, *Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents*, in J.P. Müller, M.J. Wooldridge, N.R. Jennings (a cura di), *Intelligent Agents III Agent Theories, Architectures, and Languages*, Springer, Berlino, 1996, p. 21 ss.

M.T. FRANZÉ, *La proposta normativa tedesca sulla guida autonoma, il via ai test sulle strade*, in *Cyberlaws*, 18 settembre 2018.

K. FREEMAN, *Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in State v. Loomis*, in *North Carolina Journal of Law & Technology*, 18/2016, p. 76 ss.

E. FRONZA, *"Code is Law". Note a margine del volume di Antoine Garapon e Jean Lassègue, Justice Digitale. Révolution graphique et rupture anthropologique*, in *Dir. pen. cont.*, 11 dicembre 2018.

G. FUGGETTI, *Possibilità e limiti di un diritto penale europeo*, in *Ind. pen.*, 1/1999, p. 445 ss.

E. GABELLINI, *La "comodità del giudicare": la decisione robotica*, in *Riv. trim. dir. proc. civ.*, 2019, p. 1309 ss.

S. GABORIAU, *Libertà e umanità del giudice: due valori fondamentali della giustizia. La giustizia digitale può garantire nel tempo la fedeltà a questi valori?*, in *Quest. giust.*, 4/2018, p. 11 ss.

M.C. GAETA, *La protezione dei dati personali nell'IoT, l'esempio dei veicoli autonomi*, in *Dir. inform.*, 1/2018, p. 147 ss.

A. GALASSO, *Il principio di uguaglianza nella Costituzione europea. Diritti fondamentali e rispetto della diversità*, Franco Angeli, Milano, 2007

D. GALETTA, *"Human-stupidity-in-the-loop"? Riflessioni (di un giurista) sulle potenzialità e i rischi dell'Intelligenza Artificiale*, in *federalismi.it*, 5/2023, p. 4 ss.

G. GALLO, *Tecnologie di riconoscimento facciale e diritti fondamentali a rischio: il caso "Glukhin c. Russia" dinanzi alla Corte europea dei diritti dell'uomo*, in *MediaLaws*, 3/2023, p. 189 ss.

A. GAMBARO, *Diritti della personalità*, in *Riv. dir. civ.*, 6/1981, 2, p. 519 ss.

S. GAMBINO, *Stato regionale, principio di eguaglianza, diritti sociali. Problematiche di effettività con particolare riguardo alla tutela della salute*, in *DPCE online*, 2/2021, p. 2461 ss.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, provvedimento n. 127 del 25 marzo 2021.

- *Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori*, 2023.

A. GARAPON, J. LASSEGUE, *Justice Digitale: révolutiongraphique et ruptureanthropologique*, PUF, Parigi, 2018.

A. GARGANI, *Il danno qualificato dal pericolo. Profili sistematici e politico-criminali dei delitti contro l'incolumità pubblica*, Giappichelli, Torino, 2005.

- *Reati contro l'incolumità pubblica,* in C.F. Grosso, T. Padovani, A. Pagliaro (a cura di), *Trattato di Diritto penale. Parte speciale*, IX, 1, Giuffrè, Milano 2008, p. 329 ss.

- *Il rischio nella dinamica dei reati contro l'incolumità pubblica e nei reati di pericolo astratto*, in *Cass. pen.*, 11/2017, p. 3879 ss.

F. J. GAROFOLI, *"Le regole del kaos" tra verità scientifica e ragionevole dubbio*, in *Ind. pen.*, 2/2019, p. 195 ss.

V. GAROFOLI, *Dalla non considerazione di colpevolezza alla regola dell'oltre il ragionevole dubbio*, in *Dir. pen. e proc.*, 9/2010, p. 1029 ss.

E. GARZONIO, *Responsabilità degli ISP ["Internet Service Provider" - Fornitore di servizi Internet] rispetto al trattamento automatizzato dei dati personali con finalità di comunicazione politica: applicabilità del GDPR alle piattaforme "social"*, in *MediaLaws*, 2/2019, p. 190 ss.

I. GASPARINI, *L'odio ai tempi della rete: le politiche europee di contrasto all'"online hate speech",* in *Jus*, 3/2017, p. 505 ss.

C. V. GIABARDO, *Il giudice e l'algoritmo (in difesa dell'umanità del giudicare)*, in *Giustizia insieme*, 9 luglio 2020.

P. GIACALONE, *Intelligenza artificiale, giustizia predittiva e processo tributario: problemi e prospettive*, in *Riv. dir. trib.*, 3/2023, p. 299 ss.

L. GIACOMELLI, *Ripensare l'eguaglianza. Effetti collaterali della tutela antidiscriminatoria*, Giappichelli, Torino, 2018.

M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *Dir. pen. cont.*, 29 maggio 2019.

- *Le novità della "manovra Nordio" in materia processuale: quando l'ideologia rischia di provocare un'eterogenesi dei fini*, in *Sistema Penale*, 22 Luglio 2024.

A. GIANNINI, *Intelligenza artificiale, human oversight e responsabilità penale: prove d'impatto a livello europeo*, in *Criminalia*, 2022.

L. GIORDANO, *Una nuova riforma della disciplina delle intercettazioni*, in *Dir. pen. e proc.*, 1/2024, p. 11 ss.

C. GIORGI, *Il progetto costituzionale dell'uguaglianza*, Futura, Perugia, 2014.

G. GIORGINI PIGNATIELLO, *Il contrasto alle discriminazioni algoritmiche: dall'anarchia giuridica alle "Digital Authorities"?*, in *federalismi.it*, 16/2021, p. 114 ss.

A. GIORGIS, *La costituzionalizzazione dei diritti all'uguaglianza sostanziale*, Jovene, Napoli, 1999.

G. GIUFFRIDA, F.M. RINALDI, *Big Data, Intelligenza Artificiale e Machine Learning: tra discriminazione e responsabilità algoritmica*, in S. Gozzo, C. Pennisi, V. Asero, R. Sampugnaro (a cura di), *Big Data e processi decisionali*, p. 35 ss.

I. GIUGNI, *Causalità della colpa e circolazione stradale tra prassi applicative e dubbi irrisolti*, in *Dir. Pen. Cont.*, 1/2019, p. 6 ss.

F. GIUNTA, *Illiceità e colpevolezza nella responsabilità colposa*, CEDAM, Padova, 1993, p. 334 ss.

- *Il diritto penale e le suggestioni del principio di precauzione*, in *Criminalia*, 2006, p. 229 ss.

- *Oltre la logica della punizione: linee evolutive e ruolo del diritto penale*, in E. Dolcini; C.E. Paliero (a cura di), S*tudi in onore di Giorgio Marinucci*, Giuffrè, Milano, 2006, p. 356 ss.

L. GIZZI, *Orientamenti giurisprudenziali in tema di responsabilità medica in équipe*, in *Dir. pen. e proc.*, 6/2006, p. 753 ss.

D.G. GLEAVE, R. FRISONI, A. DALL'OGLIO, C. NELSON, J. LONG, C. VOLLA, D. RANGHETTI, S. MCMINIMY, *Self Piloted Cars: the Future of Road Transport?, Research for the Transport and Tourism Committee of the European Parliament*, 2016, consultabile sul sito *web* del Parlamento europeo.

B. GOGARTY, M. HAGGER, *The Laws of Man over Vehicles Unmanned: the Legal Response to Robotic Revolution on Sea, Land and Air*, in *JLawInfoSci*, 19/2008, p. 73 ss.

B. GOGARTY, I. ROBINSON, *Unmanned Vehicles: a (Rebooted) History, Background and Current State of the Art*, in *JLawInfoSci*, 21/2012, p. 1 ss.

A. GOLIA, *Pluralità degli ordinamenti giuridici e costituzionalizzazione degli spazi digitali. Osservazioni sulla giurisprudenza dell'"Oversight Board"*, in *Quad. cost.*, 3/2023, p. 595 ss.

R. GORWA, R. BINNS, C. KATZENBACH, *Algorithmic content moderation: Technical and political challenges in the automation of platform governance*, in *Big Data & Society*, 7/2020, p. 4 ss.

G. GRASSO, *Il Trattato di Lisbona e le nuove competenze penali dell'Unione*, in M. Bertolino, L. Eusebi, G. Forti (a cura di), *Studi in onore di Mario Romano*, vol. IV, Jovene, Napoli, 2011, p. 2326 ss.

G. GRASSO, R. SICURELLA, *Lezioni di diritto penale europeo*, Giuffrè, Milano, 2007.

P. GRAZIANI, M. SANGOI, *La macchina aritmetica di Blaise Pascal*, in *Isonomia*, Istituto di Filosofia dell'Università di Urbino, 2005.

B. GRAZZINI, *"Fake news" e disinformazione*, in *Giur. it.*, 2/2024, p. 491 ss.

C. GRECO, *Quest'acquisizione non s'ha da fare: ennesimo "no" della Corte di Giustizia alla "data retention" indiscriminata in campo penale*, in *Dir. inform.*, 2/2021, p. 235 ss.

M. GRIGOLI, voce *Naufragio (dir. nav.)*, in *Enc. dir.,* XXVII, Milano, 1977, p. 559 ss.

I. GRIMALDI, *Il principio di proporzionalità della pena nel disegno della Corte Costituzionale*, in *Giurisprudenza Penale Web*, 2020, 5, p. 2 ss.

M. GROTTO, *Principio di colpevolezza, rimproverabilità soggettiva e colpa specifica*, Giappichelli, Torino, 2012.

F. GUELLA, *"Data retention" e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali*, in *DPCE online*, 2/2017, p. 19 ss.

F. GUELLA, C. PICIOCCHI, *Libera manifestazione del pensiero tra fatti di sentimento e fatti di conoscenza*, in *Quad. cost.*, 4/2013, p. 849 ss.

T. GUERINI, *Fake news e diritto penale*, Giappichelli, Torino, 2020.

L. GUERRA, *Il Sistema di credito sociale cinese tra mistificazioni e realtà*, in *Treccani online*, 13 maggio 2024.

A. GULLO, *Diffamazione e legittimazione dell'intervento penale*, Aracne, Roma, 2013.

- *Diffamazione, pena detentiva e "chilling effect": la Consulta bussa alla porta del legislatore*, in *Dir. pen. e proc.*, 2/2021, p. 217 ss.

G. HALLEVY, *The Criminal Liability of Artificial Inteligence Entitis - from Science Fiction to Legal Social Control*, in *Akron Intelectual Property Journal*, 4/2010, p. 171 ss.

- *I Robot - I, Criminal: When Science Fiction Becomes Reality: Legal Liability of Al Robots Commiting Criminal Offenses*, in *Syracuse Science and Technology Law Reporter*, 22/2010, p. 1 ss.

- *Unmanned Vehicles: Subordination to Criminal Law under the Modern Concept of Criminal Liability. Comment*, in *JLawInfoSci*, 21/2012, p. 200 ss.

- *The Basic Models of Criminal Liability of AI Systems and Outer Circles*, presentato presso *FOI, the Swedish Defense Research Agency*, Stoccolma, 11 giugno 2019.

K. HAO, *What is machine learning*, in *MIT Technology Review*, 17 novembre 2018.

M. HARRIS, *Exclusive: Arizona governor and Uber kept self-driving program secret, emails reveal*, in *The Guardian*, 28 marzo 2018.

D. O. HEBB, *The organization of behavior; a neuropsychological theory*, Wiley, New York, 1949.

F. HENKEL, J. NOWAK, N.SMIRRA, *Autonomous vehicles: the legal landscape in Germany,* in *Norton Rose Fulbright*, 11 agosto 2016.

A. HERRMANN, W. BRENNER, R. STADLER, *Autonomous Driving, How the Driverless Revolution Will Change the World*, Emerald Publishing Limited, Bingley, 2018.

J. HOCH, A. SHAMIR, *On the Strength of the Concatenated Hash Combiner when All the Hash Functions Are Weak*, in *eprint.iacr.org*, 2008.

IAEME PUBLICATION, *Exploring data lakes: a cornerstone of big data engineering*, in *International Journal of Advanced Research in Engineering and Technology (IJARET)*, Vol. 15, Issue 3, May-June, 2024, p. 211 ss.

P. IAMICELI, *Il consenso al trattamento dei dati personali e la giurisprudenza europea tra tutela dei diritti fondamentali e giustizia contrattuale*, in *Persona e Mercato*, 1/2024, p. 27 ss.

A. IANNOTTI DELLA VALLE, *La giurisdizione privata nel mondo digitale al tempo della crisi della sovranità: il "modello" dell'"Oversight Board" di Facebook*, in *federalismi.it*, 26/2021, p. 144 ss.

A. IANNUZZI, *Considerazioni sul disegno di legge "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (AC 1717). Audizione informale innanzi alle Commissioni riunite I (Affari costituzionali) e II (Giustizia) della Camera dei Deputati*, in *Inf. dir.*, 1/2024, p. 59 ss.

E. M. INCUTTI, *Il principio di non discriminazione nei rapporti contrattuali di lavoro autonomo*, in *Nuova giur. civ. comm.*, 6/2023, p. 1241 ss.

A. INGRAO, *Critica della ragione artificiale. La discriminazione algoritmica intersezionale e gli obblighi di parità di trattamento in ipotesi di impiego di sistemi decisionali automatizzati*, in *Riv. giur. lav.*, 2/2024, 2, p. 170 ss.

G. INGRAO, A. BUCCISANO, *L'intelligenza artificiale e la giustizia predittiva alla luce del progetto "Prodigit"*, in *Riv. dir. trib.*, 2022, p. 70 ss.

A. INGRASSIA, *Responsabilità penale degli "internet service provider": attualità e prospettive*, in *Dir. pen. e proc.*, 12/2017, p. 1621 ss.

C. INGRATOCI*, Autonomous vehicles in smart roads: an integrated management system for road circulation*, in *Dir. trasp.*, 2020, p. 97 ss.

F. IOVENE, *"Data retention" tra passato e futuro. Ma quale presente?*, in *Cass. pen.*, 12/2014, p. 4274 ss.

N. IRTI, *Per un dialogo sulla calcolabilità giuridica*, in A. Carleo (a cura di), *Calcolabilità giuridica*, Il Mulino, Bologna, 2017, p. 17 ss.

G. A. JACOVONE, *Il delitto di sostituzione di persona*, Jovene, Napoli, 1974.

D. KAHNEMAN, A. TWERSKY, P. SLOVIC, *Judgment under uncertainity. Heuristics and biases*, Cambridge, 1982.

J. KAPLAN in *Intelligenza artificiale. Guida al futuro prossimo*, Luiss University Press, Roma, II ed., 2018, p. 72 ss.

B. KARDON, *Is every company really an AI company?*, in *AdAge*, 2019, consultabile sul sito *web* www.adage.com.

A. KASAP, *Autonomous vehicles, tracing the Locus of regulation and liability*, Edward Elgar Publishing, Cheltenham, 2022.

C. KAWA, P.M. IANIRO DAHM, J. F. H. NIJHUIS, W.H. GIJSELAERS, *Cafeteria online: nudges for healthier food choices in a university cafeteria – a randomized online experiment,* in *National Insitutes of Health (NIH),* 2021.

M. KLETTKE, U. STÖRL, S. SCHERZINGER, *Uncovering the Evolution History of Data Lakes*, in *IEEE International Conference on Big Data (BIGDATA)*, 2017.

C.KRONCKE, *Nudging towards a stable retirement*, in *Politics and the Life Sciences*, 37, 1/2018, p. 126 ss.

F. KUNKLE, *Fatal crash with self-driving car was a first - like Bridget Driscoll's was 121 years ago with one of the first cars*, in *Washington Post*, 22 marzo 2018.

G. M. LABRIOLA, *La libertà di espressione fra ragione e storia. Nota breve su un tema vasto*, in *Notizie di Politeia*, 138/2020, p. 95 ss.

F. LAGIOIA, G. SARTOR, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in *federalismi.it*, 11/2020, p. 85 ss.

M. LAMANUZZI, *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento 2016/679/UE e nuove responsabilità per gli enti*, in *JusOnline*, 1/2017, p. 218 ss.

- *Il cyberbullismo. Prospettive criminologiche e giuridico-penali a partire dalla l. 71/2017*, in *JusOnline*, 6/2020, p. 166 ss.

- *La disinformazione ai tempi dei social media: una nuova sfida per il diritto penale?*, in *Arch. Pen.*, 1/2020.

L. LAMBO, *Obblighi di protezione*, CEDAM, Padova, 2007.

M. LANZI, *Self-driving cars e responsabilità penale. La gestione del rischio stradale nell'era dell'intelligenza artificiale*, Giappichelli, Torino, 2023.

U. LA TORRE, *Comando e comandante nell'esercizio della navigazione*, Edizioni Scientifiche, Napoli, 1997.

- *Equipaggio, comando e determinazione della rotta nella navigazione marittima*, in *Riv. Dir. Nav.* 2013, p. 95 ss.

- *Funzione di comando e sicurezza della navigazione*, in E. Turco Bulgherini, F. Salerno (a cura di), *Infrastrutture e navigazione: nuovi profili della sicurezza marittima ed aerea*, Aracne, Roma, 2013, p. 92 ss.

- *Navi senza equipaggio e shore control operator*, in *Dir. trasp.*, 2019, p. 487 ss.

G. LATTANZI, *L'omicidio stradale. Relazione al convegno sul tema "Ipotesi su una nuova figura di reato: l'omicidio stradale – Napoli 7 marzo 2014"*, in *Cass. pen.*, 2014, p. 1988 ss.

A. LAURO, *Un "devoir de justice": le sfide dell'uguaglianza nel diritto all'istruzione scolastica*, in *Costituzionalismo.it*, 1/2023, 2, p. 27 ss.

F. LA VATTIATA, *Brevi note "a caldo" sulla recente Proposta di Regolamento UE in tema di intelligenza artificiale*, in *Dir. pen. e Uomo*, 30 giugno 2021, p. 9 ss.

- *La responsabilità penale per danni da intelligenza artificiale alla prova del processo*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, E M. Proto (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Giuffrè, Milano, 2022.

F. LAVIOLA, *Regolazione della tecnologia e dimensione del tempo*, in *Osservatorio sulle fonti*, 3/2021, p. 1163 ss.

E. LECALDANO, *Identità: una critica tra storia e teoria*, in *Notizie di Politeia*, 135/2019, p. 8 ss.

S. LEONE, *Sindacato di ragionevolezza e quantum della pena nella giurisprudenza costituzionale*, in *Riv. A.I.C.*, 2017, p. 11 ss.

N. LETTIERI, *La discriminazione nell'era delle macchine intelligenti. Modelli possibili di analisi, critica e tutela*, in *GenIUS*, 1/2022, p. 10 ss.

E. LO MONTE, *Intelligenza artificiale e diritto penale: le categorie dommatiche alla prova del futuribile*, in F. Basile, M. Caterini, S. Romano (a cura di), *Il sistema penale ai confini delle hard sciences. Percorsi epistemologici tra neuroscienze e intelligenza artificiale*, Pacini Editore, Pisa, 2021, p. 41 ss.

S. LORUSSO, *"Digital evidence", "cybercrime" e giustizia penale 2.0*, in *Proc. pen. e giust.*, 4/2019, p. 821 ss.

M. LOSANO, *Il Progetto di legge Tedesco sull'auto a guida automatizzata. Appendice: il Progetto di legge e le relazioni illustrative*, in *Dir. inform.*, 2017, p. 3 ss.

- *Verso l'auto a guida autonoma in Italia*, in *Dir. inform.*, 2019, p. 423 ss.

G. LO SAPIO, *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*, in *Federalismi.it*, 2021.

G. LOSAPPIO, *Dei nuovi delitti di omicidio e lesioni stradali*, in *Dir. pen. cont.*, 30 giugno 2016.

M. LUBERTO, *I reati informatici contro il diritto alla privacy. La tutela fornita dal d.lgs. n. 196 del 2003 e dal codice penale*, in *Giur. mer.*, 2008, p. 898 ss.

L. LUDOVICI, *Disegno di legge c.d. Nordio: nuove garanzie processuali tra fughe in avanti e false partenze*, in *Leg. pen.*, 2/2024, p. 112 ss.

M. LUGATO, *Il «discorso di odio»: le coordinate giuridiche del ragionamento internazionalistico*, in *Riv. dir. int.*, 4/2022, p. 959 ss.

L. LUPÀRIA DONATI, G. FIORELLI, *Diritto probatorio e giudizi criminali ai tempi dell'Intelligenza Artificiale*, in *Dir. pen. cont.,* 2/2022, p. 39 ss.

D. LYON, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano, 2002.

G. MACCABONI, *La profilazione dell'utente telematico tra tecniche pubblicitarie online e tutela della privacy*, in *Dir. inform.*, 3/2001, 1, p. 425 ss.

A. MACCHIA, *Libero convincimento del giudice, dalle prove legali al ragionevole dubbio. Le regole europee*, in *Cass. pen.*, 6/2022, p. 2043 ss.

A. MADEO, *Diffamazione e "hate speech": quando il giudizio non è meramente critico ma discriminatorio in ragione dell'orientamento sessuale*, in *GenIUS*, 2/2022, p. 205 ss.

T. MADIEGA, *Artificial intelligence act*, Briefing 28 giugno 2023, sul sito *web* www.europarl.europa.eu.

S. MAGAGNOLI, *Divieti di discriminazione e lavoro autonomo: un primo passo nella ridefinizione dei confini del diritto del lavoro*, in *Dir. relaz. ind.*, 2/2023, p. 544 ss.

C. MAGNANI, *Nuovi media, libertà di espressione e costituzionalismo*, in *dirittifondamentali.it*, 2/2023, p. 795 ss.

S. MAGNOSI, *Circolazione stradale e responsabilità delle automobili autonome: profili penalistici*, in *Dir. trasp., Atti dell'incontro di studi «L'automazione nei trasporti marittimi, aerei e terrestri»*, Cagliari, 9-10 novembre 2018, 2019, p. 325 ss.

M. B. MAGRO, *Biorobotica, robotica e diritto penale*, in D. Provolo, S. Riondato, F. Yenisey (a cura di), *Genetics, Robotics, Law, Punishment*, Padova University Press, 2014, p. 515 ss.

- *Robot, cyborg e intelligenze artificiali*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Cybercrime*, Utet Giuridica, Milano, 2019, p. 1179 ss.

- *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, in *Leg. pen.*, 2020.

A. MALACARNE, *"Gravità" dell'ingerenza e "terzietà" dell'organo titolare del potere autorizzatorio: vecchi e nuovi princìpi in materia di "data retention"*, in *Riv. it. dir. e proc. pen.*, 3/2021, p. 1164 ss.

- *Corte di giustizia e "data retention": ultimo atto?*, in *Cass. pen.*, 12/2021, p. 4105 ss.

A. MALASCHINI, *Il regolamento europeo sull'intelligenza artificiale (IA), l'orientamento italiano e i diversi indirizzi di Stati Uniti e Regno Unito*, in *Rass. parl.*, 1/2024, p. 35 ss.

S. MANACORDA, voce *Diritto penale europeo*, in *Enciclopedia Treccani*, 2014.

A. MANGANELLI, *Piattaforme digitali e "social network", fra pluralità degli ordinamenti, pluralismo informativo e potere di mercato*, in *Giur. cost.*, 2/2023, p. 883 ss.;

V. MANES, *Il principio di offensività nel diritto penale. Canone di politica criminale, criterio ermenuetico, parametro di ragionevolezza*, Giappichelli, Torino, 2005, p. 297 ss.

- *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. Ruffolo, *Intelligenza artificiale - Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020, p. 547 ss.

V. MANES, M. CAIANIELLO, *Introduzione al diritto penale europeo*, Giappichelli, Torino, 2020.

V. MANES, N. MAZZACUVA, *GDPR e nuove disposizioni penali del Codice "privacy"*, in *Dir. pen. e proc.*, 2/2019, p. 171 ss.

G. MANFREDI, *Note sull'attuazione del principio di precauzione in diritto pubblico*, 2004, in *Riv. trim. dir. pubbl.*, 2004, p. 1086 ss.

J. MANIKA, *Big Data: the next frontier for innovation, competition and productivity, Technical report*, McKinsey Global Institute, Vol. 7, 2011, sul sito *web* www.mckinsey.com;

A. MANNA, *La tutela penale dei diritti della personalità: aspetti problematici*, in *Indice pen.*, 3/1986, p. 711 ss.

- *Prime osservazioni sul Testo Unico in materia di protezione dei dati personali: profili penalistici*, in *privacy.it*, 2003, p. 1125 ss.

- *Il quadro sanzionatorio penale e amministrativo del codice sul trattamento dei dati personali*, in *Dir. inform.*, 2003, p. 727 ss.

- *Codice della privacy: nuove garanzie per i cittadini nel Testo unico in materia di protezione dei dati personali*, in *Dir. pen. e proc.*, 2004, p. 17 ss.

- *La regola dell'oltre il ragionevole dubbio nel pericolo astratto come pericolo reale*, in *Cass. pen.*, 2/2005, p. 640 ss.

- *Problemi vecchi e nuovi in tema di diffamazione a mezzo stampa*, in *Arch. pen.*, 3/2012, p. 989 ss.

F. MANTOVANI, *Diritto Penale. Parte generale*, XI ed., CEDAM, Padova, 2020, p. 675 ss.

M. MANTOVANI, *Contributo ad uno studio sul disvalore di azione nel sistema penale vigente*, Bologna University Press, 2014.

- *In tema di omicidio stradale*, in *Dir. Pen. Cont.*, 9 dicembre 2015.

- *Profili penali del "cyberbullismo": la l. 71 del 2017*, in *Ind. pen.*, 2/2018, p. 475 ss.

R. MANZOTTI, V. TAGLIASCO, *Etica delle macchine e «coscienza artificiale»*, in *L'Arco di Giano*, 2008, p. 33 ss.

G. MARCHETTI, *Le "fake news" e il ruolo degli algoritmi*, in *MediaLaws*, 1/2020, p. 29 ss.

S. MARCHIORI, P. SOMMAGGIO, *Break the chains: a new way to consider machine's moral problems*, in *BioLaw Journal*, 3/2018, p. 15 ss.

G. MARINI, *"Rischio consentito" e tipicità della condotta. Riflessioni*, in *Scritti in memoria di Renato Dell'Andro*, Cacucci Editore, Bari, 1994, vol. II, p. 542 ss.

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 ss.

- *La responsabilità colposa: teoria e prassi*, in *Riv. it. dir. e proc. pen.*, 2012, I, p. 3 ss.

G. MARINUCCI, E. DOLCINI, G. L. GATTA, *Manuale di diritto penale. Parte generale*, Giuffrè, Milano, 2021, p. 207 ss.

B. MARR, *Man vs. machine: the 6 greatest AI challenge to showcase the power of artificial intelligence*, in *Forbes* (*online*), 21 gennaio 2021.

P. MARRA, *La sostenibile certezza nel dubbio. A proposito di un libro di Antonio Incampo e Adolfo Scalfati su "Giudizio penale e ragionevole dubbio"*, in *Diritto & questioni pubbliche*, 1/2020, p. 16 ss.

G. MARTINELLI, voce *Reti neurali*, in *Enc. Treccani*, V Appendice, 1994.

F. MARTINI, *Incertezza scientifica, rischio e prevenzione. Le declinazioni penalistiche del principio di precauzione*, in *Responsabilità penale e rischio nelle attività mediche e d'impresa (un dialogo con la giurisprudenza)*, Firenze University Press, Firenze, 2010, p. 587 ss.

M. MASCALZONI, *Sulla responsabilità del direttore di un quotidiano on line per diffamazione*, in *Giur. it.*, 6/2011, p. 1378 ss.

A. MASSARO, *"Concretizzazione del rischio" e prevedibilità dell'evento nella prospettiva della doppia funzione della colpa*, in *Cass. pen.*, 12/2009, p. 4706 ss.

- *Principio di precauzione e diritto penale: nihil novi sub sole?*, in *Dir. pen. cont.*, 9 maggio 2011.

- *Principio di affidamento e "obbligo di vigilanza" sull'operato altrui: riflessioni in materia di attività medico-chirurgica in équipe*, in *Cass. pen.*, 11/2011, p. 3857 ss.

- *Omicidio stradale e lesioni personali stradali gravi o gravissime: da un diritto penale "frammentario" a un diritto penale "frammentato"*, in *Dir. Pen. Cont.*, 20 maggio 2016.

A. MATTARELLA, *Il "cybercrime" nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite*, in *Dir. pen. e proc.*, 6/2022, p. 809 ss.

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 *Arch. pen.*, 1/2021, p. 3 ss.

O. MAZZA, *Il ragionevole dubbio nella teoria della decisione*, in *Criminalia*, 2012, p. 357 ss.

N. MAZZACUVA, *L'apparente prossimità della colpa penale a garantismo e ultima ratio*, in M. Donini, R. Orlandi (a cura di), *Reato colposo e modelli di responsabilità*, Bologna University Press, Bologna, 2013, p. 41 ss.

P. MCCORDUCK, *Machines Who Think. A Personal Inquiry into the History and Prospects of Artificial Intelligence*, A.K. Peters, 2004.

M.E. MCGRATH, *Autonomous Vehicles, Opportunities, Strategies and Disruptions*, Independent Publishing Platform, Varsavia, 2018.

R. MCLAUGHLIN, *Unmanned Naval Vehicles at Sea: USVs, UUVs, and the Adequacy of the Law*, in *JLawInfoSci*, 21/2012, p. 100 ss.

L. MEGALE, *Il Garante della "privacy" contro "ChatGPT": quale ruolo per le autorità pubbliche nel bilanciare sostegno all'innovazione e tutela dei diritti?*, in *Giornale di diritto amministrativo*, 3/2023, p. 403 ss.

P. MELLO, voce *Intelligenza artificiale*, in *Dizionario Interdisciplinare di Scienza e Fede. Cultura scientifica, filosofia e teologia*, Roma, 2002.

C. MELZI D'ERIL, *La complessa individuazione dei limiti alla manifestazione del pensiero in internet*, in *Dir. inform.*, 4-5/2011, p. 571 ss.

- *"Fake news" e responsabilità: paradigmi classici e tendenze incriminatrici*, in *MediaLaws*, 1/2017, p. 6 ss.

A. MENGHINI, *L'omicidio stradale. Scelte di politica criminale e frammentazione del sistema*, Editoriale Scientifica, Napoli, 2016.

E. MENGONI, *"Chattare" con un "nickname" riconducibile ad altri (e comunicare il loro numero telefonico) integra il reato di sostituzione di persona*, in *Cass. pen.*, 1/2014, p. 148 ss.

A. MERLO, *Considerazioni sul principio di proporzionalità nella giurisprudenza costituzionale in materia penale*, in *Riv. it. dir. e proc. pen*, 2016, p. 1427 ss.

A. MESSINA, *Profili di criticità e di invalidità delle norme sanzionatrici del GDPR*, in *Ciberspazio e Diritto*, 1/2021, p. 3 ss.

D. MESSINA, *Online platforms, profiling, and artificial intelligence: new challenges for the GDPR and, in particular, for the informed and unambiguous data subject's consent*, in *MediaLaws*, 2/2019, p. 159 ss.

G. MICELI, *Profili evolutivi della responsabilità in rete: il ruolo degli "Internet Service Provider" tra prevenzione e repressione*, in *MediaLaws*, 1/2017, p. 10 ss.

M. MILITELLO, *Principio di uguaglianza e di non discriminazione tra Costituzione italiana e Carta dei diritti fondamentali dell'Unione Europea*, in *Rassegna di diritto pubblico europeo*, 1/2010, p. 85 ss.

V. MILITELLO, *Rischio e responsabilità penale*, Giuffrè, Milano, 1988.

C. MINELLI, *La responsabilità "penale" tra persona fisica e corporation alla luce della Proposta di Regolamento sull'Intelligenza Artificiale*, in *Dir. pen. cont.*, 2/2022, p. 50 ss.

G.R. MINELLI, *Quando l'autore del reato è un robot: tra vecchi modelli imputativi e nuovi possibili paradigmi di responsabilità penale*, in F. Basile, M. Caterini, S. Romano (a cura di), *Il sistema penale ai confini delle hard sciences. Percorsi epistemologici tra neuroscienze e intelligenza artificiale*, Pacini Editore, Pisa, 2021, p. 57 ss.

N. MINISCALCO, *Smart area, circolazione dei veicoli autonomi e protezione dei dati personali*, in S. Scagliarini (a cura di), *Smart Roads e driverless cars: tra diritto, tecnologie, etica pubblica*, Giappichelli, Torino, 2019, p. 27 ss.

G. MINNITI, *Finalità cautelari della norma, sua evoluzione nel tempo e accertamento della colpa*, in *Riv. trim. dir. pen. econ.*, 2006, p. 303 ss.

M. MIRAVALLE, *I nodi gordiani della giustizia penale ad alta intensità tecnologica. Verso il giudice bocca della tecnologia?*, in *Materiali per una storia della cultura giuridica*, 1/2020, p. 301 ss.

G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, in *federalismi.it*, 16/2020, p. 266 ss.

- *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, Napoli, 2021.

- *La Corte EDU condanna il ricorso alle tecnologie di riconoscimento facciale per reprimere il dissenso politico: osservazioni a partire dal caso "Glukhin c. Russia"*, in *DPCE online*, 1/2024, p. 695 ss.

S. MOCCIA, *La politica criminale del Corpus Juris: dal Corpus Juris al diritto penale europeo?*, in *Ind. pen.*, 3/2001, p. 1425 ss.

F. MOLLO, *Sorveglianza di massa, rispetto della vita privata e trattamento di categorie particolari di dati nel quadro multilivello di tutela della persona*, in *federalismi.it*, 19/2023, p. 267 ss.

D. MONETT, C.W.P. LEWIS, *Getting clarity by defining Artificial Intelligence - A Survey*, in V.C. Muller, *Philosophy and Theory of Artificial Intelligence*, Springer, Berlino, 2017, p. 212 ss.

A. MONTAGNA, *Il difficile cammino verso un diritto penale europeo minimo*, in *Cass. pen.*, 2/2007, p. 805 ss.

M. MONTI, *Regolazione, Internet e tecnica: le implicazioni di motori di ricerca e "social networks" sulla libertà di informazione*, in *federalismi.it*, 24/2017, p. 9 ss.

- *Privatizzazione della censura e internet platforms: la libertà di espressione e i nuovi censori dell'agorà digitale*, in *Inf. dir.*, 1/2019, p. 35 ss.

D. MORANA, *La libertà di manifestazione del pensiero sulla rete tra vecchi e nuovi limiti. Introduzione*, in *MediaLaws*, 1/2020, p. 132 ss.

D. MORONDO TARAMUNDI, *Le sfide della discriminazione algoritmica*, in *GenIUS*, 1/2022, p. 22 ss.

P. MOROZZO DELLA ROCCA, *Principio di uguaglianza e divieto di compiere atti discriminatori*, Edizioni Scientifiche Italiane, Napoli, 2002.

P. MOSCARINI, *Libertà d'informare, tutela dell'onore e punibilità della diffamazione "mediatica"*, in *Dir. pen. e proc.*, 10/2022, p. 1357 ss.

A. MULÈ, *Attività medica di équipe e responsabilità di componenti per omicidio colposo*, in *Foro it.*, 5/2007, 2, p. 308 ss.

F. MUNARI, *Il «dubbio ragionevole» nel rinvio pregiudiziale*, in *federalismi.it*, 18/2022, p. 162 ss.

M. MUSI, *La nozione di nave*, in *Il diritto marittimo – quaderni*, Bologna, 2020.

- *The phenomenon of «mass»: is it time to rethink the current maritime liability regime?,* in *Riv. Dir. Nav.*, 2/2021, p. 763 ss.

G. NADDEO, *Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella "data retention saga" dinanzi alla Corte di giustizia*, in *Freedom, Security & Justice: European Legal Studies*, 2/2022, p. 188 ss.

C. NARDOCCI, *Artificial Intelligence-based Discrimination: Theoretical and Normative Responses. Perspectives from Europe*, in *DPCE online*, 3/2023, p. 2367 ss.

- *Il riconoscimento facciale sul "banco" degli imputati. Riflessioni a partire, e oltre, Corte EDU "Glukhin c. Russia"*, in *BioLaw Journal*, 1/2024, p. 279 ss.

A. NATALE, *Introduzione. Una giustizia (im)prevedibile?*, in *Quest. giust.*, 4/2018, p. 1 ss.

A. NATALINI, *De minimis non curat praetor: diritto penale giurisprudenziale e reati di pericolo astratto, tra tipicità apparente, esiguità del fatto e necessaria offensività*, in *Cass. pen.*, 11/2003, p. 3532 ss.

G. NEPPI MODONA, *Il lungo cammino del principio di offensività*, in *Studi in onore di Marcello Gallo*, Giappichelli, Torino 2004, p. 89 ss.

A. NICITA, *Libertà d'espressione e pluralismo 2.0: i nuovi dilemmi*, in *MediaLaws*, 1/2019, p. 314 ss.

N.J. NILSSON, *The Quest for Artificial Intelligence: A History of Ideas and Achievements*, Cambridge University Press, Cambridge, 2009.

M. NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di "data retention"*, in *Dir. Un. eur.*, 4/2014, p. 803 ss.

- *La disciplina internazionale ed europea della "data retention" dopo le sentenze "Privacy International" e "La Quadrature du Net" della Corte di giustizia UE*, in *Dir. Un. eur.*, 1/2021, p. 93 ss.

- *La normalizzazione della sorveglianza di massa nella prassi giurisprudenziale delle Corti di Strasburgo e Lussemburgo: verso il cambio di paradigma del rapporto "privacy v. security"*, in *Freedom, Security & Justice: European Legal Studies*, 3/2022, p. 105 ss.

- *The freedom of expression and hate speech in cyberspace*, in *Comun. intern.*, 1/2023, p. 33 ss.

M. NOCERA, *I reati nella circolazione stradale. Alla luce della giurisprudenza*, Dike giuridica, Roma, 2018.

T. NUMERICO, *Big date e algoritmi*, Carocci Editore, Roma, 2021.

M. NUZZO, *Il problema della prevedibilità delle decisioni: calcolo giuridico secondo i precedenti*, in A. Carleo (a cura di), *Calcolabilità giuridica*, Il Mulino, Bologna, 2017.

A. ODDENINO, *Decisioni algoritmiche e prospettive internazionali di valorizzazione dell'intervento umano*, in *DPCE online*, 1/2020, p. 199 ss.

A. ORSINA, *Rischio da incertezza scientifica e modelli di tutela penale*, Giappichelli, Torino, 2015.

A. ORTALDA, S. LEUCCI, *Identità digitale e protezione dei dati personali: punti di incontro e rischi nelle discipline eIDAS e RGPD*, in *Inf. dir.*, 1/2022, 2, p. 145 ss.

S. OTA, *Identification of IMO Regulations relating to Unmanned Operations of Maritime Autonomous Surface Ships – SOLAS Convention and Related Mandatory IMO instruments*, in *Papers of National Maritime Research Institute*, 17/2018, p. 227 ss.

A. PACE, *Nome, soggettività giuridica e identità personale*, in *Giur. cost.*, 1/1994, p. 103 ss.

- *Problematica delle libertà costituzionali. Parte generale*, CEDAM, Padova, 2003.

A. PACE, M. MANETTI, *La libertà di manifestazione del pensiero. Art. 21*, in G. Branca, A. Pizzorusso (a cura di), *Commentario della Costituzione*, XI, Zanichelli, Bologna, 2006.

T. PADOVANI, *Il grado della colpa*, in *Riv. it. dir. e proc. pen.*, 1969, p. 818 ss.

- *Diritto penale*, Giuffrè, Milano, 2008, p. 134 ss.

U. PAGALLO, *Saggio sui robot e il diritto penale*, in S. Vinciguerra, F. Dassano (a cura di), *Scritti in memoria di Giuliano Marini*, Edizioni Scientifiche Italiane, Napoli, 2010, p. 595 ss.

C. PAGELLA, *Responsabilità penale di un aspirante deputato per i commenti islamofobi pubblicati da terzi sulla sua pagina Facebook: la Corte EDU [Corte europea dei diritti dell'uomo] sui limiti alla libertà di manifestazione del pensiero*, in *Riv. it. dir. e proc. pen.*, 3/2023, p. 1243 ss.

A. PAGLIARO, *Limiti all'unificazione del diritto penale europeo*, in *Riv. trim. dir. pen. econ.*, 1-2/1993, p. 199 ss.

L. PALAMARA, *Note in tema di rilevanza penale del trattamento illecito di dati personali*, in *Cass. pen.*, 6/2005, p. 1898 ss.

F. PALAZZO, *Corso di diritto penale. Parte generale*, Giappichelli, Torino, 2011, p. 77 ss.

C. E. PALIERO, *La Società punita: del come, del perché e del per cosa*, in *Riv. it. dir. e proc. pen.*, 2008, p. 1516 ss.

V. PALLADINI, *"Data retention" e "privacy" in rete: verso una regolazione conforme al diritto UE?*, in *Rivista italiana di informatica e diritto*, 1/2022, 2, p. 103 ss.

A. PALMIERI, *Intelligenza artificiale ed operazioni di trattamento dei dati personali*, in *Foro it.*, 4/2023, 3, p. 210 ss.

A. PALUMBO, J. PIEMONTE, *Delega di funzioni regolamentari e lotta ai rischi sistemici causati dalla disinformazione nel "Digital Services Act": quali rischi per la libertà di espressione?*, in *MediaLaws*, 3/2023, p. 114 ss.

B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'automa artificiale*, in *Dir. inform.*, 2, 2021, p. 317 ss.

C. PANICALI, *Il "cyberbullismo": i nuovi strumenti (extrapenali) predisposti dalla legge n. 71/2017 e la tutela penale*, in *Resp. civ. prev.*, 6/2017, p. 2081 ss.

F. PAOLUCCI, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *MediaLaws*, 1/2021, p. 204 ss.

R. PASCARELLI, *La riforma dei reati di opinione: un commento alla nuova disciplina*, in *Ind. pen.*, 2/2006, p. 697 ss.

W. PAVIA, *Driverless Uber car 'not to blame' for woman's death*, in *The Times*, 21 marzo 2018.

C. PAVICH, M.V. STURLESE, *Reati stradali. Soluzioni applicative e interpretative*, Giappichelli, Torino, 2018.

E. PELLECCHIA, *Profilazione e decisioni automatizzate al tempo della "Black Box Society": qualità dei dati e leggibilità dell'algoritmo nella cornice della "responsible research and innovation"*, in *Nuove leg. civ. comm.*, 5/2018, p. 1209 ss.

M. PELISSERO, *Osservazioni critiche sulla legge in tema di reati di opinione: occasioni mancate e incoerenze sistematiche*, in *Dir. pen. e proc.*, 8/2006, p. 960 ss.

S. PELLEGATTA, *Smart cars and smart roads: the italian way for the new mobility test phase*, in *Riv. Dir. dell'Economia, dei Trasporti e dell'Ambiente*, 2022, p. 129 ss.

R. PELLICCIA, *Polizia predittiva: il futuro della prevenzione criminale?*, in *cyberlaws.it*, 9 maggio 2019.

E. PENCO, *Limiti-soglia e responsabilità colposa. Il ruolo incerto delle soglie quantitative, dalla colpa specifica al rischio consentito*, in *Riv. it. dir. e proc. pen.*, 1/2019, p. 195 ss.

B. PEREGO, *Predictive policing: trasparenza degli algoritmi, impatto sulla privacy e risvolti discriminatori*, in *BioLaw Journal*, 2/2020, p. 447 ss.

C. PERINI, *Il concetto di rischio nel diritto penale moderno*, Giuffrè, Milano, 2010.

- *La legislazione penale tra "diritto penale dell'evento" e "diritto penale del rischio"*, in *Leg. pen.*, 2012, p. 117 ss.

- *Adattamento e Differenziazione della Risposta Punitiva nella Società Del Rischio*, in G. Morgante, *Il diritto penale di fronte alle sfide della «Società del rischio». Un difficile rapporto tra nuove esigenze di tutela e classici equilibri di sistema*, Giappichelli, Torino, 2017, p. 455 ss.

S. PERON, *Diffamazione tramite mass-media*, CEDAM, Padova, 2006.

W.L. PERRY, B. MCINNIS, C.C. PRICE, S.C. SMITH, J.S. HOLLYWOOD, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, Rand, Santa Monica, 2013.

D. PETRINI, *Diffamazione "on line": offesa recata con "altro mezzo di pubblicità" o col mezzo della stampa?*, in *Dir. pen. e proc.*, 11/2017, p. 1485 ss.

V. PEZZELLA, *La diffamazione*, Utet Giuridica, Milano, 2016.

- *La diffamazione. Le nuove frontiere della responsabilità penale e civile e della tutela della privacy nell'epoca dei social, delle fake news e degli hate speeches*, Utet Giuridica, Milano, 2020.

D. PIANA, G. VICICONTE, *Considerazioni critiche sulla proposta regolativa europea in materia di intelligenza artificiale con attenzione ai profili attuativi*, in *Riv. C. conti*, 4/2022, 1, p. 7 ss.

L. PICARELLA, *Il "cybercrime" come nuova sfida definitoria al concetto di criminalità organizzata*, in *Studi sulla questione criminale*, 1/2024, p. 105 ss.

S. PICCININI, *Appunti sui diritti della personalità e sui c.d. nuovi diritti. Tutela e promozione della identità personale*, in *Dir. fam.*, 1/2021, 2, p. 227 ss.

F. PICCIONI, *L'omicidio stradale. Analisi ragionata della Legge 23 marzo 2016 n. 41*, Giappichelli, Torino, 2016.

L. PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in L. Picotti (a cura di), *Tutela penale della persona e nuove tecnologie*, CEDAM, Padova, 2013, p. 59 ss.

- *Profili di responsabilità penale per la circolazione di veicoli a guida autonoma*, in *Studi in onore di Antonio Fiorella*, Roma Tre-Press, Roma, 2021.

- *Intelligenza artificiale e diritto penale: le sfide ad alcune categorie tradizionali*, in *Dir. pen. e proc.*, 3/2024, p. 293 ss.

G. PIERACCINI, *La Costituzione e la rivoluzione informatica*, in *Rassegna Parlamentare*, 1/1997, p. 13 ss.

C. PIERGALLINI, *Danno da prodotto e responsabilità penale. Profili dommatici e politico-criminali*, Giuffrè, Milano, 2004.

- *Il paradigma della colpa nell'età del rischio: prove di resistenza del tipo*, in *Riv. it. dir. e proc. pen.*, 2005, p. 1695 ss.

- *La regola dell'"oltre ragionevole dubbio" al banco di prova di un ordinamento di civil law*, in *Riv. it. dir. e proc. pen.*, 2/2007, p. 593 ss.

- *Intelligenza artificiale: da "mezzo" ad "autore" del reato?*, in *Riv. it. dir. e proc. pen.*, 2020, p. 1746 ss.

E. PIETROCARLO, *"Predictive Policing": criticità e prospettive dei sistemi di identificazione dei potenziali criminali*, in *Dir. pen. cont.*, 2/2023, p. 114 ss.

S. PIETROPAOLI, *Un'occasione (forse) mancata. Considerazioni sulla revisione dei reati informatici proposta con il DDL Cybersicurezza*, in *Inf. dir.*, 1/2024, p. 47 ss.

C. PINELLI, *Poteri e diritti nelle piattaforme. Problemi di una prospettiva costituzionale*, in *Giur. it.*, 2/2024, p. 452 ss.

G. PINO, *Teorie e dottrine dei diritti della personalità. Uno studio di meta-giurisprudenza analitica*, in *Materiali per una storia della cultura giuridica*, 1/2003, p. 237 ss.

- *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, il Mulino, Bologna, 2003.

- *Teoria e pratica del bilanciamento: tra libertà di manifestazione del pensiero e tutela dell'identità personale*, in *Danno e resp.*, 6/2003, p. 577 ss.

- *L'identità personale*, in AA.VV., *Gli interessi protetti nella responsabilità civile*, vol. II, Utet, Torino, 2005, p. 367 ss.

A. PIOGGIA, *Il diritto alla salute alla prova della differenziazione: autonomie, organizzazione e diseguaglianza*, in *Istit. federalismo*, 1/2020, p. 37 ss.

R. PIROSA, *Tecniche biometriche e trattamento dei dati. Il caso "Clearview AI": l'avamposto di una rivoluzione pacifica*, in *Notizie di Politeia*, 151/2023, p. 95 ss.

P. PISA, *L'omicidio stradale nell'eclissi giurisprudenziale del dolo eventuale*, in *Dir. pen. e proc.*, 2016, p. 145 ss.

A. PISANI TEDESCO, *Rischi satellitari e informatici*, in D. Cerini, A. Pisani Tedesco (a cura di), *Smart mobility, smart cars e intelligenza artificiale*: *responsabilità e prospettive*, Giappichelli, Torino, 2019.

C. PISTILLI, *L'utilizzo dell'intelligenza artificiale nel campo delle attività investigative delle forze dell'ordine: tra prospettive di sviluppo ed esigenze di coordinamento,* in F. Basile, M. Caterini, S. Romano

(a cura di), *Il sistema penale ai confini delle hard sciences. Percorsi epistemologici tra neuroscienze e intelligenza artificiale*, Pacini Editore, Pisa, 2021, p. 148 ss.

D. PIVA, *Machina discere, (deinde) delinquere et puniri potest*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Giuffrè, Milano, 2022, p. 681 ss.

F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016.

V. PLANTAMURA, *La tutela penale dei dati personali*, in *Dir. inform.*, 2007, p. 649 ss.

P. F. POLI, *Attività medica in "équipe": c'è spazio per il principio di affidamento?*, in *Giur. it.*, 5/2021, p. 1204 ss.

S. POLLASTRELLI, R. ACQUAROLI, *Il reato di omicidio stradale*, Giuffrè, Milano, 2017.

O. POLLICINO, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in *Percorsi costituzionali*, 1/2014, p. 45 ss.

- *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, in *MediaLaws*, 1/2018, p. 3 ss.

M. POLVANI, *La diffamazione a mezzo stampa*, CEDAM, Padova, 1998.

A. PROVERA, *Responsabilità medica svolta in èquipe*, in *Riv. it. med. leg.*, 3/2011, p. 822 ss.

D. PROVOLO, *Il sistema sanzionatorio del novellato Codice della "privacy" e la tutela penale "patchwork" dei dati genetici e dei dati biometrici*, in *Riv. trim. dir. pen. econ.*, 1-2/2019, p. 242 ss.

S. PUDDU, *Diritto all'istruzione e contrasto alle diseguaglianze: profili amministrativistici e spunti dall'agenda 2030*, in *Dir. e proc. amm.*, 1/2024, p. 181 ss.

L. M. PUENTE ABA, *Criminal product liability, causal link and big data: a first approach - Responsabilità penale per il prodotto, causalità e dati massivi: una prima approssimazione*, in *Studi sulla questione criminale*, 3/2023, p. 41 ss.

S. PUGNO, *Accertamento del nesso di causalità e colpa specifica nella circolazione stradale*, in *Giur. it.*, 12/2003, p. 2254 ss.

D. PULITANÒ, *Il diritto penale fra vincoli di realtà e sapere scientifico*, in *Riv. it. dir. e proc. pen.*, 2006, p. 821 ss.

- *Gestione del rischio da esposizioni professionali*, in *Cass. pen.*, 2/2006, p. 787 ss.

- *Colpa ed evoluzione del sapere scientifico*, in *Dir. pen. e proc.*, 5/2008, p. 652 Ss.

A. PUNZI, *Il dialogo delle intelligenze tra umanesimo e tecnoscienza*, in Persona e Mercato, 2/2023, p. 161 ss.

S. QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *Leg. pen.*, 18 dicembre 2018.

- *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"*, in *Cass. pen.*, 4/2019, p. 1748 ss.

F.A. QUERCI, *La figura giuridica del comandante di nave e aeromobile*, Giuffrè, Milano, 1964.

S. QUINTARELLI, *Forum AI and Law*, in *BioLaw Journal*, 1/2020, p. 493 ss.

E. C. RAFFIOTTA, *Dalla "self-regulation" alla "over-regulation" in ambito digitale: come (e perché) di un necessario cambio di prospettiva*, in *Osservatorio sulle fonti*, 2/2023, p. 245 ss.

A. RANGHINO, *Diffamazione e "social network": l'attribuzione del "post" all'imputato tra prova logica e prova diretta*, in *MediaLaws*, 3/2023, p. 200 ss.

F. RATTO TRABUCCO, *L'"hate speech" nell'esperienza dei "social networks" e della giurisprudenza americana*, in *Rivista della Cooperazione Giuridica Internazionale*, 57/2017, pp. 85 ss.

C. M. REALE, M. TOMASI, *Libertà d'espressione, nuovi media e intelligenza artificiale: la ricerca di un nuovo equilibrio nell'ecosistema costituzionale*, in *DPCE online*, 1/2022, p. 325 ss.

N. RECCHIA, *Il principio di proporzionalità nel diritto penale. Scelte di criminalizzazione e ingerenza nei diritti fondamentali*, Giappichelli, Torino, 2020.

A. REGINA, *Colpa ed evento. Note a margine di Cass., Sez. IV, 17 maggio 2006 (caso Marghera)*, in S. Vinciguerra, F. Dassano (a cura di), *Scritti in memoria di Giuliano Marini*, 2010, p. 728 ss.

P. RESCIGNO, *I diritti della personalità e la loro rilevanza costituzionale (a proposito di un recente libro)*, in *Dir. inf.*, 2/1986, p. 333 ss.

G. RESTA, *Diritti della personalità: problemi e prospettive*, in *Dir. inf.*, 6/2007, p. 1043 ss.

G. RIGHETTI, *Trattato di diritto marittimo*, Giuffrè, Milano, 1987, p. 913 ss.

S. RIONDATO, *Competenza penale della Comunità europea. Problemi di attribuzione attraverso la giurisprudenza*, CEDAM, Padova, 1996.

- *Robotica e diritto penale (robot, ibridi, chimere, "animali tecnologici")*, in D. Provolo, S. Riondato, F. Yenisey (a cura di), *Genetics, Robotics, Law, Punishment*, Padova University Press, 2014, p. 600 ss.

- *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 ss.

L. RISICATO, *Linee guida e colpa "non lieve" del medico. Il caso delle attività di équipe*, in *Giur. it.*, 8-9/2014, p. 2065 ss.

G. ROCCHI, *L'interruzione del nesso causale tra condotta ed evento e la posizione di garanzia del capo dell'"équipe" chirurgica*, in *Cass. pen.;* 3/2016, p. 907 ss.

S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna, 1973.

- *La "privacy" tra individuo e collettività*, in *Pol. dir.*, 1974, p. 545 ss.

- *Il mondo nella rete. Quali i diritti, quali i vincoli*, Editori Laterza, Bari, 2014.

A. ROIATI, *L'introduzione dell'omicidio stradale e l'inarrestabile ascesa del diritto penale della differenziazione*, in *Dir. Pen. Cont.*, 1 giugno 2016, p. 3 ss.

B. ROMANO, *In the Era of AI. Exploring New Frontiers in Cybercrime and Safeguarding Personal and Health Data*, in *Corti Supreme e Salute*, 1/2024, p. 461 ss.

M. S. ROMANO, *Danni punitivi ed eccesso di deterrenza: gli (incerti) argini costituzionali*, in *Foro it.*, 4/1990, 4, p. 175 ss.

L. ROMANÒ, *La responsabilità penale al tempo di ChatGPT: prospettive de iure condendo in tema di gestione del rischio da intelligenza artificiale generativa*, in *Dir. pen. cont.*, 1/2023, p. 70 ss.

A. ROMEO, *"Bad Man" e "Puzzled Man" davanti ad un "chatbot". Il bisogno di accesso cognitivo al diritto e le promesse dell'intelligenza artificiale*, in *dirittifondamentali.it*, 1/2024, p. 22 ss.

- *L'era degli algoritmi e la sua incidenza nell'ambito della certezza del diritto: un connubio sospetto*, in *Lav. giur.*, 1/2024, p. 5 ss.

C. ROSSANO, *L'eguaglianza giuridica nell'ordinamento costituzionale*, Jovene, Napoli, 1966.

B. ROSSI, *La responsabilità del capo dell'equipe medico-chirurgica*, in *Cass. pen.*, 11/2019, p. 3980 ss.

L. ROSSI, *Dall'uso all'abuso: quando la libertà di espressione sconfina nel negazionismo*, in *Riv. it. dir. e proc. pen.*, 1/2020, p. 369 ss.

S. ROSSI, *Il diritto alla salute tra equità e sostenibilità. Colloquio sulle forme dell'eguaglianza in sanità*, in *BioLaw Journal*, 2/2019, p. 7 ss.

- *Il sistema penale della navigazione. Contributo allo studio del diritto penale marittimo*, Editoriale Scientifica, Napoli, 2020.

C. RUGA RIVA, *Principio di precauzione e diritto penale. Genesi e contenuto della colpa in contesti di incertezza scientifica*, in E. Dolcini, C.E. Paliero (a cura di), *Studi in onore di Giorgio Marinucci*, Giuffrè, Milano, 2006.

U. RUFFOLO, *Self driving cars, Auto driverless e responsabilità*, in U. Ruffolo (a cura di), *Intelligenza artificiale e responsabilità*, Giuffrè, Milano, 2017, p. 49 ss.

- *Intelligenza Artificiale, "machine learning" e responsabilità da algoritmo*, in *Giur. it.*, 7/2019, p. 1689 ss.

- *Piattaforme, A.I. generativa e libertà di (formazione e) manifestazione del pensiero. Il caso ChatGPT*, in *Giur. it.*, 2/2024, p. 472 ss.

- *Piattaforme e "content moderation" negoziale*, in *Giur. it.*, 2/2024, p. 442 ss.

E. RULLI, *Giustizia predittiva, intelligenza artificiale e modelli probabilistici. Chi ha paura degli algoritmi?*, in *Analisi giuridica dell'economia*, 2018, p. 533 ss.

S. RUSSELL, P. NORVIG, *Artificial Intelligence: A Modern Approach*, Pearson, Londra, 2014.

E. SACCHETTO, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *Leg. pen.*, 16 ottobre 2020.

G. SALCUNI, *Culture penalistiche a confronto: diritto penale nazionale vs diritto penale europeo*, in *Arch. pen.*, 2/2011, p. 445 ss.

- *L'europeizzazione del diritto penale: problemi e prospettive*, Giuffrè, Milano, 2011

A. M. SALERNO, *Responsabilità medica "in équipe": cooperazione colposa, posizione di garanzia degli organi apicali e principio di auto-responsabilità dei singoli cooperanti*, in *Riv. it. med. leg.*, 2/2014, p. 595 ss.

M. SALTORI, *Come decide un'auto senza pilota chi muore in un incidente stradale*, *online* sul sito *web* www.thevision.com.

I. SALVADORI, *Il trattamento senza consenso di dati personali altrui reperibili su Internet costituisce reato?*, in *Dir. pen. e proc.*, 4/2006, p. 467 ss.

- *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Riv. it. dir. e proc. pen.*, 1/2021, p. 83 ss.

P. SAMMARCO, *Osservazioni sulla responsabilità da informazioni inesatte fornite da un "chatbot"*, in *Dir. inform.*, 1/2024, p. 133 ss.

A. SANTOSUOSSO, G. SARTOR, *La giustizia predittiva: una visione realistica*, in *Giur. it.*, 7/2022, p. 1760 ss.

L. SAPONARO, *Il dubbio ragionevole alla ricerca di una definizione*, in *Giur. it.*, 2/2018, p. 469 ss.

G. SCACCIA, *Gli "strumenti" della ragionevolezza nel giudizio costituzionale*, Giuffrè, Milano 2000.

L. SCAFFARDI, *"Data retention" e diritti della persona*, in *Costituzionalismo.it*, 2/2017, p. 55 ss.

A. SCIORTINO, *"Fake news" e "post"-verità nella società dell'algoritmo*, in *dirittifondamentali.it*, 2/2021, p. 422 ss.

E. SELVAGGI, *Sulla libertà di espressione*, in *Cass. pen.*, 1/2013, p. 342 ss.

A. P. SEMINARA, *"Marketing" d'influenza e pubblicità non trasparente: la responsabilità dell'inserzionista, degli "influencer" e dell'"internet service provider"*, in *Persona e Mercato*, 3/2023, p. 548 ss.

M. A. SENOR, *Un primo commento alla legge sul cyberbullismo*, in *MediaLaws*, 1/2017, p. 23 ss.

P. SEVERINO, *Intelligenza artificiale e diritto penale*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020, p. 533 ss.

C. SEVERONI, *Prime considerazioni su un possibile inquadramento giuridico e sul regime di responsabilità nella conduzione dei veicoli a guida autonoma*, in *Dir. trasp.*, 2018, p. 331 ss.

- *Soccorso e mezzi di trasporto autonomi,* in *Dir. trasp.* 2018, p. 72 ss.

M. SHIOKARI, S. OTA, *Considerations on the Regulatory Issues for realization of Maritime Autonomous Surface Ships*, in *J. Physics: Conference Series*, 2019, p. 1 ss.

F. SICCARDI, *Le navi autonome. Maritime Autonomous Surface Ships (MASS)*, in *Dir. mar.*, 2019, p. 848 ss.

A. SIGNORELLI, *La prevedibilità delle e nella decisione giudiziaria*, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, E M. Proto (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Giuffrè, Milano, 2022, p. 997 ss.

A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1/2019, p. 69 ss.

R. SIMONE, *La responsabilità civile non è solo compensazione: "punitive damages" e deterrenza*, in *Foro it.*, 9/2017, 1, p. 2644 ss.

B. SIRGIOVANNI, *Informed Consent to Processing of Genetic Data*, in *The Italian Law Journal*, 2/2022, p. 955 ss.

V. SMITH, *Rationality in economics: constructivist and ecological forms*, Leiden, 2007.

G. SMORTO, *Distribuzione del rischio e tutela dei diritti nel regolamento europeo sull'intelligenza artificiale. Una riflessione critica*, in *Foro it.*, 5/2024, 5, p. 208 ss.

M. SOLINAS, *Tutela penale della privacy dopo il GDPR: la frettolosa giustapposizione delle fonti è scaturigine di un sistema farraginoso, che crea confusione*, in *Resp. civ. prev.*, 2/2020, p. 663 ss.

M. SOMALVICO, *L'intelligenza artificiale*, Hewlett-Packard, Milano, 1987.

E. SOMMA, *"Oltre ogni ragionevole dubbio". Una formula enfatica da contestualizzare: meglio, da evitare*, in *Riv. it. dir. e proc. pen.*, 1/2014, p. 366 ss.

C. SOTIS, *Il diritto senza codice. Uno studio sul sistema penale europeo vigente*, Giuffrè, Milano, 2007.

A. SPANGARO, *Il concetto di profilazione tra "direttiva madre" e GDPR*, in *Giur. it.*, 7/2022, p. 1579 ss.

A. F. SPAGNUOLO, E. SORRENTINO, *Alcune riflessioni in materia di trasformazione digitale come misura di semplificazione*, in *federalismi.it*, 8/2021, p. 275 ss.

E. SPASIANO, *Comandante della nave o dell'aeromobile*, in *Enc. dir. VII*, 1960, 688 ss.

A. SPENA, *Libertà di espressione e reati di opinione*, in *Riv. it. dir. e proc. pen.*, 2-3/2007, p. 689 ss.

E. SQUILLACI, *Ombre e (poche) luci nella introduzione dei reati di omicidio e le personali lesioni stradali*, in *Dir. Pen. Cont.*, 18 aprile 2016.

G. STAMPANONI BASSI, *Sostituzione di persona commessa nella rete Internet*, in *Cass. pen.*, 1/2014, p. 146 ss.

P. STANCATI, *Il diritto fondamentale comunitario alla libera manifestazione del pensiero: profili critici e ricostruttivi*, in *Politica del diritto*, 2/2005, p. 171 ss.

- *Lineamenti evolutivi della libertà di manifestazione del pensiero e della informazione: rivoluzione mediatica, "buona" e "cattiva" televisione, multiculturalismo, fenomenologia terroristica*, in *Dir. soc.*, 3/2005, p. 313 ss.

C. STARCK, *L'applicazione del principio di uguaglianza*, in *Dir. soc.*. 2/1985, p. 237 ss.

S. STEFANIZZI, *Riflessioni metodologiche sul concetto e sull'uso dei Big Data*, in S. Gozzo, C. Pennisi, V. Asero, R. Sampugnaro (a cura di), *Big Data e processi decisionali*, Egea, Milano, 2020, p. 17 ss.

A. STIANO, *Ancora sul bilanciamento tra la tutela del diritto alla privacy e l'utilizzo di strumenti di sorveglianza di massa: tra garanzie procedurali e sostanziali*, in *Riv. dir. int.*, 3/2021, p. 904 ss.

S. STIEGLITZ, B. ROSS, A.K. JUNG, *Do social bots dream of electric sheep? A categorisation of social media bot accounts*, in *Proceedings of the 28th Australasian Conference on Information Systems (ACIS)*, 2017, p. 89 ss.

L. STORTONI, *L'incostituzionalità dei reati di opinione: una questione liquidata?*, in *Foro it.*, 4/1979, 1, p. 899 ss.

- *Angoscia tecnologica ed esorcismo penale*, in *Riv. it. dir. e proc. pen.*, 1/2004, p. 83.

A. STRACUZZI, *Data retention: il faticoso percorso dell'art. 132 Codice Privacy nella disciplina della conservazione dei dati di traffico*, in *Dir. inform.*, 4-5/2008, p. 585 ss.

A. STRINGI, G. DIOGUARDI, V. CARETTI, *"Problematic internet use" (piu) e cyberbullismo in adolescenza. Vittimizzazione, condotte a rischio e percezione del fenomeno tra pari: una ricerca*, in *Rass. it. crim.*, 4/2022, p. 290 ss.

G. SUFFIA, A. LAVORGNA, S. ICARDI, *Polizia "smart" tra paure e realtà: un'analisi esplorativa sulla rappresentazione mediatica dello "smart policing" in Italia*, in *Studi sulla questione criminale*, 3/2022, p. 95 ss.

C. SUNSTEIN, *Il diritto della paura. Oltre il principio di precauzione*, Il Mulino, Bologna, 2010.

- *Nudging: a very short guide*, in *Journal of consumer policy*, 37/2014, p. 583 ss.

H. SURDEN, *Machine Learning and Law*, in *Washington Law Review*, 2014, p. 87 ss.

G. TADDEI ELMI, F. ROMANO, *Il robot tra ius condendum e ius conditum*, in *Inf. dir.,* 2016, p. 115 ss.

M. L. TAMPONI, *In tema di diffamazione a mezzo stampa*, in *Giur. it.*, 11/2006, p. 2145 ss.

A. TEDESCHI TOSCHI, *Il reato di sostituzione di persona "online" di fronte a "socialbot" e ritratti "AI-generated" ["Artificial Intelligence" - Intelligenza Artificiale]. In favore di una interpretazione estensiva dell'art. 494 del codice penale*, in *MediaLaws*, 3/2023, p. 90 ss.

A. TEDESCHI TOSCHI, G. BERNI FERRETTI, *Social media, profili artificiali e tutela della reputazione. Come l'avvento dei social bot per la gestione dei profili social possa rappresentare una grave minaccia per la reputazione delle persone e quali potrebbero essere le risposte a tale pericolo*, in *Inf. dir.*, 3/2021, p. 107 ss.

- *La responsabilità per la diffamazione compiuta da un'Intelligenza artificiale. Possibili scenari costruiti partendo dall'esempio dell'IA Tay*, in *Ciberspazio e diritto*, 2023, p. 173 ss.

- *Il contrasto legislativo ai "socialbot". Alcuni spunti per una riforma in Italia*, in *Inf. dir.*, 1/2023, p. 155 ss.

C. TELESCA, *«Driverless Cars»: profili di responsabilità civile e penale*, in *Riv. Dir. Nav.*, 2019, p. 183 ss.

C.G. TERRANOVA, *Responsabilità da circolazione di veicoli*, in *Dig. disc. priv.*, XVII, Torino, 1998, p. 90 ss.

A. TESAURO, *La diffamazione come reato debole e incerto*, Giappichelli, Torino, 2005.

R. THALER, C. SUNSTEIN, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Penguin Books, Londra, 2008.

S. THOBANI, *Percorsi giurisprudenziali in tema di accertamento dell'elemento soggettivo della P.A.: colpa generica e colpa specifica*, in *Giur. it.*, 1/2013, p. 189 ss.

- *Richieste preventive di consenso al trattamento dei dati: quando la cautela rischia di essere eccessiva*, in *Dir. inform.*, 3/2020, p. 499 ss.

E. THOMAS, *Why Oakland Police Turned Down Predictive Policing*, in *vice.com*, 28 dicembre 2016.

G. TIBERI, *Il caso "Tele2 Sverige/Watson": una "iconica" sentenza della Corte di Giustizia nella saga sulla "data retention"*, in *Quad. cost.*, 2/2017, p. 434 ss.

R. TITOMANLIO, *Il principio di precauzione fra ordinamento europeo e ordinamento italiano*, Giappichelli, Torino, 2018.

S. TOGNAZZI, *Il diritto di difesa e l'accesso alle intercettazioni in fase cautelare*, in *Foro it.*, 3/2024, 2, p. 124 ss.

M. TOMASI, *La Corte EDU torna sui caratteri del discorso politico online: una diluizione della libera manifestazione del pensiero?*, in *DPCE online*, 1/2024, p. 741 ss.

S. TOMMASI, *"Digital services act" e "artificial intelligence act": tentativi di futuro da armonizzare*, in *Persona e Mercato*, 2/2023, p. 279 ss.

G. TORALDO, *Un difficile bilanciamento tra la conservazione dei dati per fini di sicurezza e il diritto all'oblio del condannato (riabilitato)*, in *DPCE online*, 1/2024, p. 617 ss.

G. TORCHIANI, *Auto a guida autonoma: cosa sono e come funzionano*, 18 maggio 2021, sul sito *web* www.ai4business.it.

F. TORRE, *"Data retention": una ventata di "ragionevolezza" da Lussemburgo (a margine della sentenza della Corte di giustizia 2 marzo 2021, C-746/18)*, in *Consulta online*, 2/2021, p. 615 ss.

M. TORRE, *Considerazioni su perquisizione, sequestro e intercettazioni digitali*, in *Dir. pen. e proc.*, 6/2024, p. 811 ss.

E. TOSI, *Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo*, in *Contr. impr.*, 3/2020, p. 1115 ss.

R. TRANQUILLI LEALI, *Lineamenti della comunità viaggiante nel diritto della navigazione*, Pacini Editore, Roma, 1982.

- *La tutela della sicurezza dei passeggeri nel trasporto marittimo tra comandante della nave e pilota da remoto*, in *Dir. trasp.* 2019, p. 471 ss.

F. TRAPELLA, *La rivoluzione digitale alla prova della riforma*, in *Arch. pen.*, 3/2022, p. 999 ss.

P. TRAVERSO, *Breve introduzione tecnica all'Intelligenza Artificiale*, in *DPCE online*, 1/2022, p. 155 ss.

C. TREVISI, *La regolamentazione in materia di Intelligenza artificiale, robot, automazione: a che punto siamo*, in *Medialaws*, 21 maggio 2018.

E. TROISI, *Decisione algoritmica, "Black-Box" e AI etica: il diritto di accesso come diritto a ottenere una spiegazione*, in *Jus civile*, 4/2022, p. 953 ss.

F. TRONCONE, *Il delitto di naufragio colposo: una fattispecie di nuovo attuale*, in *Studi Marittimi*, 1996, p. 46 ss.

P. TRONCONE, *Profili penali del codice della privacy*, in *Riv. pen.*, 12/2004, p. 1147 ss.

- *La tutela penale della riservatezza e dei dati personali. Profili dommatici e nuovi approdi normativi*, Edizioni Scientifiche Italiane, Napoli, 2020.

- *Nuove possibili scelte di politica criminale per il reato di pubblicazione o diffusione di notizie false ("fake news"), esagerate o tendenziose*, in *Ind. pen.*, 2/2021, p. 614 ss.

L. TRUCCO, *"Data retention": la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. it.*, 8-9/2014, p. 1850 ss.

L. TULLIO, *L'obbligazione di protezione nel trasporto marittimo ed aereo*, in *Dir. trasp.*, 2013, p. 349 ss.

A. M. TURING, *Computing machinery and intelligence*, in *Mind – A Quarterly Review of Psychology and Philosophy*, LIX, 236, 1950, p. 433 ss.

G, TUZET, *Libero convincimento e ragionevole dubbio secondo Gaetano Carlizzi*, in *Diritto & questioni pubbliche*, 2/2019, p. 13 ss.

G. UBERTIS, *Processo penale telematico, intelligenza artificiale e costituzione - telematic criminal proceedings, artificial intelligence and the constitution*, in *Cass. pen.*, 2/2024, p. 439 ss.

C. VALDITARA, *"Private" e "public enforcement" nel contrasto alle "fake news"*, in *Dir. inform.*, 3/2021, p. 493 ss.

A. VALSECCHI, *Il nuovo volto della discrezionalità giudiziaria: prospettive e pericoli a partire dalla giurisprudenza americana sui "risk assessment tools" impiegati nel "sentencing"*, in *federalismi.it*, 17/2023, p. 303 ss.

E. VARANI, *Diritto alla privacy e trattamento dei dati sensibili in ambito sanitario: dalla Carta dei diritti fondamentali dell'Unione Europea al D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"*, in *Giur. it.*, 8-9/2005, p. 1769 ss.

R.VEAL, H. RINGBOM, *Unmanned ships and the international regulatory framework*, in *Journal of International Maritime Law*, 2017, p. 100 ss.

R. VEAL, M. TSINPLIS, *The navigation of Unmanned ships into the lex maritima,* in *LMLQ*, 2017, p. 303 ss.

R. VEAL, M. TSIMPLIS, A. SERDY, S. QUINN, A. NTOVAS, *Liability for Operation in Unmanned Maritime Vehicles with Differing Levels of Autonomy*, Institute of Maritime Law, Brussels, 2016.

G. VECCHIO, *Riflessioni sullo stato della libertà di espressione nell'attuale contesto informativo*, in *dirittifondamentali.it*, 3/2023, p. 14 ss.

A. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto. La "data retention" al test di legittimità*, in *Dir. pubbl. comp. eur.*, 3/2014, p. 1224 ss.

P. VELTEN, *Diritto penale europeo*, in *Criminalia*, 2006, p. 125 ss.

P. VENEZIANI, *Regole cautelari "proprie" ed "improprie" nella prospettiva delle fattispecie colpose causalmente orientate*, CEDAM, Padova, 2003.

F. VERDE, *Diffamazione a mezzo stampa e l'esimente dell'esercizio del diritto*, Cacucci, Bari, 2009.

G. VERMIGLIO, *La nave e l'aeromobile*, in L. Tullio, M. Deiana (a cura di), *Il cinquantenario del Codice della navigazione*, ISDIT, Cagliari, 1993, p. 114 ss.

F. VIGANÒ, *Un'importante pronuncia della Consulta sulla proporzionalità della pena*, in *Dir. pen. cont.*, 14 novembre 2016.

- *La proporzionalità della pena. Profili di diritto penale e costituzionale*, Giappichelli, Torino, 2021.

I. VINGIANO-VIRICEL, *Véhicule autonome: qui est responsable?, Impacts de la délégation de conduite sur les régimes de responsabilité*, LexisNexis, New York, 2019.

A. VISCONTI, *Onore, reputazione e diritto penale*, EDUCatt, Milano, 2011.

- *Alcune considerazioni criminologiche e politico-criminali sulle c.d. "Fake News"*, in *Jus*, 1/2020, p. 43 ss.

B. VLASIC, N.E. BOUDETTE, *Self-Driving Tesla Was Involved in Fatal Crash, U.S. Says*, in *The New York Times*, 30 giugno 2016.

D. WAKABAYASHI, *Self-Driving Uber Car Kills Pedestrian in Arizona, Where Robots Roam*, in *The New York Times*, 19 marzo 2018.

J. WEIZENBAUM, *ELIZA – a computer program for the study of natural language communication between man and machine,* Massachussets Istitute of Technology, Cambridge, Mass, 1966.

M. A. WÓJCIK-SUFFIA, *Algorithmic Discrimination in M-Health: Rethinking the US Nondiscrimination Legal Framework Through the Lens of Intersectionality*, in *BioLaw Journal*, 1/2024, p. 367 ss.

E. XINLAN, *137 Questions: Criminal Risk Assessment Algorithms as a Case Study for Data Ethics*, in *Stanford Rewired*, 2020, consultabile sul sito *web* https://stanfordrewired.com/post/137-questions.

G. ZACCARIA, *Figure del giudicare: calcolabilità, precedenti, decisione robotica*, in *Riv. dir. civ.*, 2/2020, p. 277 ss.

A. ZACCHIA, *L'individuazione della regola cautelare non scritta in tema di colpa generica*, in *Cass. pen.*, 6/2014, p. 2114 ss.

P. ZAMPELLA, *Navi autonome e navi pilotate da remoto, spunti per una riflessione*, in *Dir. trasp.* 2019, p. 588 ss.

L. ZAPPALÀ, *Transparency and Comprehensibility of Working Conditions and Automated Decisions: Is It Possible to Open the Black Box?*, in *The Italian Law Journal*, 2/2023, p. 623 ss.

G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, Milano, 2015.

- *Diritti digitali. Informatica giuridica per le nuove professioni*, Raffaello Cortina Editore, Milano, 2022.

M. ZINCANI, *Reati di pericolo*, in F. Giunta (a cura di), *Diritto penale*, Giuffrè, Milano, 2008, p. 202 ss.

S. ZUNARELLI, M. M. COMENALE PINTO, *Manuale di diritto della navigazione e dei trasporti. Vol. I*, CEDAM, Padova, 2023.

S. ZUNARELLI, A. ROMAGNOLI, *Contratto di trasporto marittimo di persone*, Giuffrè, Milano, 2012, p. 110 ss.