





Università degli studi di Napoli Federico II

**Innovazione e Diritto** - Rivista trimestrale on line fondata nel 2005 dal prof. Raffaele Perrone Capano, autore e responsabile scientifico del Progetto di informatizzazione diffusa della Facoltà di Giurisprudenza, e di catalogazione in formato digitale della Biblioteca storica, a supporto della ricerca e della didattica.

Il Progetto, approvato dal MIUR nel 2004, per un importo complessivo di 1.350.00 €, era stato finanziato per il 70% dall'UE, per il 26% dalla Facoltà, attraverso il riconoscimento delle spese effettuate nel settore informatico nel biennio precedente, e per il restante 4% dal MIUR.

Innovazione e Diritto è stata, fin dalla nascita, una rivista ad accesso libero, a supporto delle attività dei dottorati di ricerca e dei giovani studiosi della Facoltà. L'adesione di numerosi colleghi, professori e ricercatori di altre Università italiane, ne ha consolidato in breve tempo la dimensione nazionale.

Dal 2012, in seguito alla trasformazione delle Facoltà in Dipartimenti, la Rivista ha proseguito l'attività, per l'impegno di un gruppo di professori e ricercatori di numerose Università italiane che hanno assicurato il regolare flusso di contributi scientifici di elevata qualità. Il nuovo assetto editoriale ha favorito l'estensione degli interessi scientifici della Rivista ai settori più direttamente investiti dalla crisi finanziaria del 2008, la più grave dal dopoguerra. L'orizzonte più ampio ha comportato una parallela specializzazione della produzione scientifica, e ne ha amplificato la diffusione e l'impatto.

Un primo punto di svolta ha preso avvio all'inizio del 2018, con la scelta della cadenza trimestrale, per lasciare spazio alla pubblicazione di numeri speciali, di Atti di convegno e di altre iniziative promosse dalla Rivista, affiancata dall'indicazione nel sottotitolo di: "Rivista di Diritto tributario e dell'Economia". Un secondo punto si è concretizzato in una nuova partenza, basata su una piattaforma digitale avanzata, coerente con le indicazioni dell'ANVUR per le riviste di classe A e con gli standard definiti da Google per la massima diffusione internazionale dei contenuti.

# Legal reasoning in the age of artificial intelligence

di **Emanuela Di Rauso**

*Dottoranda di ricerca in Imprenditorialità e Innovazione -  
Dipartimento di Economia - Università degli Studi della Campania  
"Luigi Vanvitelli"*

## **ABSTRACT**

The use of artificial intelligence now influences every aspect of individual and collective life and is rapidly changing not only the economic sphere, but also the political and social sphere, without, however, being able to hypothesize with certainty the outcomes. In the face of such overwhelming progress, legal thinking is still lagging far behind. The legislator struggles to follow changing and elusive cases and it is not clear which interpretative and applicative tools can be used by jurists. This paper proposes to fill the gap, stimulating a path of reflection that places law and its foundations at the center of the investigation. The aim is to explore – and, if possible, understand – how the use of intelligent machines and programs can influence the development and completion of legal reasoning.

Artificial intelligence is the key to enter a new world, which is not necessarily the dystopian world of literature or science fiction cinema, but which will certainly be characterized by impressive transformative processes, affecting politics, economics, personal relationships, professional training and education, justice, health, just to mention the most important spill-over points of artificial intelligence developments.

In the face of these transformations and major changes, law must adapt its responses, and in some cases must imagine entirely new responses. The interest of law in artificial intelligence finds an almost

"natural" justification. Law is, in a realist perspective, a product of social forces, the reflection of needs and problems of contemporary social life; therefore, artificial intelligence is now, and will increasingly be, an essential element in people's lives, in the system of social relations. It is a matter of finding a synthesis between technological innovation and the principles that must guide the work of the jurist, in order to ensure an adequate protection of rights.

## **SINTESI**

*L'impiego dell'intelligenza artificiale influenza ormai ogni aspetto della vita individuale e collettiva e sta mutando con rapidità non solo l'ambito dell'economia, ma anche quello politico e sociale, senza che peraltro si possano ipotizzarne con certezza gli esiti. A fronte di tale travolgente progresso, la riflessione giuridica è ancora in forte ritardo. Il legislatore fatica a inseguire fattispecie mutevoli e sfuggenti e non è chiaro quali strumenti interpretativi ed applicativi possano essere in concreto adoperati dai giuristi. Questo lavoro propone per l'appunto di colmare la lacuna, stimolando un percorso di riflessione che ponga nuovamente al centro dell'investigazione il diritto ed i suoi fondamenti. L'obiettivo è quello di esplorare - e se possibile comprendere - come l'uso di macchine e programmi intelligenti possa influenzare lo sviluppo ed il compimento del ragionamento giuridico.*

*L'intelligenza artificiale è la chiave di ingresso in un mondo nuovo, che non è per forza di cose il mondo distopico della letteratura o del cinema di fantascienza, ma che certamente sarà caratterizzato da processi trasformativi imponenti, che riguardano la politica, l'economia, le relazioni personali, la formazione professionale e l'istruzione, la giustizia, la salute, solo per citare i punti di ricaduta più importanti degli sviluppi dell'intelligenza artificiale.*

*Di fronte a queste trasformazioni e ai grandi cambiamenti il diritto deve adeguare le sue risposte, e in alcuni casi deve immaginare risposte completamente nuove. L'interesse del diritto per l'intelligenza artificiale trova una giustificazione quasi "naturale". Il diritto è, in una prospettiva realista, un prodotto di forze sociali, il riflesso di esigenze e problemi della vita sociale contemporanea; l'intelligenza artificiale quindi è ormai, e sempre più lo sarà, un elemento essenziale nella vita delle persone, nel sistema di relazioni sociali. Si tratta di trovare una sintesi tra l'innovazione tecnologica ed i principi che devono guidare l'attività del giurista, al fine di garantire comunque una adeguata tutela dei diritti.*

## **SOMMARIO**

**1.** Metodologia, criterio di ricerca, fonti e domanda di ricerca  
**1.1.** Introduzione  
**1.2.** Studio della Privacy nell'ambito dell'Artificial Intelligence  
**1.3.** Intelligenza artificiale: implicazioni etiche in materia di Privacy e Diritto penale  
**1.4.** L'intelligenza artificiale e il Law Enforcement - **2.** La decisione giudiziale e gli Automated Decision Systems - **2.1.** Gli strumenti di Intelligenza artificiale che "commettono reati" - **2.2.** Come è possibile adattare i principi fondamentali del costituzionalismo con l'uso diffuso dell'Intelligenza artificiale? - **2.3.** Come si sta evolvendo la legislazione internazionale in tema di intelligenza artificiale? - **2.4.** Quale utilizzo è possibile dell'intelligenza artificiale nella giustizia? - **3.** Risultati di ricerca e conclusioni

## **1. Metodologia, criterio di ricerca, fonti e domanda di ricerca**

La metodologia utilizzata per il seguente lavoro è la revisione sistemica della letteratura, prendendo in considerazione le fonti dall'anno 2020 ad oggi. Le banche date utilizzate sono: Juris, Researchgate, Scopus, Google Scholar. Inoltre, sono state prese in considerazione molti testi presenti presso la biblioteca dell'Università degli Studi della Campania "Luigi Vanvitelli". Le parole chiave di ricerca sono state: Intelligenza artificiale - Innovazione tecnologica - Digitalizzazione - Tutela del diritto - Privacy.

La revisione sistemica della letteratura è stata svolta in questo modo:

- 1) Raccolta degli articoli attraverso le banche dati;
- 2) Attenta analisi degli articoli;
- 3) Messa in evidenza tutte le componenti che forniscono una panoramica chiara per poter rispondere in modo esaustivo alle domande di ricerca poste nel corso del seguente lavoro. Le domande di ricerca poste sono le seguenti:

- 1) In che modo l'intelligenza artificiale può aiutare il legislatore nei casi in cui vi siano lacune nell'ordinamento giuridico?

- 2) Perché i giuristi dovrebbero fare affidamento all'intelligenza artificiale nel prendere decisioni?

- 3) Quali progressi e miglioramenti può portare l'intelligenza artificiale?

Il lavoro attraverso una revisione anche dei decreti applicati dal 2022 ad oggi cerca di rispondere alle seguenti domande di ricerca e cerca inoltre di fornire importanti spunti per applicare l'intelligenza artificiale al diritto.

### *1.1. Introduzione*

Uno dei motivi per cui l'intelligenza artificiale<sup>1</sup> rappresenta un tema

---

<sup>1</sup> Si faccia riferimento a C. CATH, S. WACHTER, B. MITTELSTADT, M. TADDEO, L. FLORIDI, "Artificial Intelligence and the Good Society": the US, EU, and UK approach, in Science and Eng. Ethics, 2018 pp. 12-20.

così forte nell'agenda di nazioni e comunità è che si stima che questa possa raggiungere, in un lasso di tempo relativamente breve di (cinque anni), il valore di 190,61 miliardi di dollari con un tasso annuo costante di crescita del 36%. anche in Italia l'interesse sembra rimanere a livello alto (quantomeno per le istituzioni che se ne devono occupare e nelle dichiarazioni dell'Agenda digitale italiana); ma secondo i dati dell'Osservatorio Artificial Intelligence del Politecnico di Milano, solo il 12% delle imprese ha portato a regime almeno un progetto di intelligenza artificiale. Ad oggi un'azienda su due non si è ancora mossa ma sta per farlo (l'8% è in fase di implementazione, il 31% ha in corso dei progetti pilota, il 21% ha stanziato del budget). Le applicazioni più diffuse sono, ovviamente, quelle di *virtual assistant/chatbot*. Le imprese italiane però hanno una visione ancora confusa delle opportunità dell'intelligenza artificiale. L'ascesa del mercato dei sistemi di intelligenza artificiale, con tutte le implicazioni ad essa connesse, porta delle conseguenze di ordine economico, etico e socio-antropologico che non risparmiano neanche il settore della giustizia penale.<sup>2</sup>

### *1.2. Studio della Privacy nell'ambito dell'Artificial Intelligence*

Le intelligenze artificiali (IA) possono comportare numerosi benefici dal punto di vista sociale ed ambientale e fornire vantaggi competitivi alle imprese, ma il loro impiego può anche rivelarsi rischioso per gli individui e la società,<sup>3</sup> dando luogo a potenziali problematiche di tipo etico e nell'ambito della protezione dei dati personali. Proprio per questo gli Stati e le organizzazioni internazionali hanno avvertito la necessità di un approccio che possa promuovere l'adozione delle IA affrontandone e gestendone i relativi rischi, di modo tale da delineare un quadro giuridico uniforme per il loro sviluppo, la loro

---

<sup>2</sup> S. GABORIAU, "Libertà e umanità del giudice: due valori fondamentali della giustizia. La giustizia digitale può garantire nel tempo la fedeltà a questi valori?" *Questione Giustizia*, fasc. 4, 2018.

<sup>3</sup> L. BENNET MOSES, J. CHAN "Assumptions, Evaluation, and Accountability, in *Policing and Society*", 2016, pp. 45-60.

commercializzazione ed il loro utilizzo in grado, al contempo, di garantire la sicurezza e i diritti fondamentali delle persone e delle imprese. La proposta di Regolamento presentata dalla Commissione europea in data 21 aprile 2021 stabilisce, appunto, un'infrastruttura giuridica omogenea per lo sviluppo, la commercializzazione e l'utilizzo delle IA in grado di garantire la sicurezza e i diritti fondamentali, che troverà applicazione ai soggetti pubblici e privati, alla sola condizione che il sistema sia immesso sul mercato dell'Unione o che il suo utilizzo abbia effetti sulle persone ivi situate (potendo perciò riguardare sia i fornitori che gli utenti). Questo nuovo quadro di riferimento si fonda su una classificazione dei sistemi di IA basata sul rischio. In primo luogo, i sistemi di IA che comportano un rischio minimo per i diritti o la sicurezza dei cittadini possono essere liberamente sviluppati ed utilizzati nel rispetto delle norme vigenti, con la possibilità per i fornitori di aderire a codici di condotta volontari redatti sulla base degli stessi criteri previsti per i sistemi ad alto rischio.

In secondo luogo, i sistemi a rischio limitato sono sottoposti ad obblighi di trasparenza qualora interagiscano con le persone, secondo meccanismi tali da rendere gli individui consapevoli di interagire con una macchina e consentire sempre loro di scegliere liberamente se proseguire o meno nel loro utilizzo. In terzo luogo, i sistemi di IA che comportano un rischio inaccettabile sono vietati in quanto considerati una minaccia per la sicurezza, i mezzi di sussistenza e i diritti<sup>4</sup> fondamentali delle persone. Nello specifico, non saranno ammessi quei sistemi che, tra le altre cose, manipolano il comportamento umano attraverso tecniche subliminali per aggirare il libero arbitrio degli utenti, sfruttano le vulnerabilità di specifici gruppi di individui a causa della loro età o di loro particolari caratteristiche, oppure consentono ai governi di attribuire un "punteggio sociale" agli individui. Anche l'uso dell'identificazione biometrica remota in tempo

---

<sup>4</sup> A. D'ALOIA, *"Intelligenza artificiale e diritto: Come regolare un mondo nuovo"*, 2020, pp. 48-90.

reale in spazi accessibili al pubblico con finalità di contrasto è in linea di principio vietata, salvi gli usi per la ricerca mirata di potenziali vittime specifiche di un reato, per la risposta ad una minaccia imminente di attacco terroristico o per l'individuazione degli autori di reati gravi.

Infine, un numero limitato di sistemi di IA sono considerati ad alto rischio a causa delle loro ripercussioni potenzialmente negative sulla sicurezza delle persone o sui loro diritti fondamentali. Più particolarmente, la proposta individua due categorie di sistemi IA ad alto rischio, quelli destinati ad essere utilizzati come componenti di sicurezza di prodotti soggetti ad una valutazione di conformità *ex ante* da parte di terzi, e quelli indipendenti (ossia non integrati in prodotti), di cui all'Allegato III della proposta di Regolamento, identificati sulla base di criteri quali, tra gli altri, il livello di utilizzo dell'applicazione di IA,<sup>5</sup> la sua finalità prevista, il numero di persone potenzialmente interessate, la dipendenza dai risultati e l'irreversibilità dei danni. Onde poter essere immessi sul mercato, questi sistemi dovranno rispettare gli obblighi specifici previsti dalla proposta, relativi i) ad un sistema di valutazione e attenuazione dei rischi, consistente in un processo continuo eseguito durante l'intero ciclo di vita del sistema, di modo da rendere i rischi residui accettabili, ii) all'utilizzo di insiemi di dati di elevata qualità che riducano al minimo i rischi di risultati discriminatori, iii) alla conservazione e all'aggiornamento dei documenti necessari per dimostrare che il sistema è conforme ai requisiti della proposta, iv) alla predisposizione di strumenti che consentano la registrazione automatica degli eventi durante l'utilizzo del sistema, v) alla trasparenza e alla fornitura di informazioni che ne consentano un utilizzo appropriato da parte degli utenti, vi) alla sorveglianza umana, di modo da prevenire o ridurre al minimo i rischi per la sicurezza e la salute degli individui, e vii) ad un livello di robustezza, accuratezza e cybersicurezza appropriato.

---

<sup>5</sup> E. BASSOLI, *"Algoritmica giuridica. Intelligenza artificiale e diritto"*, 2022, pp. 200-241.

La proposta prevede anche diversi obblighi per i fornitori dei sistemi di IA ad alto rischio, che dovranno essere soddisfatti prima della loro immissione sul mercato europeo. Più particolarmente, oltre ad attuare sistemi di gestione della qualità per garantire la conformità ai nuovi requisiti e ridurre al minimo i rischi per gli utenti e gli interessati, a conservare tutta la necessaria documentazione nonché a collaborare con le autorità nazionali competenti, i fornitori dovranno sottoporre il sistema ad una valutazione di conformità, di modo da dimostrare che lo stesso rispetta i requisiti previsti. Poiché è sempre più diffusa la preoccupazione che le IA possano essere sviluppate ed utilizzate in maniera contraria ai valori e all'etica democratica liberale, garantendo alle imprese vantaggi significativi senza appropriati controlimiti, negli ultimi tempi l'Unione europea ha avvertito la necessità di instaurare un dialogo con gli Stati Uniti, da sempre punto di riferimento in materia di IA, dove il dibattito sulla loro regolamentazione ha avuto luogo tanto a livello statale che federale, portando così all'introduzione, nel 2021, di progetti di legge o risoluzioni in almeno 16 Stati. Nella sua comunicazione del 2 dicembre 2020 relativa alla nuova<sup>6</sup> agenda UE-USA per il cambiamento globale, la Commissione europea ha ribadito l'importanza di interventi comuni in materia di IA fondati sull'idea che sia necessario un approccio antropocentrico, e che affrontino aspetti potenzialmente critici per le libertà democratiche, quali il riconoscimento facciale, proponendosi di avviare trattative per un accordo transatlantico sull'intelligenza artificiale e per definire un progetto di norme regionali e globali in linea con i valori comuni. Nel giugno 2020, inoltre, è stata istituita la Global Partnership on Artificial Intelligence (GPAI), un'iniziativa multilaterale che riunisce i principali esperti in diversi settori al fine di colmare il divario tra teoria e pratica attraverso la ricerca avanzata ed attività incentrate sulle priorità

---

<sup>6</sup> Si faccia riferimento a E. LATIFAH, A.H. BAJREKTAREVIC, M.N. IMANULLAH, *"Digital Justice in Online Dispute Resolution: The Shifting from Traditional to the New Generation of Dispute Resolution"*, in *Brawijaya Law Journal - Journal of Legal Studies*, vol. 6, aprile 2019.

legate alle IA. Promossa da Canada e Francia durante la loro presidenza del G7, l'iniziativa, che conta 19 membri tra cui Australia, Nuova Zelanda e, per l'appunto, Unione europea e Stati Uniti, mira a fornire un foro di condivisione della ricerca multidisciplinare e per identificare le questioni chiave in materia di AI, con l'obiettivo di facilitare la collaborazione internazionale, ridurre le duplicazioni, fungere da modello di riferimento e promuovere la fiducia nell'adozione di IA affidabili.

### *1.3. Intelligenza artificiale: implicazioni etiche in materia di Privacy e Diritto penale*

Da un punto di vista squisitamente normativo, troviamo all'interno dell'ordinamento e, nello specifico, nel sistema giudiziario un primo quadro di riferimento. Si tratta, a dire la verità, di un quadro composito ed eterogeneo dove a fianco di norme di diritto positivo, troviamo forme di *soft law*. Il più importante riconoscimento dei sistemi di intelligenza artificiale e la possibilità di un suo consapevole utilizzo nell'ambito dei sistemi giudiziari è rinvenibile nella Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi giudiziari e nei loro ambienti adottata dalla Commissione europea per l'efficienza nella giustizia<sup>7</sup> (CEPEJ) il 4 e 5 dicembre 2018. La Carta nello specifico definisce un quadro di principi utili a intraprendere e affrontare lo sviluppo dell'intelligenza artificiale nei processi giudiziari nazionali e va letto nell'ambito del più vasto sistema di garanzie costituito dalla CEDU e dalla normativa generale sul trattamento dei dati personali (Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 - GDPR). Questo strumento di *soft law* si articola in 5 principi e 4 Appendici: una, contenente uno studio approfondito dello stato dell'arte e delle problematiche aperte sull'uso dell'intelligenza artificiale nei sistemi giudiziari, la seconda contenente una griglia sui possibili utilizzi dell'intelligenza artificiale

---

<sup>7</sup> Si veda A. TRAVERSI, *"Intelligenza artificiale applicata alla giustizia"*, 2005, pp. 50-84.

nei sistemi giudiziari, la terza che reca un glossario, la quarta una *checklist* di autovalutazione della compatibilità dei modelli di utilizzo con i principi recati dalla Carta. L'articolo 1 è relativo ai diritti fondamentali, sulla cui base si definisce che il trattamento dei dati giudiziari e delle decisioni deve avere dei fini chiaramente individuati, nel pieno rispetto dei diritti fondamentali garantiti dalla Convenzione europea sui Diritti dell'Uomo e dalla Convenzione sulla protezione dei dati personali. Vi è poi il principio della non discriminazione secondo cui le applicazioni dell'intelligenza artificiale non devono riprodurre o aggravare le discriminazioni, pur esistenti all'interno della società, e portare ad analisi<sup>8</sup> o pratiche deterministiche che non tengano cioè conto delle situazioni particolari. Si pensi a tale proposito, in particolare, a quanto avviene negli Stati Uniti dove si è scelto di ricorrere a sistemi di valutazione automatizzata di predizione del rischio di recidiva (*risk assessment tools*). Questi strumenti, tuttavia, possono innescare l'introduzione di pregiudizi di ordine razziale o comunque relativi all'appartenenza a determinati contesti. Vi è poi il principio di qualità e sicurezza relativo al trattamento dei dati: i dati trattati tramite l'apprendimento automatico dovrebbero provenire da originali certificati e la loro integrità dovrebbe essere garantita in tutte le fasi del trattamento. In questo contesto il principale riferimento è all'utilizzo dei cosiddetti *open data*. Gli strumenti nominati finiscono per avere una forte incidenza sul principio della trasparenza, dell'imparzialità e dell'equità nel trattamento delle decisioni giudiziarie. In questo caso, l'attenzione si pone sul fatto che debba essere garantita la possibilità di effettuare dei controlli da parte di autorità o di esperti esterni in merito al trattamento dei dati. Rimane ben agganciato al tema in questione, il problema del rapporto tra tutela dei diritti di proprietà intellettuale e brevettuale di quanti hanno sviluppato il prodotto di intelligenza artificiale e la necessità di

---

<sup>8</sup> T. KING, N. AGGARWAL, M. TADDEO, L. FLORIDI, "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions, in *Science and Engineering Ethics*", 2019, pp. 25-45.

rendere trasparente e riproducibile il giudizio. Infine, il principio del controllo dell'utente: ogni utente dovrebbe essere informato, in un linguaggio chiaro e comprensibile, della natura vincolante o non vincolante delle soluzioni proposte dagli strumenti di intelligenza artificiale, delle diverse opzioni disponibili e del loro diritto all'assistenza di un avvocato e al ricorso a un tribunale. Si parla, in un'accezione ampia, di una generale alfabetizzazione informatica del pubblico circa l'utilizzo dell'intelligenza artificiale, in particolare modo nell'ambito dei giudizi penali, al fine di conferire maggiore autonomia e consapevolezza all'uso.

Da un punto di vista squisitamente normativo, troviamo all'interno dell'ordinamento e, nello specifico, nel sistema giudiziario un primo quadro di riferimento. Si tratta, a dire la verità, di un quadro composito ed eterogeneo dove a fianco di norme di diritto positivo, troviamo forme di *soft law*. Il più importante riconoscimento dei sistemi di intelligenza artificiale e la possibilità di un suo consapevole utilizzo nell'ambito dei sistemi giudiziari è rinvenibile nella Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi giudiziari e nei loro ambienti adottata dalla Commissione europea per l'efficienza nella giustizia<sup>9</sup> (CEPEJ) il 4 e 5 dicembre 2018. La Carta nello specifico definisce un quadro di principi utili a intraprendere e affrontare lo sviluppo dell'intelligenza artificiale nei processi giudiziari nazionali e va letto nell'ambito del più vasto sistema di garanzie costituito dalla CEDU e dalla normativa generale sul trattamento dei dati personali (Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 - GDPR). Questo strumento di *soft law* si articola in 5 principi e 4 Appendici: una, contenente uno studio approfondito dello stato dell'arte e delle problematiche aperte sull'uso dell'intelligenza artificiale nei sistemi giudiziari, la seconda contenente una griglia sui possibili utilizzi dell'intelligenza artificiale nei sistemi giudiziari, la terza che reca un glossario, la quarta una

---

<sup>9</sup> Si veda A. TRAVERSI, *"Intelligenza artificiale applicata alla giustizia"*, 2005, pp. 50-84.

*checklist* di autovalutazione della compatibilità dei modelli di utilizzo con i principi recati dalla Carta. L'articolo 1 è relativo ai diritti fondamentali, sulla cui base si definisce che il trattamento dei dati giudiziari e delle decisioni deve avere dei fini chiaramente individuati, nel pieno rispetto dei diritti fondamentali garantiti dalla Convenzione europea sui Diritti dell'Uomo e dalla Convenzione sulla protezione dei dati personali. Vi è poi il principio della non discriminazione secondo cui le applicazioni dell'intelligenza artificiale non devono riprodurre o aggravare le discriminazioni, pur esistenti all'interno della società, e portare ad analisi<sup>10</sup> o pratiche deterministiche che non tengano cioè conto delle situazioni particolari. Si pensi a tale proposito, in particolare, a quanto avviene negli Stati Uniti dove si è scelto di ricorrere a sistemi di valutazione automatizzata di predizione del rischio di recidiva (*risk assessment tools*). Questi strumenti, tuttavia, possono innescare l'introduzione di pregiudizi di ordine razziale o comunque relativi all'appartenenza a determinati contesti. Vi è poi il principio di qualità e sicurezza relativo al trattamento dei dati: i dati trattati tramite l'apprendimento automatico dovrebbero provenire da originali certificati e la loro integrità dovrebbe essere garantita in tutte le fasi del trattamento. In questo contesto il principale riferimento è all'utilizzo dei cosiddetti *open data*. Gli strumenti nominati finiscono per avere una forte incidenza sul principio della trasparenza, dell'imparzialità e dell'equità nel trattamento delle decisioni giudiziarie. In questo caso, l'attenzione si pone sul fatto che debba essere garantita la possibilità di effettuare dei controlli da parte di autorità o di esperti esterni in merito al trattamento dei dati. Rimane ben agganciato al tema in questione, il problema del rapporto tra tutela dei diritti di proprietà intellettuale e brevettuale di quanti hanno sviluppato il prodotto di intelligenza artificiale e la necessità di rendere trasparente e riproducibile il giudizio. Infine, il principio del

---

<sup>10</sup> T. KING, N. AGGARWAL, M. TADDEO, L. FLORIDI, "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions, in *Science and Engineering Ethics*", 2019, pp. 25-45.

controllo dell'utente: ogni utente dovrebbe essere informato, in un linguaggio chiaro e comprensibile, della natura vincolante o non vincolante delle soluzioni proposte dagli strumenti di intelligenza artificiale, delle diverse opzioni disponibili e del loro diritto all'assistenza di un avvocato e al ricorso a un tribunale. Si parla, in un'accezione ampia, di una generale alfabetizzazione informatica del pubblico circa l'utilizzo dell'intelligenza artificiale, in particolare modo nell'ambito dei giudizi penali, al fine di conferire maggiore autonomia e consapevolezza all'uso.

#### *1.4. L'intelligenza artificiale e il Law Enforcement*

Il *law enforcement* è un concetto che si traduce con l'applicazione di legge. Questo si riferisce a qualsiasi sistema attraverso il quale soggetti individuati e autorizzati agiscono in modo organizzato per dare attuazione alla legge. Si tratta di macchine robotiche, non necessariamente umanoidi, utilizzate per una varietà di compiti, come ad esempio attività di pattugliamento, sorveglianza, disinnescamento di bombe, individuazione di atteggiamenti sospetti, riconoscimento facciale. In merito a tali applicazioni, è lecito chiedersi quanto sia ampio il livello di autonomia delle macchine nello svolgimento delle funzioni predette. Inoltre, queste applicazioni utilizzano e immagazzinano un elevato numero dei dati in relazione ai quali potrebbe porsi un problema di privacy. Rientrano in tale categoria anche gli strumenti di "polizia predittiva che attraverso l'applicazione di metodi statistici hanno l'obiettivo di predire chi commetterà un reato. I software di polizia predittiva si distinguono principalmente in due grandi categorie: quelli che sono volti ad individuare le cosiddette "zone calde" (hotspots), ovvero i possibili luoghi che potranno essere lo scenario di determinati reati; quelli che, ispirandosi invece all'idea del *crime linking*, seguono le serialità criminali<sup>11</sup> di determinati

---

<sup>11</sup> Si veda G. HALLEVY, "The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control", in *Akron Intellectual Property Journal*, 2010.

soggetti (individuati o ancora da individuare), per prevedere dove e quando costoro commetteranno il prossimo reato. Infine, questi sistemi sembrano chiudersi in una sorta di “circolo vizioso” per cui in una certa misura si alimentano con i dati prodotti dal loro stesso utilizzo.

## **2. La decisione giudiziale e gli Automated Decision Systems**

Un’ulteriore modalità di utilizzo degli strumenti di intelligenza artificiale è costituita dai cosiddetti *automated decision systems* al fine di tentare la composizione di liti, ma anche di prevenirle e di risolvere le controversie. I sistemi automatizzati per le decisioni si basano su la capacità di analizzare un’enorme quantità di dati e sull’aver ormai predisposto dei dispositivi in grado di usare la teoria dei giochi, l’analisi dei risultati positivi e le strategie di negoziazione per risolvere le questioni. Seppure questo tipo di prodotti siano utilizzati prevalentemente nelle controversie civili, non è sfuggito alla Commissione europea il rischio collegato all’utilizzo di questi sistemi in ambito penale. La Commissione, infatti, nella già citata Carta etica europea per l’uso dell’intelligenza artificiale nei sistemi giudiziari e nei loro ambienti ha messo in guardia sul fatto che “anche se non sono specificamente progettati per essere discriminatori, l’uso di algoritmi basati sull’IA ha mostrato il rischio di favorire la rinascita di teorie deterministiche a scapito delle teorie dell’individualizzazione della pena”. Ma oltre alle problematiche collegate alla discriminazione, ci sono altre questioni che alcuni studiosi hanno messo in evidenza e sono: il fatto che il mezzo di prova usato più frequentemente nel processo penale per l’accertamento dei fatti è la testimonianza ed un computer non riuscirebbe a giudicare se questa sia vera oppure falsa o ancora reticente; inoltre, i criteri di valutazione delle prove sono diversi e non predeterminati, e questo, specialmente in un processo indiziario, rendere ancora più complicato per un algoritmo stabilire se si tratti di indizi “gravi, precisi e concordanti” ai sensi dell’art. 192,

comma 2, C.p.p. Gli strumenti di intelligenza artificiale che “commettono reati” Infine, consideriamo i casi di interazione tra diritto penale e intelligenza artificiale non perché quest’ultima possa essere utilizzata ai fini di una semplificazione ed efficientamento del procedimento ma perché lo strumento di intelligenza artificiale si potrebbe rendere protagonista nella commissione di un reato. Un aspetto problematico finora non considerato nei casi di impiego dell’intelligenza artificiale può verificarsi qualora gli strumenti dell’IA finiscano per “commettere dei reati”. La stessa locuzione deve essere mantenuta tra virgolette perché sono soggette alla responsabilità<sup>12</sup> penale le persone fisiche, ma in questo caso qual è la persona fisica che dovrebbe essere perseguita? Quelli che un tempo erano scenari quasi fantascientifici, ad oggi rappresentano problemi di forte attualità in grado, in ultima analisi, di mettere potenzialmente a dura prova il sistema giudiziario vigente. Uno strumento di intelligenza artificiale potrebbe essere utilizzato, in questo caso sotto il controllo di un umano, per commettere un reato.

Si pensi ad esempio a quanto avveniva con il bagarinaggio *online*: alcuni soggetti, grazie all’utilizzo di bot, acquistavano una gran quantità di biglietti, ad una velocità che non era comparabile a quella di qualsiasi umano, e poi li rivendevano *online* ad un prezzo maggiorato. È evidente la necessità di individuare nuove fattispecie di reato che possano essere applicate in casi di condotte criminose attraverso gli strumenti dell’intelligenza artificiale. In fondo l’ipotesi sopra riportata è l’eventualità più semplice da risolvere, ma cosa succede se invece ci troviamo di fronte ad un sistema di intelligenza artificiale, basato sull’apprendimento e con un discreto livello di autonomia, che commette un reato? Che fine fa il principio del “*machina delinquere non potest*”? Non avrebbe senso parlare di responsabilità né morale né giuridica della macchina, dal momento che questa è priva di coscienza e di intenzionalità delle proprie azioni, priva della capacità di determinarsi diversamente. Né essa potrebbe

---

<sup>12</sup> Si veda C. BAGNOLI, “*Teoria della responsabilità*”, 2019, pp. 23-40.

mai sensatamente essere rimproverata per un fatto da lei materialmente cagionato, perché al contrario dell'uomo non è libera ma determinata. Ma con l'intelligenza artificiale e negli algoritmi complessi la struttura non è completamente etero-determinata, non sono più integralmente preimpostati, chiusi e non suscettibili di cambiamenti, ma sono aperti ad auto-modifiche strutturali, determinate dall'esperienza della macchina. La macchina "ricorda" il passato, apprende dal proprio "vissuto" grazie al *machine learning* e modifica il proprio comportamento, di conseguenza, adattandolo così ai nuovi stimoli nel frattempo ricevuti. Addirittura, in molti casi l'intelligenza artificiale non si limita ad apprendere dalla propria esperienza, ma, come succede in un gruppo di pari, impara dall'esperienza dei propri simili, mediante il ricorso alle tecnologie di cloud computing. Sembra un futuro lontano nel tempo, ma non lo è: abbiamo già visto le macchine a guida autonoma, i droni da combattimento non teleguidati; i robot chirurgici. In questo campo è impossibile non citare il lavoro di Gabriel Hallevy, un penalista israeliano che si è occupato a lungo del problema dei rapporti tra diritto penale e intelligenza artificiale, secondo cui non vi sono dei veri e propri argomenti validi da spendere contro la già attuale perseguibilità e punibilità di soggetti artificiali intelligenti, quali robot chirurgici, droni autonomi o *self-driving cars*. Ma se i sistemi di intelligenza artificiale, almeno secondo alcuni studiosi, possono essere responsabili di reati, ne possono anche subire. Si apre qui un ulteriore campo di indagine per il diritto penale: l'intelligenza artificiale può essere vittima di reato?

### *2.1. Gli strumenti di Intelligenza artificiale che "commettono reati"*

Infine, consideriamo i casi di interazione tra diritto penale e intelligenza artificiale non perché quest'ultima possa essere utilizzata ai fini di una semplificazione ed efficientamento del procedimento ma perché lo strumento di intelligenza artificiale si potrebbe rendere protagonista nella commissione di un reato. Un aspetto problematico

finora non considerato nei casi di impiego dell'intelligenza artificiale può verificarsi qualora gli strumenti dell'IA finiscano per "commettere dei reati". La stessa locuzione deve essere mantenuta tra virgolette perché sono soggette alla responsabilità penale le persone fisiche, ma in questo caso qual è la persona fisica che dovrebbe essere perseguita? Quelli che un tempo erano scenari quasi fantascientifici, ad oggi rappresentano problemi di forte attualità in grado, in ultima analisi, di mettere potenzialmente a dura prova il sistema giudiziario vigente. Uno strumento di intelligenza artificiale<sup>13</sup> potrebbe essere utilizzato, in questo caso sotto il controllo di un umano, per commettere un reato. Si pensi ad esempio a quanto avveniva con il bagarinaggio *online*: alcuni soggetti, grazie all'utilizzo di bot, acquistavano una gran quantità di biglietti, ad una velocità che non era comparabile a quella di qualsiasi umano, e poi li rivendevano *online* ad un prezzo maggiorato. È evidente la necessità di individuare nuove fattispecie di reato che possano essere applicate in casi di condotte criminose attraverso gli strumenti dell'intelligenza artificiale. In fondo l'ipotesi sopra riportata è l'eventualità più semplice da risolvere, ma cosa succede se invece ci troviamo di fronte ad un sistema di intelligenza artificiale, basato sull'apprendimento e con un discreto livello di autonomia, che commette un reato? Che fine fa il principio del "*machina delinquere non potest*"? Non avrebbe senso parlare di responsabilità né morale né giuridica della macchina, dal momento che questa è priva di coscienza e di intenzionalità delle proprie azioni, priva della capacità di determinarsi diversamente. Né essa potrebbe mai sensatamente essere rimproverata per un fatto da lei materialmente cagionato, perché al contrario dell'uomo non è libera ma determinata. Ma con l'intelligenza artificiale e negli algoritmi complessi la struttura non è completamente etero-determinata, non sono più integralmente preimpostati, chiusi e non suscettibili di cambiamenti, ma sono aperti ad auto-modifiche

---

<sup>13</sup> GABRIEL HALLEVY, "*Liability for Crimes Involving Artificial Intelligence Systems*", Springer 2015, pp. 78-100.

strutturali, determinate dall'esperienza della macchina. La macchina "ricorda" il passato, apprende dal proprio "vissuto" grazie al *machine learning* e modifica il proprio comportamento, di conseguenza, adattandolo così ai nuovi stimoli nel frattempo ricevuti. Addirittura, in molti casi l'intelligenza artificiale non si limita ad apprendere dalla propria esperienza, ma, come succede in un gruppo di pari, impara dall'esperienza dei propri simili, mediante il ricorso alle tecnologie di *cloud computing*. Sembra un futuro lontano nel tempo, ma non lo è: abbiamo già visto le macchine a guida autonoma, i droni da combattimento non teleguidati; i robot chirurgici. In questo campo è impossibile non citare il lavoro di Gabriel Hallevy, un penalista israeliano che si è occupato a lungo del problema dei rapporti tra diritto penale e intelligenza<sup>14</sup> artificiale, secondo cui non vi sono dei veri e propri argomenti validi da spendere contro la già attuale perseguibilità e punibilità di soggetti artificiali intelligenti, quali robot chirurgici, droni autonomi o *self-driving cars*.

## 2.2. Come è possibile adattare i principi fondamentali del costituzionalismo con l'uso diffuso dell'Intelligenza artificiale?

L'IA poggia su una enorme, incalcolabile, quantità di dati, che sono il suo mondo. Il problema dei dati non è solo la tutela della privacy di chi li 'produce' e li fa circolare più o meno consapevolmente utilizzando le innumerevoli risorse del mondo digitale; e nemmeno il divario di efficienza tra noi e i nuovi sistemi agenti artificiali nel trattare questi dati, e nel ricavare da essi informazioni, outputs, indicazioni che poi servono a ricondizionare e riorientare i comportamenti e le scelte da cui quei dati derivano. Chi controlla questi dati ha in mano formidabili strumenti di potere e di influenza: economica, sociale, politica. E se questo potere è concentrato nella disponibilità di pochi grandissimi attori su scala mondiale, allora diventa anche una questione politica, un problema di sovranità. I

---

<sup>14</sup> Si veda M. SOMALVICO, F. AMIGONI, V. SCHIAFFONATI, "Intelligenza artificiale", Enciclopedia della Scienza e della Tecnica, febbraio 2021.

giganti del web sono poteri immensi sia sul piano economico che su quello – persino più insidioso – del controllo e dell’indirizzamento dei processi sociali e culturali; come è stato detto, “Facebook definisce chi siamo, Amazon definisce cosa vogliamo e Google definisce cosa pensiamo”. Benjamin Bratton segnala che stiamo assistendo ad uno shifting della sovranità, *“from state to individual, from state to corporation, from law to protocol, from institution to network, (in definitiva) from land to Cloud”*. L’AI, le sue risorse informazionali, il “mondo online”, costituiscono una realtà ‘totale’, che investe l’esperienza umana interamente, nelle sue proiezioni individuali e collettive, economiche e politiche, private e istituzionali. In secondo luogo, i sistemi di AI saranno uno dei grandi blocchi dello sviluppo economico mondiale in questo secolo. La sfida è (e sarà) quella di orientare (o almeno di ridurre i contrasti di) questa nuova imponente evoluzione tecnologica ed economica rispetto ai principi di tutela della dignità e della sicurezza umana, e dei diritti fondamentali. Una sorta di attualizzazione del messaggio contenuto nel secondo comma (e per certi versi anche nel terzo comma) del nostro art. 41 Cost., e più in generale in tutto il disegno costituzionale di società, fondato sulla centralità del lavoro, sulla dignità umana e sull’utilità sociale. La *AI revolution* ha bisogno di essere accompagnata e ‘corretta’ da un pensiero ‘costituzionale’, deve produrre una risposta in termini di concettualizzazione di diritti e principi, allo stesso modo di come la rivoluzione industriale ha prodotto l’evoluzione welfarista degli Stati liberali nel XIX secolo e il costituzionalismo sociale del XX secolo. Lo sviluppo della robotica e dei sistemi di AI avrà (sta già avendo) una serie di ricadute significative sul mercato del lavoro, sulla stessa sicurezza (e su molti diritti e libertà) nei luoghi di lavoro in considerazione delle più diffuse occasioni di coesistenza e di interazione tra umani e agenti “artificiali”. La sfida dell’AI richiede un aggiornamento complessivo dei modelli di istruzione e formazione professionale (e dello stesso principio costituzionale secondo cui “la scuola è aperta a tutti”) alla novità profonda del contesto digitale, e

un ripensamento di alcune strutture portanti del welfare. Per Roberto Cingolani, l'attuale modello di educazione e formazione professionale "poteva funzionare quando le rivoluzioni tecnologiche avvenivano nella scala di qualche generazione, ma oggi non più"; questo scienziato, attuale Ministro per la Transizione Ecologica nel Governo Draghi, propone di intersecare "la storia, la filosofia, le scienze umane con i nuovi orizzonti della tecnologia<sup>15</sup>".

2.3. *Come si sta evolvendo la legislazione internazionale in tema di intelligenza artificiale?*

In pochi anni si è assistito ad una proliferazione di documenti normativi internazionali e sovranazionali (essenzialmente del tipo 'soft law', combinato con strumenti di *self-regulation*, con l'eccezione del GDPR) sullo sviluppo dei sistemi di AI.

Comincia a delinearsi una "via europea all'IA" (da ultimo si può vedere il documento "*Getting the future right. Artificial Intelligence and fundamental rights*", pubblicato dalla European Union Agency for Fundamental Rights), che aspira a combinare l'implementazione dei sistemi intelligenti, quale fattore di innovazione, di profitto e di progresso a vari livelli, con l'attenzione ai rischi<sup>16</sup> e alle criticità che essi implicano, dentro un quadro etico-giuridico chiaro e riconoscibile, capace di affrontare l'impatto dell'IA *in primis* in termini di sostenibilità, di responsabilità, di diritti delle persone, di vantaggi per la società, di attendibilità e trasparenza dei processi decisionali. D'altronde, si tratta di un percorso normale quando ci si pone di fronte a tecnologie 'emergenti'. Il diritto procede in modo 'progressivo', sussidiario; ma questo, come è stato sottolineato giustamente, "può rappresentare l'approccio migliore per affrontare problemi complessi e diversi caratterizzati da incertezza".

In diversi Paesi poi cominciano ad essere approvate leggi in tema di responsabilità delle driverless cars (Germania), o sulla profilazione

---

<sup>15</sup> G. MASTROBUONI, "*Crime is Terribly Revealing: Information Technology and Police Productivity*", 2017, pp. 34-49.

<sup>16</sup> G. ZARA, "*Tra il probabile e il certo. La valutazione dei rischi di violenza e di recidiva criminale*", *Diritto penale contemporaneo*, 20 maggio 2016, pp. 42-58.

delle decisioni giudiziarie (Francia). Insomma, è un cantiere aperto, e siamo appena agli inizi.

#### 2.4. *Quale* utilizzo è possibile dell'intelligenza artificiale nella giustizia?

L'uso di *AI systems* nel processo e nelle attività di *crime prevention* è in forte crescita, ed è uno dei temi più controversi e al tempo stesso affascinanti di questo nuovo orizzonte tematico del diritto. L'utilità della decisione giudiziaria "robotica" o "algoritmica" viene declinata soprattutto nel senso della rapidità e della oggettività (potremmo dire anche esattezza della decisione non condizionata da fattori "soggettivi", emozionali, di adeguatezza professionale delle parti e del giudice, finanche di pregiudizi legati al sesso o all'orientamento sessuale, alla razza, alla religione, alla nazionalità, ecc.). La rapidità è sicuramente un aspetto importante del giusto processo. Il principio della ragionevole durata dei processi esprime da tempo una rilevanza pienamente costituzionale (art. 111 Cost. e art. 6 Convenzione EDU).

Sul piano dei principi costituzionali non è meno importante l'effettività e la pienezza del diritto alla difesa delle parti, la qualità della decisione giurisdizionale, la capacità del giudice di far emergere la irriducibile peculiarità dei fatti e di calibrare su di essi la decisione, in particolare (o almeno) quando davanti al giudice arrivano questioni scientifiche o rivendicazioni concrete inedite, non classificabili statisticamente, difficili da collocare in una dimensione standardizzata. È possibile ricondurre sempre agli schemi astratti della computazione algoritmica la straordinaria varietà dei fatti che il diritto è chiamato a considerare (in modo ragionevole e con proporzionalità), le sue clausole indeterminate, le emozioni, le speranze. I precedenti sono un elemento importante, e spesso decisivo, anche nell'attuale forma 'umana' della giurisdizione. Tuttavia, per la decisione algoritmica questa sembra una condizione immodificabile, geneticamente legata ai modi della sua costruzione. Il diritto 'umano' è invece aperto al dinamismo, alla 'invenzione' (nel senso di 'scoperta') di significati nuovi e mai in passato elaborati o

concepiti, alla fiducia che un'opinione isolata, perché non ancora giunta a maturazione, possa diventarlo dopo qualche anno, di fronte a contesti culturali e sociali modificati. Il luogo "critico" di questa riflessione è soprattutto il processo penale: del resto, nessun altro sotto-sistema istituzionale ha un impatto potenzialmente più pesante su diritti umani fondamentali, come la libertà personale, il diritto alla sicurezza, la dignità umana, il diritto<sup>17</sup> ad un giusto processo e a non essere considerati colpevoli fino a che non venga accertata la propria responsabilità (nella nostra Costituzione 'definitivamente'), il diritto del condannato a sperare nella rieducazione e nel reinserimento sociale. Si registrano casi in cui un software (Compas) ha contribuito alla valutazione del rischio di recidiva del condannato. La decisione finale è stata del giudice 'umano', ma l'algoritmo ha tracciato la base statistica. In altre parole, l'algoritmo è stato solo uno degli strumenti a disposizione del Giudice per esercitare la sua discrezionalità, ed è servito a supportare e completare altri elementi di valutazione. L'affermazione del principio di 'non esclusività' della decisione algoritmica sembra ancora saldo, e le tecniche di AI mantengono una natura strumentale, di ausilio, rispetto all'attività del Giudice. Il Giudice è soggetto soltanto alla legge, dice la Costituzione: e questo significa, tra le altre cose, che la legge può essere 'affiancata', orientata nell'applicazione da strumenti ulteriori, ma non sostituita mettendo il Giudice di fronte ad automatismi applicativi dipendenti dall'esito di procedure algoritmiche, per quanto alimentate e 'allenate' dai dati dei precedenti giurisprudenziali. Bisogna chiedersi però se è sufficiente; alcuni studiosi richiamano "la travolgente forza pratica dell'algoritmo": «un indubbio plusvalore pratico connesso alle scelte suggerite automaticamente (dal sistema, dall'algoritmo, dalla profilazione automatica), rispetto alla quale ci si può discostare, ma a patto di impegnarsi in un notevole sforzo (e rischio) valutativo».

Sul piano comparato, l'Estonia sta lavorando ad un progetto di

---

<sup>17</sup> A. SANTOSUOSSO, "Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto", 2020, pp. 150-200.

legge per applicare le decisioni automatizzate di tipo algoritmico alle controversie civili di valore economico basso, con la previsione di una possibilità di impugnazione della decisione di fronte ad una Corte 'umana'; in Canada, invece, e segnatamente nella Provincia della British Columbia, è attivo dal 2017 un modello di ODR (*online Dispute Resolution*) relativo ad alcuni '*small claims*', in particolare nell'ambito della responsabilità civile<sup>18</sup> derivante dalla circolazione stradale e delle controversie condominiali, che prevede la completa devoluzione del giudizio al sistema automatizzato, con la garanzia dell'impugnabilità delle decisioni davanti ad una *court of appeal*.

### **3. Risultati di ricerca e conclusioni**

L'emersione del diritto alla protezione dei dati personali discende direttamente dallo sviluppo delle tecnologie informatiche e telematiche e dal ruolo centrale assunto dall'informazione nel nuovo contesto economico e sociale. Sicché ogni consociato diventa, oggi, consapevole della necessità di non impedire che i propri dati circolino, ma tenendo bene in conto dei pericoli per i diritti e le libertà individuali che possono derivare da tale circolazione. Recenti episodi di cronaca hanno già fatto emergere i rischi associati a tutto ciò, legati alla sicurezza ma anche derivanti dall'uso dei dati, non confinati nella sfera digitale ma che possono incidere sulla vita fisica delle persone. In questo contesto assume valenza dirimente la nozione di "sovranità digitale" quale snodo della necessaria tutela statutale in ambito nazionale e internazionale. In mancanza, la sottrazione dell'ambito a una tutela ordinamentale è destinata ad esporre i diritti fondamentali di ognuno all'arbitrio di pochi, aprendo il passo al totalitarismo digitale. Nel difficile equilibrio fra innovazione digitale, da un lato, e diritti e libertà delle persone, dall'altro, è evidente e chiaro il segnale di pericolo per quelle pubbliche amministrazioni che non hanno ancora preso sul serio la pianificazione della propria

---

<sup>18</sup> C. CASTELLI, D. PIANA, "*Giusto processo e intelligenza artificiale*", 2019, pp. 78-95.

trasformazione digitale, garantendo al tempo stesso la tutela dei diritti degli interessati.