Il volume raccoglie i contributi presentati nel corso del convegno *"Intelligenza artificiale, dati e diritto"*, svoltosi a Cagliari il 12 e 13 dicembre 2024, su iniziativa del Centro Dipartimentale di Eccellenza "Diritto, innovazione e sviluppo sostenibile" del Dipartimento di Giurisprudenza dell'Università degli Studi di Cagliari. L'evento ha offerto un'occasione significativa di dialogo e di riflessione critica, coinvolgendo giovani studiose e studiosi provenienti da diversi atenei italiani, selezionati mediante una *call for papers* aperta a tutte le aree del sapere giuridico.

Obiettivo dell'iniziativa è stato quello di promuovere un approfondimento sulle molteplici sfide giuridiche poste dal crescente impiego dell'intelligenza artificiale nei più diversi ambiti dell'economia e della società, con particolare – seppur non esclusiva – attenzione alle questioni relative al trattamento e alla protezione dei dati personali. La discussione si è sviluppata tenendo conto sia delle più recenti innovazioni tecnologiche – tra cui l'emergere dei modelli generativi *general purpose* – sia degli ultimi interventi normativi, *in primis* l'entrata in vigore del Regolamento (UE) 2024/1689, noto come *AI Act*.

Tali trasformazioni impongono al giurista di confrontarsi con una revisione critica delle categorie tradizionali del diritto e di riformulare strumenti di tutela individuale e collettiva alla luce di un contesto socio-tecnologico in rapida evoluzione. In questo scenario, come evidenziato dalle discussioni che hanno preceduto e seguito l'approvazione dello *AI Act*, sarà cruciale la costante ricerca di un equilibrio, non privo di complessità, tra l'esigenza di promuovere l'innovazione e sostenere la competitività delle imprese, da un lato, e l'imperativo assiologico di garantire il rispetto dei diritti fondamentali, dall'altro.

Su queste premesse, il presente volume si propone di offrire un contributo al dibattito – ormai strutturalmente pervasivo – sulle implicazioni giuridiche dell'intelligenza artificiale, valorizzando in particolare le voci "emergenti" della comunità scientifica, naturalmente più sensibili alle dinamiche di trasformazione in atto, nel quadro di un percorso integrato e interdisciplinare di ricerca. La struttura del volume riflette in larga misura quella del convegno e si articola in diverse sezioni tematiche, ciascuna dedicata a un'area di particolare rilevanza nel rapporto tra diritto e intelligenza artificiale.

ISBN 979-12-5965-601-8

€ 40,00

41

D. Amoroso e A. Deffenu **Intelligenza artificiale, dati e diritto**

UNICA UNIVERSITÀ DEGLI STUDI DI CAGLIARI | DIPARTIMENTO DI ECCELLENZA 23 27

PUBBLICAZIONI DEL DIPARTIMENTO DI GIURISPRUDENZA – SERIE II 41

INTELLIGENZA ARTIFICIALE, DATI E DIRITTO

a cura di
Daniele Amoroso e Andrea Deffenu

CACUCCI EDITORE
BARI

Daniele Amoroso è professore associato di Diritto internazionale presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Cagliari. I suoi interessi di ricerca includono il rapporto tra diritto interno e diritto internazionale, i diritti umani e il diritto dell'IA. È tra i curatori dell'*Handbook on Meaningful Human Control of Artificial Intelligence Systems* (Edward Elgar, 2024).

Andrea Deffenu è professore ordinario di Diritto costituzionale presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Cagliari. Di recente ha pubblicato un manuale di Istituzioni di diritto pubblico con Andrea Cardone e Fulvio Cortese e si è interessato degli sviluppi più attuali del regionalismo Italiano. Dirige il Centro dipartimentale di eccellenza "Diritto, innovazione e sviluppo sostenibile".

UNICA UNIVERSITÀ DEGLI STUDI DI CAGLIARI | DIPARTIMENTO DI ECCELLENZA 23 27

PUBBLICAZIONI DEL DIPARTIMENTO DI GIURISPRUDENZA – SERIE II 41

INTELLIGENZA ARTIFICIALE, DATI E DIRITTO

a cura di

Daniele Amoroso e Andrea Deffenu

CACUCCI EDITORE

BARI

La pubblicazione del Volume è stata finanziata dal Dipartimento di Giurisprudenza dell'Università degli Studi di Cagliari nell'ambito del progetto "Dipartimenti di eccellenza 2023-2027".

I contributi sono stati sottoposti a referaggio.

L'Archivio della Casa Editrice Cacucci, con decreto prot. n. 953 del 30.3.2022 della Soprintendenza Archivistica e Bibliografica della Puglia-MiC, è stato dichiarato ***di interesse storico particolarmente importante*** *ai sensi degli articoli 10 c. 3, 13, 14 del d. lgs. n. 42/2004.*

© 2025 Cacucci Editore – Bari
Via Nicolai, 39 – 70122 Bari – Tel. 080/5214220
http://www.cacucciditore.it e-mail: info@cacucci.it

Indice

Prefazione

di **Daniele Amoroso e Andrea Deffenu**

Il volume raccoglie i contributi presentati nel corso del convegno *"Intelligenza artificiale, dati e diritto"*, svoltosi a Cagliari il 12 e 13 dicembre 2024, su iniziativa del Centro Dipartimentale di Eccellenza "Diritto, innovazione e sviluppo sostenibile" del Dipartimento di Giurisprudenza dell'Università degli Studi di Cagliari. L'evento ha offerto un'occasione significativa di dialogo e di riflessione critica, coinvolgendo giovani studiose e studiosi provenienti da diversi atenei italiani, selezionati mediante una *call for papers* aperta a tutte le aree del sapere giuridico, in linea con l'approccio inclusivo e interdisciplinare promosso dal Centro.

Obiettivo dell'iniziativa è stato quello di promuovere un approfondimento rigoroso e attuale sulle molteplici sfide giuridiche poste dal crescente impiego dell'intelligenza artificiale nei più diversi ambiti dell'economia e della società, con particolare – seppur non esclusiva – attenzione alle questioni relative al trattamento e alla protezione dei dati personali. La discussione si è sviluppata tenendo conto sia delle più recenti innovazioni tecnologiche – tra cui l'emergere dei modelli generativi *general purpose* – sia degli ultimi interventi normativi, in primis l'entrata in vigore del Regolamento (UE) 2024/1689, noto come *AI Act* e, sul piano interno, del DDL n. 1146 poi divenuto Legge n. 132 del 23 settembre 2025 recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale".

Tali trasformazioni impongono al giurista di confrontarsi con una revisione critica delle categorie tradizionali del diritto e di riformulare strumenti di tutela individuale e collettiva alla luce di un contesto socio-tecnologico in rapida evoluzione. In questo scenario, come evidenziato dalle discussioni che hanno preceduto e seguito l'approvazione dello *AI Act*, sarà cruciale la costante ricerca di un equilibrio, non privo di complessità, tra l'esigenza di promuovere l'innovazione e sostenere la competitività delle imprese, da un lato, e l'imperativo assiologico di garantire il rispetto dei diritti fondamentali, dall'altro.

Su queste premesse, il presente volume si propone di offrire un contributo al dibattito – ormai pervasivo – sulle implicazioni giuridiche dell'intelligenza artificiale, valorizzando in particolare le voci "emergenti" della comunità scientifica,

naturalmente più sensibili alle dinamiche di trasformazione in atto, nel quadro di un percorso integrato e interdisciplinare di ricerca.

La struttura del volume riflette in larga misura quella del convegno e si articola in diverse sezioni tematiche, ciascuna dedicata a un'area di particolare rilevanza nel rapporto tra diritto e intelligenza artificiale.

La prima sezione, *IA, democrazia e diritti umani*, raccoglie contributi che indagano le implicazioni dell'intelligenza artificiale in relazione alla tutela dei diritti fondamentali, alla qualità democratica delle istituzioni e ai processi di inclusione sociale. Il saggio di Pietro Villaschi apre il volume analizzando in prospettiva giuridico-costituzionale il fenomeno del *targeting* politico-elettorale *online*, con particolare attenzione ai rischi di manipolazione del consenso e alle sfide poste alla disciplina della comunicazione politica e alla tutela del pluralismo informativo. Luigi Prosia propone una riflessione sul tema delle disuguaglianze strutturali generate dal trattamento automatizzato dei dati, attraverso un'indagine sul ruolo delle azioni collettive e delle tutele sistemiche nella regolazione degli squilibri informativi e delle discriminazioni algoritmiche. Alice Civitella affronta il delicato tema dell'impiego di sistemi di intelligenza artificiale in ambito militare, concentrandosi sulle tensioni tra sicurezza, sorveglianza e diritto alla *privacy* e interrogandosi su rapporto tra quest'ultimo e le garanzie previste dal diritto internazionale umanitario. Sabrina El Sabi si sofferma sull'uso dei sistemi di riconoscimento delle emozioni, proponendo un'analisi critica di queste tecnologie alla luce dei diritti fondamentali e suggerendo l'impiego di strumenti di valutazione preventiva dell'impatto sui diritti, quali i *fundamental rights impact assessments*. Nel contributo di Salvatore Amato, infine, viene esaminato l'impatto dell'IA sul diritto all'istruzione delle persone migranti adulte, mettendo in luce i rischi di esclusione e marginalizzazione connessi all'utilizzo di tecnologie non adeguatamente calibrate sulle esigenze dei soggetti vulnerabili.

La seconda sezione, *IA, processo e procedimento*, si concentra sulle trasformazioni indotte dall'intelligenza artificiale nei diversi ambiti della giurisdizione (civile e penale) e dell'attività amministrativa e tributaria, offrendo una panoramica articolata degli impieghi attuali e potenziali della tecnologia nei meccanismi decisionali, istruttori e di controllo. Francesca Casciaro affronta l'impatto dell'intelligenza artificiale sul processo civile, indagando i possibili utilizzi dei sistemi automatizzati nella redazione degli atti e nelle fasi decisionali. Il saggio mette in rilievo i profili di compatibilità con i principi costituzionali del giusto processo, discutendone le implicazioni in tema di validità degli atti. Thomas Di Candia esamina invece il ricorso a sistemi di IA nella giustizia penale, soffermandosi in particolare sulla raccolta e l'elaborazione delle statistiche processuali. Il contributo discute le criticità connesse alla gestione automatizzata dei dati giudiziari e pone interrogativi sulla trasparenza e sulla funzione conoscitiva dei flussi informativi nel processo penale. Andrea Tronci guarda invece alla c.d. amministrazio-

ne algoritmica, esaminando l'impiego dell'IA nei procedimenti amministrativi e i suoi riflessi sul principio di trasparenza. L'analisi prende in esame la trasformazione della funzione amministrativa nell'ottica della decisione automatizzata, evidenziando le sfide che essa pone in termini di accessibilità, comprensibilità e controllo delle decisioni. Francesca De Vincentiis, infine, si occupa dell'utilizzo dell'IA nell'ambito dei controlli fiscali, analizzando l'adozione di sistemi predittivi e di profilazione del rischio da parte dell'amministrazione finanziaria. Il saggio approfondisce le tensioni tra l'efficienza dell'azione amministrativa e la necessità di garantire un adeguato livello di tutela dei diritti del contribuente, anche alla luce del principio di proporzionalità e del divieto di discriminazione.

La terza sezione si occupa di *IA, imprese e mercati*. Lorenzo Rodio Nico analizza con approccio sistematico il contenuto dell'*AI Act*, inquadrandolo nel contesto della regolazione delle tecnologie di frontiera. Il suo scritto riflette criticamente sull'equilibrio, non sempre agevole, tra esigenze di promozione dell'innovazione e garanzie di trasparenza, responsabilità e inclusività nell'utilizzo dei sistemi di intelligenza artificiale, mettendo in luce le connessioni tra il nuovo quadro regolatorio europeo e le traiettorie evolutive della governance tecnologica. Anche il contributo di Enza Cirone muove dall'*AI Act*, analizzando l'evoluzione e la funzione degli spazi di sperimentazione normativa (*regulatory sandboxes*) nel contesto dell'innovazione tecnologica. Il lavoro si sofferma sulle implicazioni giuridiche e regolatorie di questi strumenti, pensati per bilanciare promozione dell'innovazione e garanzie democratiche, attraverso un ambiente controllato in cui testare soluzioni di IA. Lorenzo Mariconda propone una riflessione sull'adozione di strumenti di IA nell'ambito delle imprese sociali, sottolineando le potenzialità di tali tecnologie per favorire un coinvolgimento più ampio degli *stakeholder* e per supportare il bilanciamento tra interessi economici e finalità solidaristiche, anche alla luce delle sfide poste dall'impatto ambientale e sociale delle scelte algoritmiche. Ludovica Serreli esplora le implicazioni dell'intelligenza artificiale per il consumatore digitale, mettendo in luce i rischi connessi alla profilazione, alla manipolazione delle scelte e alla concentrazione del potere di mercato nelle mani delle grandi piattaforme, nonché le relative lacune del diritto vigente in materia di tutela della parte debole del rapporto contrattuale. Riccardo Lazzardi, infine, affronta il tema della responsabilità da prodotto difettoso, con particolare riferimento all'utilizzo dell'intelligenza artificiale nella produzione alimentare. Il contributo analizza il regime europeo di responsabilità oggettiva, soffermandosi sulle sfide interpretative poste dal principio di precauzione e dall'esimente del rischio da sviluppo, in relazione all'introduzione di tecnologie intelligenti nella filiera agroindustriale.

La quarta e ultima sezione è dedicata a *IA e categorie generali del diritto*, e riunisce tre saggi che affrontano in prospettiva teorica l'impatto dell'intelligenza artificiale sugli schemi concettuali della tradizione giuridica. Giacomo Puggioni

esamina il fenomeno degli *smart contract*, soffermandosi sulle implicazioni concettuali dell'auto-esecuzione delle prestazioni e sulle tensioni che essa genera rispetto ai paradigmi classici dell'autonomia privata e del consenso. Giulia Bazzoni si concentra invece sulla responsabilità civile nell'impiego di sistemi automatizzati, affrontando le questioni relative alla causalità, all'imputazione soggettiva e alla standardizzazione dei modelli di condotta nei contesti in cui le decisioni sono assunte o mediate da algoritmi. Chiude il volume il contributo di Matthias Da Rold, che propone una riflessione sistematica sui mutamenti che l'IA impone alle categorie fondamentali del diritto, suggerendo la necessità di un adattamento del lessico e degli schemi interpretativi alla luce delle trasformazioni tecnologiche in atto.

* * *

Si ringraziano tutte le autrici e gli autori per il rigore scientifico e la disponibilità dimostrata, nonché i colleghi e le colleghe del Dipartimento di Giurisprudenza che, insieme al prof. Giovanni Fabio Licata dell'Università di Catania, hanno contribuito alla realizzazione del convegno e del volume in qualità di *discussant* e revisori, offrendo agli autori/relatori spunti preziosi di confronto e riflessione.

Un ringraziamento particolare va, infine, al dott. Matteo Zampella, per il supporto a tutto tondo garantito lungo l'intero percorso, dalla redazione della *call* alla cura degli aspetti organizzativi del convegno.

Sezione I
IA, DEMOCRAZIA E DIRITTI UMANI

Targeting politico-elettorale *online*, tutela dei dati personali e formazione dell'opinione pubblica: i nuovi regolamenti dell'Unione europea alla ricerca di un (difficile) equilibrio

di **Pietro Villaschi**

1. *Introduzione*

Al tempo del cosiddetto "capitalismo della sorveglianza"[1], la comunicazione politica sta subendo processi di evoluzione profonda e ancora non pienamente comprensibili nella loro esatta portata.

La diffusione di una comunicazione sempre più monodirezionale e disintermediata, la circolazione di notizie false e la disseminazione di disinformazione, la capacità di chiunque di ricevere, ma anche di farsi produttore di informazione, l'emersione di figure carismatiche che sanno approfittare delle opportunità offerte dalle piattaforme digitali stanno radicalmente cambiando il modo di "fare politica".

In questo quadro, in rapida e mutevole evoluzione, uno degli strumenti più significativi consiste nel ricorso al *targeting* politico-elettorale, ossia all'invio di messaggi *marked oriented* a gruppi selezionati di elettori allo scopo di intercettarne le rispettive preferenze. Ciò è particolarmente vero nei periodi di campagna elettorale, ove una profilazione massiva gioca un ruolo decisivo nella costruzione e nella manipolazione del consenso[2].

Questo fenomeno incide sul diritto dei cittadini-elettori, che nella realtà digitale sono anche utenti, ad essere informati e, più in generale, sul principio del

---

[1] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Londra, 2019.

[2] Cfr. F. Balaguer Callejon, *La Constituciòn del algoritmo*, Madrid, 2023, p. 68 ss.

pluralismo dei media, che, come emerge nella giurisprudenza costituzionale[3], costituiscono un presupposto fondamentale per il funzionamento del sistema democratico.

Non solo. Il ricorso a queste pratiche, nel favorire un rapporto sempre più diretto tra elettori ed eletti, ha un effetto di "rimbalzo" sul sistema politico-partitico, incentivando l'ascesa sulla scena pubblica di *leader* carismatici "digitali" che proprio da una comunicazione priva di barriere traggono la loro forza. Più di recente, si assiste a un fenomeno nuovo, ossia all'alleanza tra queste figure carismatiche e i proprietari delle grandi piattaforme digitali su cui la comunicazione politica si svolge, in un intreccio di interessi politici ed economici non sempre chiaro.

Più in generale, evidenti sono le conseguenze sui sistemi democratici nel loro insieme, in termini di qualità del discorso pubblico e politico, di strutturazione del rapporto tra rappresentanti e rappresentati, di gestione delle campagne elettorali e, in definitiva, di esito delle elezioni, dato il rischio di distorsione del consenso al quale queste pratiche espongono.

In risposta a queste sfide l'Unione europea ha deciso, a differenza di altre realtà (si pensi agli Stati Uniti)[4], di costruire un complesso quadro regolatorio, in cui una molteplicità di atti normativi differenti si intrecciano e si intersecano tra loro.

Ci si riferisce, anzitutto, al *Digital Services Act* (*DSA*), il regolamento sui servizi digitali[5], che, assieme al *Digital Markets Act* (*DMA*)[6], costituisce uno dei pilastri

---

[3] *Ex plurimis*, cfr. Corte cost., sent. n. 202 del 1976; Corte cost., sent. n. 148 del 1981; Corte cost., sent. n. 826 del 1988, Corte cost., sent. n. 112 del 1993. Sul diritto ad essere informati cfr. P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, p. 233 ss.; P. Costanzo, *(voce) Informazione nel diritto costituzionale*, in *Dig. Pubb.*, VIII, Torino, 1992; R. Zaccaria, L. Capecchi, *La libertà di manifestazione del pensiero*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, XII, Padova, 1990, p. 300; A. Pace, *Libertà di informare e diritto ad essere informati. Due prospettive a confronto nell'interpretazione e nelle prime applicazioni dell'art. 7, co. 1, t.u. della radiotelevisione*, in *Dir. pubbl.*, n. 2, 2007. Più di recente, ricostruisce le principali questioni in materia L. Cianci, *Il diritto ad essere informati alla prova delle strategie di microtargeting per la comunicazione politica*, in *Nomos. Le attualità nel diritto*, 1/2023, pp. 1-24.

[4] Cfr. F. Donati, *La protezione dei diritti fondamentali nel regolamento sull'intelligenza artificiale*, in *Rivista Aic*, 1/2025, p. 8, che scrive: "*Gli USA hanno seguito un modello 'market-driven', che confida sulle dinamiche spontanee del mercato per realizzare il benessere economico e sociale*".

[5] *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC.*

[6] *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and amending Directives (EE) 2019/1937 and (EU) 2020/1828.*

del *Digital Services Package* e pone significativi oneri in capo alle grandi piattaforme (c.d. *VLOPs* e *VLOSEs*). A questi regolamenti ha fatto seguito il regolamento sulla trasparenza e sul *targeting* della pubblicità politica (*RPA*)[7], che si applica specificamente alla comunicazione politica *online* e che sarà operativo, salve alcune limitate previsioni già in vigore, a partire dal prossimo ottobre. Più di recente, è stato approvato l'*Artificial Intelligence Act* (AI ACT)[8], che pur non prevedendo previsioni a*d hoc* specificamente dedicate alla profilazione – in quanto sul punto rinvia al regolamento sulla protezione dei dati personali, ossia al *GDPR* – costituisce la cornice di sfondo, dal momento che i più recenti sistemi di targetizzazione e profilazione si basano sulle potenzialità offerte dai sistemi di intelligenza artificiale[9].

Da ultimo, a testimonianza dell'estrema attualità e importanza delle tematiche qui considerate, lo scorso 6 dicembre, con una decisione unica nel suo genere, la Corte costituzionale rumena ha annullato il primo turno delle elezioni presidenziali in Romania proprio per una (supposta) campagna dis-informativa *online*, che avrebbe distorto la formazione del consenso degli elettori a tal punto da inficiarne la libertà di voto. Trattasi di una pronuncia che apre scenari inediti, dimostrando plasticamente, al di là della condivisibilità o meno degli approdi cui la Corte è giunta, come la relazione tra rappresentanti e rappresentati risenta, oggi, dei processi insiti nella rivoluzione digitale.

2. *Il* targeting *politico-elettorale* online*: coordinate fondamentali*

Con *targeting* si intende una serie di tecniche che, tramite la raccolta e l'analisi dei dati personali degli utenti rinvenibili *online*, mirano a intercettarne le preferenze, al fine di sottoporre loro messaggi personalizzati.

---

[7] *Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising.*

[8] *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*

[9] Cfr., sempre, F. Donati, *La protezione dei diritti fondamentali*, cit., p. 1 ss. V., anche, G. Gometz, *Intelligenza artificiale, profilazione e nuove forme di discriminazione*, in *Teoria e storia del diritto privato*, numero speciale 2022, p. 1 ss.; A. Adinolfi, *Processi decisionali automatizzati e diritto antidiscriminatorio dell'Unione europea*, in A. Adinolfi, A. Simoncini (a cura di), *Protezione dei dati personali, e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, 2022, p. 31 ss.

Nate originariamente per finalità di *marketing*, queste pratiche sono oggi impiegate per esigenze di costruzione del consenso politico.

Sui *social media* è possibile fare propaganda fondamentalmente in due modi: come semplice utente condividendo i contenuti sul profilo oppure pagando la piattaforma, affinché pubblicizzi i contenuti politici di una determinata pagina/profilo.

Ne è conferma il fatto che gli attori politici concentrano sempre maggiori risorse in questa direzione. Prendendo a riferimento la campagna elettorale per le elezioni politiche italiane del 25 settembre 2022, si può constatare che, nell'ultimo mese, Fratelli d'Italia, partito che ha poi vinto le elezioni, ha speso più di 140.000 euro solo su *Facebook*; la pagina personale di Matteo Salvini, con oltre cinque milioni di *followers*, è stata, invece, la più seguita, spendendo su *Facebook* 63.520 euro. È interessante, altresì, che il partito della Lega abbia deciso di promuovere la pagina del *leader* più di quella del partito: sulla pagina ufficiale della Lega sono stati, infatti, investiti solo 6.008 euro. La pagina personale di Silvio Berlusconi e quella di Forza Italia hanno speso meno di 15.000 euro, addirittura quasi 110 volte meno delle pagine di Fratelli d'Italia e di Giorgia Meloni assieme, a testimonianza del diverso approccio all'uso dei *social* da parte dei due leader. Per quanto riguarda la coalizione di centro-sinistra, Più Europa ha investito ben 55.222 euro su *Facebook* negli ultimi 30 giorni di campagna elettorale. *Trend* simile quello del Partito Democratico, che ha speso 46.540 euro dal 22 agosto al 20 settembre 2022, e dell'alleanza Verdi-Sinistra, che ha speso quasi tutto negli ultimi giorni di campagna elettorale. Oltre alle spese delle due coalizioni principali sono significative anche quelle dell'alleanza formata da Azione e Italia viva. Dal 22 agosto al 20 settembre 2022, la pagina di Carlo Calenda ha speso 16.136 euro, quella di Azione 8.741 euro, quella di Matteo Renzi 1.360 euro e quella di Italia viva 12.510 euro. Al contrario, è singolare che un partito, abile nell'uso e sfruttamento delle potenzialità delle moderne tecnologie come il MoVimento 5 Stelle, non abbia investito quasi nulla in pubblicità su *Facebook*. Piuttosto, è stato il *leader*, Giuseppe Conte, ad aver speso 16.308 euro solo nell'ultimo mese.

Con riferimento alle elezioni europee 2024, nell'ultima settimana di campagna elettorale, ossia tra il 3 e il 9 giugno, Fratelli d'Italia è il partito che ha peso più di tutti sui *social network*, con una spesa pari a 60.700 euro, circa 9mila euro al giorno. Segue Matteo Salvini (44.200 euro) e il partito della Lega (4.800 euro), che sommati arrivano a 49.000 euro di inserzioni. Il terzo posto spetta a Elly Schlein e al Partito Democratico, che in totale hanno investito 33.400 euro (15.500 per la pagina di Schlein e 17.900 per quella del partito). Minori gli importi di Italia Viva (9.500 euro) e Matteo Renzi (23.600 euro) e di Più Europa (9.800 euro) ed Emma Bonino (15.200 euro). Nell'ultima settimana di campagna elettorale, Azione e il suo segretario Carlo Calenda hanno speso complessivamente 18.800 euro, mentre il Movimento 5 Stelle e Giuseppe Conte 16.500.

L'alleanza Verdi-Sinistra ha investito circa 15mila euro, mentre Forza Italia è il partito che ha speso di meno, circa 4mila euro.

Peraltro, quelli qui riportati sono i soli dati delle pagine *online* "ufficiali" dei partiti e dei rispettivi leader, cui va aggiunto tutto l'insieme di inserzioni, difficilmente tracciabili, aventi contenuto politico, che riempiono quotidianamente le bacheche *online* degli utenti e che provengono dalle fonti più disparate.

Da quanto precede, se ne deduce una sempre maggior attenzione da parte degli attori politici nei confronti dei *social media* quali mezzi di costruzione del consenso. La fortuna e l'appetibilità di questi strumenti risiede nella circostanza che essi sono dotati di un potenziale partecipativo, di una velocità, di una capacità di raggiungere, capillarmente, i destinatari di gran lunga superiore rispetto ai *media* tradizionali. Tuttavia, proprio le loro stesse caratteristiche si rivelano particolarmente adatte a strategie di manipolazione degli elettori, fondate sulla profilazione dell'utente. La profilazione, a sua volta, si mischia spesso alla disseminazione di disinformazione o di notizie, immagini e profili falsi, oggi facilmente creabili grazie alle capacità di elaborazione sempre maggiori dei sistemi di intelligenza artificiale[10].

3. *Le conseguenze del* targeting *politico-elettorale* online

La rivoluzione digitale aveva inizialmente suscitato diffuse speranze circa il potenziale democratico derivante da strumenti di comunicazione, come *Internet*, in grado di decentrare la produzione e il consumo di informazione, favorire il confronto tra gli utenti, abbattere filtri e barriere spazio-temporali, dando vita ad una comunicazione orizzontale e fluida[11]. In questo senso, nel pensiero dei primi cyber-utopisti, la Rete avrebbe avuto la capacità di curare, almeno in parte, le disfunzioni delle moderne democrazie, ravvivando il coinvolgimento dei cittadini nella vita politica, favorendo la libera circolazione delle idee, dando vita a nuovi spazi di confronto tra tutti i consociati in condizioni di isegoria. L'uso della Rete era, in altri termini, immaginato per essere pluralista, aperto e libero, come nessuno spazio comunicativo sino ad allora sperimentato nella storia dell'umanità[12].

La realtà delle cose si è mossa in direzione differente. L'interazione sui *social* si è sviluppata sulla base di algoritmi che profilano gli utenti in base alle loro

---

[10] Cfr. G. Proietti, *L'impianto regolatorio della società dell'informazione tra vecchi e nuovi equilibri. Il fenomeno del deep fake*, in *MediaLaws*, 1/2024, p. 1 ss.

[11] F. Donati, *La protezione dei diritti fondamentali*, cit., p. 10 ss.

[12] Cfr. C. S. Sunstein, *Infotopia: How many minds produce knowledge*, Oxford, 2006, p. 1 ss.; J. Waldron, *Principio di maggioranza e dignità della legislazione*, Milano, 2001, p. 140 ss.

preferenze; favoriscono l'incontro tra idee analoghe, rafforzando convincimenti pregressi e relativi pregiudizi; consentono di selezionare i destinatari del messaggio e, dunque, permettono ad uno stesso soggetto di indirizzare messaggi diversi e anche incoerenti a porzioni segmentate del proprio pubblico; favoriscono la circolazione di notizie false, tendenziose e di contenuti disinformativi; consentono forme di comunicazione disintermediate e una relazione tra rappresentanti e rappresentati di natura iper-personale; più di recente, l'emersione di sistemi di intelligenza artificiale favorisce nuove forme di manipolazione, tra cui la diffusione di immagini false, la produzione automatica di testi, la creazione di *bot* o *troll*[13].

Per comprendere il fenomeno, va considerato che la profilazione, prima ancora che in ambito politico, è stata ampiamente utilizzata a fini pubblicitari per mostrare agli utenti prodotti e servizi più conferenti coi rispettivi profili, arrivando a guidare e condizionare le scelte del consumatore, che non è esposto in tal modo a prodotti e servizi alternativi, ma solamente a quelli per la sua persona ritenuti più appetibili.

Dal *marketing* questi sistemi sono stati ben presto impiegati ai fini di commercializzazione del messaggio politico, risultando in grado così di influenzare l'orientamento elettorale degli utenti[14].

Questo salto di qualità della profilazione ha posto una serie di interrogativi.

In primo luogo, viene in rilievo un tema di protezione dati personali degli utenti, stante il fatto che gli algoritmi che vengono impiegati a questo scopo si nutrono di dati, il cui trattamento è autorizzato spesso in assenza di una reale consapevolezza che alcuni servizi, proposti apparentemente come gratuiti dalle piattaforme, nascondono, in realtà, una commercializzazione dei dati stessi. In secondo luogo, la profilazione determina la creazione di *filter bubbles*, entro cui l'utente viene sostanzialmente isolato e nelle quali si assiste ad un rafforzamento delle posizioni iniziali e dei relativi pregiudizi, con una forte cyber-polarizzazione del dibattito pubblico[15].

---

[13] F. Zuiderveen Borgesius, J. Möller, S. Kruikemeier, R. Fathaigh, K. Irion, T. Dobber, C. Bodo, C. De Vreese, *Online Political Microtargeting: Promises and Threats for Democracy*, in *Utrecht Law Rev.*, 1/2018, p. 82 ss.

[14] Sul punto, v. T. Dobber, R. Fathaigh, F. Zuiderveen Borgesius, *The regulation of online political micro-targeting in Europe*, in *Internet Policy Rev.*, 4/2019, p. 5 ss.; G. D'Ippolito, *Comunicazione politica online: dal messaggio politico commercializzato alle sponsorizzazioni sui social network*, in *MediaLaws*, 1/2020, p. 167 ss.

[15] Cfr. K. Klonic, *The New Governors: The People, Rules, and Processes Governing Online Speech*, in *Harvard Law Rev.*, 1/2018, p. 1599 ss.; G. Ziccardi, *L'uso dei social network in politica tra alterazione degli equilibri democratici, disinformazione, propaganda e dittatura dell'algoritmo: alcune considerazioni informatico-giuridiche*, in *Ragion pratica*,

In secondo luogo, la profilazione impatta sui partiti politici, per quanto riguarda il loro rapporto con l'elettorato, la relazione con i nuovi intermediari della società digitale e, inoltre, l'organizzazione interna. Per un verso, trattasi di pratiche che se adottate su larga scala risultano molto onerose, favorendo così le forze con maggiori risorse finanziarie. Sotto altro profilo, i candidati sono messi nelle condizioni di modellare la propria immagine in base alle aspettative dell'elettorato. Inoltre, poiché alcuni utenti non sono molto attivi *online*, i partiti potrebbero basare la loro campagna politica solo sull'analisi dei dati forniti dagli utenti che fanno un uso più frequente dei *social media*, producendo un fenomeno di "presbiopia" nel mercato politico-elettorale[16].

In terzo luogo, le campagne *online* si svolgono in un contesto di disintermediazione mediatica. Chiunque sul *Web* può cercare informazioni, ma anche produrle e condividerle, aumentando esponenzialmente il numero delle fonti di informazione e la loro capacità espansiva. Questa assenza di mediazione provoca, tuttavia, una forte personalizzazione del sistema politico e partitico: nel *targeting* i leader trovano lo strumento per dare vita ad una comunicazione senza filtri con i propri elettori, il che favorisce la scalata dei partiti politici da parte di veri e propri "*outsider*", che si rivelano molto più abili rispetto ai politici di professione nel comunicare con la base elettorale. Un esempio in questo senso è chiaramente il caso di Donald Trump, che è riuscito a imporsi dall'esterno in un partito storicamente molto forte e strutturato come quello repubblicano americano[17] e che, anche grazie alla sua forza mediatica sui *social*, ha conquistato dapprima nel 2016 e nuovamente nel 2024 la Casa Bianca[18].

Fenomeno più recente, e ancor più preoccupante, è quello dell'alleanza tra tali *leader* carismatici e i proprietari più influenti delle piattaforme: un esempio in questo senso è la pericolosa commistione di interessi tra Elon Musk, proprietario della piattaforma *X*, e Trump nel corso della campagna elettorale per le ultime presidenziali USA, che ha trovato conferma anche nei primi mesi del

---

1/2020, p. 51 ss.

[16] Elemento quest'ultimo che, tuttavia, ha anche un riflesso positivo, nel senso che testimonia come non tutti gli elettori siano attivi online e, quindi, come una parte dell'elettorato sfugga all'effetto di queste tecniche di costruzione del consenso.

[17] Sulla scalata di Trump nei confronti del partito repubblicano americano, v. M. Calise, *Il destino dei partiti*, in *Quad. cost.*, 1/2023, p. 101 ss.

[18] Sulla vittoria di Trump alle ultime elezioni presidenziali e sulle strategie adottate in campagna elettorale, che dimostrano una grande capacità di formazione del consenso online, ma anche una particolare abilità nella costruzione di un rapporto diretto e "reale" con l'elettorato, cfr. F. Clementi, *Tra dilemmi ed opportunità: la vittoria di Donald Trump e le sfide per la democrazia negli Stati Uniti*, in *Federalismi*, 28/2024, pp. IV-XII.

mandato. Processo che testimonia, ancor più chiaramente, l'involuzione in senso leaderistico delle democrazie moderne, ove si assiste all'affermazione di enormi concentrazioni di potere.

Infine, a livello più generale, le tecniche di *targeting* comportano la frammentazione dell'opinione pubblica in gruppi chiusi e polarizzati[19]. L'effetto combinato di *fake news*, *cyber-cascades* e *confirmation bias* tende ad alterare la percezione della realtà, andando così a incidere sul versante passivo della libertà d'informazione, ossia il diritto ad essere informati che, come la Corte costituzionale ha riconosciuto, "va determinato e qualificato in riferimento ai principi fondanti della forma di Stato delineata dalla Costituzione, i quali esigono che la nostra democrazia sia basata su una libera opinione pubblica e sia in grado di svilupparsi attraverso la pari concorrenza di tutti alla formazione della volontà generale"[20].

Di qui la necessità di una regolazione di questi processi, onde scongiurare una distorsione patologica dei presupposti stessi della rappresentanza politica e della partecipazione democratica.

4. *Il cambio di passo dell'Unione europea: dal* Digital Services Act*, al Regolamento relativo alla trasparenza e al* targeting *della pubblicità politica, all'*Artificial Intelligence Act

Nonostante l'assoluta rilevanza del fenomeno, per lungo tempo il quadro è stato caratterizzato da una sostanziale auto-regolamentazione da parte delle piattaforme, che hanno gestito in autonomia i rispettivi spazi, ponendo gli utenti di fronte all'alternativa tra l'accettare la profilazione oppure restare esclusi dal servizio.

Di fronte a questo scenario, l'Unione europea ha deciso un importante cambio di passo.

Tra i provvedimenti più significativi si può, anzitutto, menzionare il Regolamento (UE) 2022/2065, c.d. *Digital Services Act* (*DSA*), pubblicato il 27 ottobre 2022 e direttamente applicabile dal 17 febbraio 2024[21]. Assieme al *Digital Markets Act*, approvato poche settimane prima e che mira, invece, ad assicurare la concorrenza nel mercato interno dei servizi digitali, esso costituisce uno dei

---

[19] Cfr., sul punto, M. Betzu, *I baroni del digitale*, Napoli, 2022, p. 1 ss.; A. Cardone, *«Decisione algoritmica» vs decisione politica? A.I. Legge. Democrazia*, Napoli, 2021, p. 72 ss.

[20] Corte cost., sent. n. 112 del 1993, Considerato in Diritto n. 7.

[21] Per le piattaforme *online* e i motori di ricerca di dimensioni molto grandi, come ad esempio *Meta*, *X*, *Tik Tok*, *Amazon*, *Google*, gli obblighi si applicano, invece, già dal 25 agosto 2023.

pilastri fondanti del *Digital Services Package*, strategia attuata dall'Unione al fine di assicurare uno spazio digitale prevedibile, sicuro e affidabile.

In primo luogo, sotto il profilo soggettivo, il *DSA* si applica ai "prestatori di servizi intermediari" (sia *mere conduit*, che *caching*, che *hosting*), ossia tutti quei soggetti che forniscono "un qualsiasi servizio, normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario".

In secondo luogo, il regolamento prevede:

a) alcune disposizioni generali, che si applicano a tutti i prestatori di servizi (sezione I, articoli 11-15);
b) una serie di previsioni aggiuntive relative ai prestatori di servizi di *hosting*, incluse le piattaforme *online* (sezione II, articoli 16-18);
c) una serie di disposizioni relative esclusivamente ai fornitori di piattaforme online (sezione III, articoli 19-28).
d) alcune disposizioni ulteriori, che si applicano a quei fornitori di piattaforme *online*, che consentono ai consumatori di concludere contratti a distanza con gli operatori commerciali (sezione IV, articoli 29-32).
e) infine, obblighi supplementari per le piattaforme e i motori di ricerca di dimensioni molto grandi (sezione V, articoli 33-44). Con "piattaforme e motori di ricerca molto grandi" (d'ora in poi, rispettivamente, "*VLOPs*" e "*VLOSEs*") si intendono quei soggetti, che hanno un numero medio mensile di utenti attivi pari o superiore a 45 milioni nell'Unione. Il riconoscimento avviene a seguito di una procedura, disciplinata dall'art. 33 del regolamento, che si conclude con una decisione della Commissione europea.

Tra le previsioni più significative, l'articolo 26 stabilisce che i fornitori di piattaforme *online* provvedono affinché, per ogni singola pubblicità, i destinatari del servizio siano in grado di identificare in modo chiaro: a) che l'informazione costituisce una *pubblicità*, anche attraverso contrassegni visibili; b) la *persona fisica o giuridica* per conto della quale viene presentata o pagata la pubblicità; c) le informazioni rilevanti relative ai *parametri* utilizzati per determinare il destinatario della pubblicità e, laddove applicabile, alle modalità di modifica di detti parametri da parte dell'utente. Il legislatore europeo ha qui recepito le indicazioni che erano state formulate dall'*European Data Protection Board* in relazione ai rischi di elusione del *GDPR*, regolamento concepito in un periodo storico in cui le problematiche di cui si tratta erano solo agli inizi.

Inoltre, i fornitori di piattaforme *online* sono tenuti a mettere a disposizione dei destinatari del servizio una funzionalità che consenta di dichiarare se i contenuti che forniscono contengano comunicazioni commerciali. Sempre in un'ottica di trasparenza, all'articolo 27, si prevede che i fornitori di piattaforme *online*, che si avvalgono di sistemi di raccomandazione, specifichino nelle loro

condizioni generali, in un linguaggio chiaro e intellegibile, i principali parametri utilizzati nei loro sistemi di raccomandazione, nonché qualunque opzione a disposizione dei destinatari del servizio che consente loro di modificare tali parametri. Inoltre, i fornitori di piattaforme *online* debbono rendere disponibile anche una funzionalità che consente al destinatario del servizio di selezionare e modificare in qualsiasi momento l'opzione preferita relativa ai parametri con cui vengono determinate le pubblicità.

Con riguardo, invece, ai dati sottoponibili o meno a profilazione, l'articolo 26 § 3 stabilisce un divieto assoluto di presentare pubblicità ai destinatari del servizio basata sulla profilazione delle categorie speciali di dati personali di cui all'articolo 9, § 1, del *GDPR*. Questo significa che le piattaforme non possono più profilare gli utenti utilizzando dati relativi all'origine razziale o etnica, alle opinioni politiche, alle convinzioni religiose o filosofiche, all'appartenenza sindacale, 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. La disposizione va letta in combinato disposto con l'art. 28 del *DSA*, che vieta, altresì, che sia presentata pubblicità basata su dati personali di utenti del servizio che siano minori.

Obblighi supplementari sono stabiliti per i *VLOPs* e i *VLOSEs*, i quali sono, anzitutto, tenuti ad individuare, analizzare e valutare gli eventuali rischi sistemici derivanti dalla progettazione o dal funzionamento del loro servizio (artt. 34-35).

Inoltre, all'art. 38, si stabilisce che, in aggiunta ai requisiti di cui al già citato art. 27, i *VLOPs* e i *VLOSEs* assicurano all'utente almeno un'opzione per i loro sistemi di raccomandazione che non sia basata sulla profilazione.

All'art. 39, si prevede, altresì, che tutte le piattaforme di dimensioni molto grandi, che presentano pubblicità sulle loro interfacce *online*, compilano e rendono accessibile al pubblico, in una specifica sezione, un registro contenente una serie di informazioni per l'intero periodo durante il quale presentano la pubblicità. Tale registro deve, inoltre, necessariamente stabilire: a) il contenuto della pubblicità, compreso il nome del prodotto, del servizio, del marchio e l'oggetto della pubblicità; b) la persona fisica o giuridica per conto della quale viene presentata o pagata la pubblicità; c) il periodo durante la quale viene presentata la pubblicità; d) un'indicazione volta a precisare se la pubblicità fosse destinata a essere presentata a uno o più gruppi specifici di destinatari del servizio e, in tal caso, i principali parametri utilizzati a tal fine; e) le comunicazioni commerciali pubblicate; f) il numero totale di destinatari del servizio raggiunti e, ove opportuno, i dati aggregati suddivisi per ciascuno Stato membro relativi al gruppo o ai gruppi di destinatari ai quali la pubblicità era specificamente destinata.

Il *DSA* si muove, quindi, su un ampio raggio di azione, disciplinando l'intero mercato dei servizi digitali e integrando, in questo modo, le previsioni contenute nel *GDPR*.

La prima fondamentale linea direttrice è quella della trasparenza. Trattasi di una scelta condivisibile, essendo oggi obbligatorio indicare per conto di chi e con quali parametri gli avvisi pubblicitari sono presentati agli utenti. Incisivi anche gli interventi in materia di profilazione, essendo precluso che le categorie di dati ex art. 9 *GDPR* o i dati che abbiano ad oggetto soggetti minorenni possano essere trattati. In questo modo, la disciplina contenuta nel *GDPR* viene irrigidita e resa applicabile al contesto digitale che si è, nel mentre, concretizzato.

Non mancano, tuttavia, profili critici[22]. Anzitutto, le previsioni in parola si applicano, sotto il profilo soggettivo, ai soli *hosting provider* e non a tutti i titolari del trattamento. Dal punto di vista oggettivo, non è facile perimetrare la nozione di "speciale categoria di dati" ex art. 9 *GDPR*, rendendo quindi possibile che i divieti pur formalmente presenti siano aggirati dalle piattaforme.

Negli ultimi mesi si è anche potuta verificare una prima "messa a terra" di queste previsioni.

La Commissione europea ha aperto, infatti, un procedimento formale, proprio sulla base del *DSA*, nei confronti di Meta, sul presupposto che l'azienda non si sia adeguata alle prescrizioni in tema di pubblicità ingannevole e di disinformazione, in tema di trasparenza e di visibilità dei contenuti politici, che non abbia valutato diligentemente e attenuato adeguatamente i rischi connessi agli effetti di *Facebook* e *Instagram* sul dibattito civico e sui processi elettorali, che il suo sistema di notifica degli illeciti non sia conforme agli *standard* stabiliti sempre dal *DSA*. La procedura è ancora in corso, in attesa delle risposte di Meta alle obiezioni sollevate dalla Commissione e delle possibili determinazioni di quest'ultima.

Sotto altro profilo, apre scenari inediti la decisione di Meta di offrire agli utenti dell'Unione europea una versione delle piattaforme *Facebook* e *Instagram*, per la prima volta, senza pubblicità e profilazione, ma a pagamento. Trattasi di un'opzione che viene offerta in alternativa a quella gratuita rispetto alla quale, invece, nulla cambia. Tale formula, tuttavia, ha destato l'attenzione della Commissione europea, che ha comunicato alla società che tale modello non sarebbe conforme all'articolo 5, § 2, del *Digital Markets Act*, dal momento che non permetterebbe agli utenti di optare per un servizio che utilizzi un quantitativo

[22] A commento, cfr. P. Cesarini, *The Digital Services Act: a Silver Bullet to Fight Disinformation?*, in *Medialaws.eu*, 8 febbraio 2021, p. 1 ss.; C. Frisani, *Il Digital Services Act: le prospettive di riforma per una maggior tutela online*, in *Ius in Itinere*, 9 Novembre 2022, p. 1 ss.; O. Grandinetti, *Le piattaforme digitali come "poteri privati" e la censura online*, in *Riv. it. inf. dir.*, 1/2022, p. 175 ss.; E. Birritteri, *Contrasto alla disinformazione, Digital Services Act e attività di private enforcement: fondamento, contenuti e limiti degli obblighi di compliance e dei poteri di auto-normazione degli operatori*, in *MediaLaws*, 2/2023, pp. 52-87; L. Catanzano, *Libertà di espressione e verità artificiali. Quale marketplace of ideas nella società dell'algoritmo?*, in *MediaLaws*, 1/2024, p. 1 ss.

inferiore dei loro dati personali, ma che sia comunque equivalente al servizio che prevede gli annunci pubblicitari personalizzati e consenta agli utenti di esercitare il loro diritto di acconsentire liberamente alla combinazione dei propri dati. Ad avviso della Commissione, per garantire il rispetto del regolamento sui mercati digitali, gli utenti che non intendono dare il loro consenso dovrebbero comunque avere accesso a un servizio equivalente che utilizzi un quantitativo inferiore dei loro dati personali, in questo caso ai fini della personalizzazione degli annunci pubblicitari. La procedura è anche in questo caso ancora in corso e occorrerà, pertanto, verificarne l'esito[23].

Tali vicende dimostrano che, una volta data una determinata una cornice di regole, anche piuttosto dettagliata, occorre far seguire una lunga fase di implementazione, durante la quale le piattaforme stanno, peraltro, tentando di aggirare i limiti e i divieti posti dalla normativa euro-unitaria per preservare il proprio *business*.

Il *Digital Services Act*, tuttavia, non è, come detto, un regolamento concepito specificamente per la comunicazione elettorale e politica. Ciò spiega perché l'Unione europea, passati solo pochi mesi dalla sua entrata in vigore, ha approvato un nuovo regolamento *ad hoc* per la propaganda e la pubblicità politica ed elettorale *online*, ossia il *Regolamento (UE) 2024/900 del Parlamento europeo e del Consiglio del 13 marzo 2024 relativo alla trasparenza e al targeting della pubblicità politica*.

Esso si applicherà, salve alcune limitate previsioni già in vigore, a partire dall'ottobre 2025.

Lo scopo è duplice: da un lato, assicurare il corretto funzionamento del mercato interno della pubblicità politica e dei servizi connessi; dall'altro, tutelare le persone fisiche con riguardo al trattamento dei dati personali[24].

La proposta si muove, quindi, su alcune linee principali. Anzitutto, sono posti una serie di obblighi di trasparenza e diligenza in capo ai "prestatori di servizi di pubblicità politica", definiti come "una persona fisica o giuridica impegnata nella prestazione di servizi di pubblicità politica". Con "pubblicità politica" ci si riferisce, invece, "alla preparazione, collocazione, promozione, pubblicazione, consegna o diffusione, con qualsiasi mezzo, di un messaggio fornito normalmente dietro retribuzione o tramite attività interne o nell'ambito di una campagna

---

[23] Cfr. R. Sabia, *L'enforcement pubblico del Digital Services Act tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni*, in *MediaLaws*, 2/2023, pp. 88-113.

[24] Su questo regolamento, cfr., tra i primi commenti, M. Z. van Drunen, N. Helberger, R.O. Fathaigh, *The beginning of EU political advertising law: unifying democratic visions through the internal market*, in *Internet Policy Review*, 30/2022, pp. 181-199.

di pubblicità politica: a) di, a favore o per conto di un attore politico, salvo se di natura meramente privata o meramente commerciale; oppure b) che possa e sia inteso a influenzare l'esito di un'elezione o referendum, un comportamento di voto o un processo legislativo o regolamentare, a livello dell'Unione, nazionale, regionale o locale" (art. 3).

Una delle previsioni più significative è quella prevista dall'art. 11, ove si stabilisce che gli editori di pubblicità politica provvedano affinché ogni messaggio di pubblicità politica riporti in modo chiaro, visibile e senza ambiguità: a) una dichiarazione che attesti che si tratti di un messaggio di pubblicità politica; b) lo *sponsor* del messaggio di pubblicità politica e, ove possibile, l'entità che controlla lo *sponsor*; c) l'indicazione dell'elezione, del referendum o del processo legislativo o regolamentare cui è connesso il messaggio di pubblicità politica in questione; d) una dichiarazione attestante che il messaggio di pubblicità politica è stato oggetto di tecniche di *targeting* o di consegna del messaggio; e) un avviso di trasparenza che contenga le informazioni prescritte dal regolamento stesso. Inoltre, gli editori di pubblicità politica sono tenuti ad assicurare agli utenti la possibilità di segnalare che un determinato messaggio di pubblicità politica non è conforme al regolamento e debbono predisporre un sistema di notifica idoneo allo scopo (secondo un meccanismo che richiama quanto previsto dal *DSA* in tema di segnalazione di discorsi d'odio e di contenuti non corrispondenti al vero).

Trattasi di prescrizioni che seguono le raccomandazioni dell'*European Data Protection Supervisor*[25], collocandosi come supplementari rispetto ai già importanti obblighi di trasparenza stabiliti dal *Digital Services Act*.

Primo obiettivo della nuova normativa è quello di responsabilizzare il titolare del trattamento, dal momento che la tenuta di specifici registri e una maggiore trasparenza sulle tecniche di profilazione dovrebbero spingere le piattaforme a trattare i dati degli utenti in senso effettivamente conforme alla normativa eurounitaria. In secondo luogo, le norme in materia di trasparenza si pongono a tutela degli stessi attori politici che, nel momento in cui dovessero fare ricorso a queste tecniche, sarebbero più consapevoli delle modalità con cui si esplica la profilazione. Infine, si intendono tutelare gli utenti, i quali sarebbero finalmente in grado di visualizzare, contestualmente alla diffusione del messaggio pubblicitario, tutta una serie di informazioni utili per comprendere su quali basi proprio quello specifico messaggio viene loro presentato[26].

---

[25] Cfr. European Data Protection Supervisor, *Opinion No 2/2022 of 20 January 2022 on the Proposal for Regulation on the transparency and targeting of political advertising*, p. 9 ss.

[26] Cfr. M. Van Drunen, E. Groen-Reijman, T.Dobber, A. Noroozian, P. Leerssen, N. Helberger, C. H. de Vreese, F. Votta, *Transparency and (no) more in the Political Advertising Regulation*, in *Internet Policy Review*, 1/2022, p. 1 ss.

Con riferimento, invece, alla normativa in materia di *targeting*, il regolamento prevede che il trattamento dei dati personali sia consentito a determinate condizioni. Più nello specifico, le tecniche di *targeting* o di consegna del messaggio pubblicitario in ambito di pubblicità politica *online* sono, d'ora in poi, ammissibili solo se il titolare del trattamento ha raccolto: a) i dati personali presso l'interessato; b) l'interessato ha prestato il proprio consenso esplicito al trattamento separato dei dati personali a fini di pubblicità politica; c) e, inoltre, solo se tali tecniche non comportano la "profilazione", quale definita all'articolo 4, punto 4), del regolamento (UE) 2016/679 e all'articolo 3, punto 5), del regolamento (UE) 2018/1725. Il legislatore europeo ha scelto una linea piuttosto rigorosa, stabilendo, quindi, un divieto assoluto di *targeting* per determinate categorie di dati, considerate particolarmente sensibili.

Con riguardo, invece, ai dati non sottoposti a protezione speciale il trattamento è limitato a quelli che siano frutto di un consenso esplicito dell'interessato, prestato unicamente a fini della pubblicità politica *online* e purché non si tratti, chiaramente, di profilazione. Anche sotto questo profilo, il testo presenta una formulazione particolarmente severa e sicuramente rafforzativa rispetto alle analoghe previsioni contenute nel *GDPR*.

Trattasi, pertanto, di una novità importante, dal momento che le piattaforme dovranno ottenere necessariamente un espresso consenso al trattamento da parte degli utenti. Tuttavia, rimane il fatto che potrebbe non essere sufficiente agire esclusivamente sul piano dei doveri informativi del titolare del trattamento[27]: sarebbe infatti una mera finzione credere che il consenso prestato dall'utente sia effettivamente informato, consapevole e libero e, pertanto, tale base giuridica potrebbe risultare, alla prova dei fatti, insufficiente[28].

Per quanto lo sforzo del legislatore europeo sia quindi lodevole, non mancano punti interrogativi e nodi irrisolti. Da un lato, le previsioni in parola potranno essere aggirate senza grandi difficoltà dalle piattaforme: non essendo stato previsto un divieto generale ed assoluto di *targeting* per scopi politici, rimane, infatti, aperta la possibilità che gli utenti possano essere profilati per il tramite di dati apparentemente non sensibili, i c.d. "dati inferiti". Dall'altro, vi è un rischio diametralmente opposto: la proliferazione di una serie di regolamenti in un breve lasso di tempo rischia di rendere estremamente complesso e intricato il quadro normativo, non solo per coloro che fanno uso di tali pratiche (si pensi ai

---

[27] D. Sborlini, *Profilazione elettorale e protezione dei dati personali: prospettive di soluzione in ambito europeo*, in *Dir. inf.*, 1/2022, p. 1173 ss.

[28] Aspetto questo evidenziato anche dalla Corte di Giustizia dell'Unione europea nella sentenza del 4 Luglio 2023, *case C-252/21, Meta Platform Inc. and Others v. Bundeskartellamt* (§§ 147-148).

candidati e alle forze politiche che partecipano alle elezioni e che debbono fare campagna elettorale *online*), ma anche per le stesse piattaforme che potrebbero essere indotte ad abbandonare il mercato europeo qualora tali regole dovessero divenire eccessivamente onerose.

A completare il panorama normativo, da ultimo, non può non citarsi l'*Artificial Intelligence Act*, approvato dal Parlamento il 13 marzo 2024 e dal Consiglio il 21 maggio 2024[29], primo regolamento al mondo a disciplinare, in modo organico, i sistemi di intelligenza artificiale[30].

Obiettivo è quello di promuovere un'intelligenza artificiale antropocentrica e affidabile e, in questo modo, garantire un livello elevato di protezione dei diritti fondamentali[31].

Per fare questo, l'Unione ha scelto di adottare un modello di governance "*rights-driven*"[32], in quanto volto essenzialmente alla tutela dei diritti della persona contro le minacce derivanti dalla tecnologia, e seguire un approccio "*risk-based*", in base al quale, al crescere del rischio del sistema di AI per i diritti fondamentali, si inaspriscono parallelamente le regole e gli oneri.

---

[29] L'intero Regolamento sarà applicabile dal 2 agosto 2026 ad eccezione: dei divieti relativi a pratiche di intelligenza artificiale proibite (ossia a rischio inaccettabile), che troveranno applicazione già dal 2 febbraio 2025; dei codici di buone pratiche, che dovranno essere pronti dal 2 maggio 2025; delle prescrizioni relative ai sistemi di AI per finalità generali, che troveranno applicazione dal 2 agosto 2025; degli adempimenti per i sistemi di AI ad alto rischio, che troveranno applicazione: (i) dal 2 agosto 2026, nel caso di sistema di AI ad alto rischio che rientri all'interno dell'Allegato III; oppure (ii) dal 2 agosto 2027, nel caso in cui tali sistemi di AI ad alto rischio rientrino nell'elenco della normativa di armonizzazione dell'Unione presente all'interno dell'Allegato I.

[30] Cfr., *ex plurimis*, A. Quintavalla, J. Temperman (a cura di), *Artificial Intelligence and Human Rights*, Oxford, 2023; G. Sartor, *L'intelligenza artificiale e il diritto*, Torino, 2022; O. Pollicino, P. Dunn, *Intelligenza artificiale e democrazia. Opportunità e rischi di disinformazione e discriminazione*, Milano, 2024.

[31] Ai sensi del Considerando 1, obiettivo del regolamento è: "migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di AI) nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale (AI) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di AI nell'Unione, nonché promuovere l'innovazione".

[32] Cfr. F. Donati, *La protezione dei diritti fondamentali*, cit., p. 6.

Non è questa la sede, chiaramente, per un'analisi approfondita dell'*AI ACT*, che meriterebbe ben altra trattazione. Per quello che qui più interessa, è sufficiente ricordare che tale regolamento lascia, anzitutto, impregiudicato l'obbligo di rispettare il *GDPR* in materia di trattamento dei dati personali[33]. Ne è un esempio il fatto che la dichiarazione di conformità necessaria per i sistemi ad alto rischio deve prevedere un'attestazione sulla conformità alla disciplina dell'Unione in materia di protezione dei dati personali.

Ne consegue che, in tema di trattamento dei dati personali degli utenti, tale regolamento non incide, sul diritto, riconosciuto dall'art. 22 del *GDPR*, a non essere sottoposti ad una "decisione basata unicamente sul trattamento automatizzato" e che produca effetti giuridici che lo riguardano o che incida in modo analogo sulla sua persona. Le previsioni dell'*AI ACT* non rientrano, in altre parole, nelle eccezioni al divieto generale stabilito dall'art. 22 *GDPR* in materia di profilazione.

Sul punto, la Corte di Giustizia dell'Unione europea ha offerto, di recente, alcuni importanti chiarimenti. Nella sentenza del 7 dicembre 2023, *Schufa Holding AG*[34], ha, infatti, precisato che della disposizione in parola va data un'interpretazione estensiva a tutela degli utenti: in particolare, il divieto di trattamento automatizzato dei dati degli utenti deve applicarsi sempre qualora sussista un sufficiente grado di probabilità che la decisione automatizzata possa produrre, direttamente o indirettamente, effetti negativi nei confronti di una persona. La Corte ha, altresì, stabilito che la decisione basata unicamente sul trattamento automatizzato dei dati, ove ammessa, deve comunque essere accompagnata da una serie di misure volte a ridurre il rischio di errori e a garantire la sicurezza dei dati personali, nonché da oneri di informazione, contestazione e ricorso all'intervento umano. Questo avrà significative ricadute anche per tutti i sistemi di AI di natura predittiva che si fondano sul trattamento dei dati personali degli utenti e

[33] Cfr., in particolare, l'art. 2, comma 7, *AI Act*. In materia, cfr. A. Adinolfi, A. Simonicini (a cura di), *Protezione dei dati personali, e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, 2022; M. Bassini, O. Pollicino, *Intelligenza artificiale e protezione dei dati personali*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione? Diritti fondamentali, dati personali e regolazione.* Vol. I, Bologna, 2022, p. 269 ss.; E. C. Raffiotta, M. Baroni, *Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, ivi, p. 363 ss.

[34] CGUE, sentenza 7 dicembre 2023, C-634/21, *Schufa Holding AG*, ECLI:EU:C:2023:957. A commento, cfr. C. Silvano, *La nozione di "decisione completamente automatizzata" sotto la lente della Corte di Giustizia: il caso Schufa*, in *Rivista interdisciplinare sul diritto delle amministrazioni pubbliche*, 4/2024, pp. 270-306.

che saranno sempre più impiegati anche nel campo della comunicazione politica ed elettorale nei prossimi anni.

5. *Una decisione inedita: la sentenza della Corte costituzionale rumena del 6 dicembre 2024*

Come illustrato nelle pagine che precedono, profondi processi di trasformazione stanno segnando il modo di fare propaganda elettorale e di costruire il consenso politico. Parallelamente, specie a livello sovra-nazionale, si cerca di approntare una serie di misure per governare e contenere questi fenomeni che si esplicano nella realtà digitale.

In questo quadro, si colloca la sentenza della Corte costituzionale rumena n. 32 del 6 dicembre 2024[35], pronuncia che, già all'indomani della sua pubblicazione, ha suscitato un ampio clamore nell'opinione pubblica.

I giudici costituzionali della Romania hanno, infatti, assunto una decisione drastica e inaspettata, annullando l'esito del primo turno delle elezioni presidenziali per una supposta campagna elettorale dis-informativa svoltasi *online* a favore di uno dei contendenti.

Una breve premessa è qui necessaria.

A dispetto dei sondaggi, infatti, il primo turno delle elezioni presidenziali era stato vinto dal candidato di estrema destra e filo-russo Georgescu che, al ballottaggio, avrebbe dovuto sfidare la seconda classificata, la candidata liberale ed europeista Lasconi. Era stato, invece, sconfitto a sorpresa il premier in carica Colacu.

I servizi segreti rumeni avevano messo in guardia dal rischio che, per mano di interferenze russe, la formazione del consenso degli elettori sarebbe stata gravemente alterata, in particolare a causa dell'attivazione di oltre 25.000 *account* sospetti su *Tik Tok* diretti a favorire, con una campagna capillare, proprio Georgescu a danno degli altri candidati.

Sulla base di queste premesse, a soli due giorni dallo svolgimento del secondo turno previsto per l'8 dicembre, la Corte costituzionale ha, pertanto, deciso di annullare e di far ripetere le elezioni, facendo precipitare il Paese nel *caos* politico e istituzionale, suscitando le proteste dei candidati giunti al ballottaggio e segnando una decisione senza precedenti.

Le motivazioni, invero molto succinte, addotte dalla Corte dimostrano plasticamente tutta la rilevanza che la formazione del consenso *online* riveste oggi, nella realtà digitale, al fine di condizionare l'esito delle consultazioni elettorali.

[35] HOTĂRÂREA nr. 32 din 6 decembrie 2024 privind anularea procesului electoral cu privire la alegerea Președintelui României din anul 2024.

La premessa teorica da cui muovono i giudici costituzionali rumeni risiede nello stretto collegamento tra libertà del voto, tenuta della democrazia e diritto a essere informati, ossia proprio la dimensione passiva della libertà di informazione di cui si diceva (*retro* § § 2 e 3).

Afferma, difatti, la Corte che "la libertà degli elettori di formarsi un'opinione include il diritto di essere correttamente informati prima di prendere una decisione. Più precisamente, tale libertà implica il diritto di ottenere informazioni corrette sui candidati e sul processo elettorale da tutte le fonti, inclusi i canali *online*, nonché la protezione contro influenze ingiustificate, attraverso atti/azioni illegali o sproporzionate, sul comportamento di voto. La pubblicità politica può talvolta trasformarsi in un veicolo di disinformazione, soprattutto quando [...] non dichiara il proprio carattere politico, proviene da sponsor esterni all'Unione o è soggetta a tecniche di targeting o di diffusione del materiale pubblicitario".

A sostegno delle proprie argomentazioni la Corte cita qui proprio il Regolamento (UE) 2024/900 del Parlamento Europeo e del Consiglio del 13 marzo 2024 sulla trasparenza e il *targeting* della pubblicità politica, di cui si è discorso in precedenza (*retro* § 4).

Nel corso della campagna elettorale, ad avviso dei giudici, "il carattere liberamente espresso del voto è stato violato attraverso la disinformazione degli elettori mediante una campagna elettorale in cui uno dei candidati ha beneficiato di una promozione aggressiva, condotta eludendo la legislazione nazionale in materia elettorale e sfruttando abusivamente gli algoritmi delle piattaforme social".

Ne discenderebbe che sarebbe "stata compromessa la parità di opportunità dei concorrenti elettorali, riflettendo un'alterazione del diritto stesso di essere eletti". Le irregolarità nella campagna elettorale avrebbero, inoltre, "penalizzato i concorrenti, creando una chiara disuguaglianza tra il candidato che ha manipolato le tecnologie digitali e gli altri partecipanti al processo elettorale". Inoltre, ad avviso dei giudici costituzionali, "un candidato ha violato la legislazione elettorale relativa al finanziamento della campagna elettorale per le presidenziali".

L'insieme combinato, quindi, di alterazione della formazione del consenso degli elettori tramite l'uso sofisticato delle tecnologie dell'informazione e della comunicazione, violazione delle regole in tema di trasparenza e di finanziamento, mancato rispetto della pari concorrenza tra tutti i candidati ha determinato vizi tali da determinare l'annullamento del processo elettorale e la necessità di ripetizione delle elezioni.

Trattasi di una pronuncia che suscita più di un interrogativo.

I temi che i giudici costituzionali sollevano sono certamente seri. Si è detto, infatti, che la capacità manipolativa della comunicazione *online* può essere tale da distorcere la percezione della realtà da parte degli elettori e incidere sul risultato delle elezioni stesse. Parimenti, quello della trasparenza delle fonti di finanziamento, specie in campagna elettorale, è un tema centrale, che, oggi, in

un tempo in cui la comunicazione *online* rende tutto più fluido e impalpabile, dimostra ancor di più la sua attualità. Lo stesso può dirsi con riferimento alla *par condicio* elettorale, che, proprio in un contesto come quello *online*, fatica a trovare effettiva applicazione, trattandosi spesso di regole rimaste ancorate al sistema radio-televisivo.

Se, quindi, la rilevanza delle tematiche qui considerate è evidente, a lasciare perplessi è l'esito cui la Corte costituzionale approda. La decisione di annullare un'elezione già avvenuta è, infatti, una scelta radicale, che rischia di minare la tenuta del sistema istituzionale nel suo insieme e la fiducia che gli elettori possono avere nella democrazia rappresentativa, la quale nel momento elettorale trova la sua prima e fondamentale fonte di legittimazione.

A sostegno possono essere addotti due ordini di ragione fondamentali.

Il primo è che una decisione così gravida di conseguenze avrebbe dovuto essere sorretta, quantomeno, da una motivazione più argomentata e strutturata. La Corte costituzionale rumena, invece, liquida in passaggi piuttosto succinti il tutto, senza fornire elementi puntuali a sostegno della propria prospettazione, ma facendo genericamente riferimento al fatto che sarebbero state accertate una serie di irregolarità nel processo elettorale.

La seconda ragione va ancora più a fondo del problema. Ci si chiede cioè se si possa davvero porre, come ragione a fondamento dell'annullamento di un'elezione, la distorsione del consenso politico quale frutto di una campagna manipolatoria *online*, anche qualora si disponga di prove inconfutabili in tal senso.

Cosa si intende, infatti, esattamente per manipolazione? Qual è la differenza tra una semplice influenza sul voto elettorale e una illegittima distorsione del consenso? E, ancora, anche qualora una manipolazione sia realmente avvenuta quali criteri dovrebbero essere seguiti per determinare che essa abbia inciso a tal punto sul voto dell'elettore da invalidare l'esito dell'intera elezione?

Diversamente, infatti, dall'ipotesi in cui si siano verificati brogli nel corso della consultazione (rispetto ai quali è più agevole accertare un collegamento oggettivo con i risultati elettorali), in questo caso si tratta di dimostrare che una campagna *online* avrebbe alterato la volontà degli elettori (concetto questo, peraltro, sfuggente), a tal punto da incidere sull'esito dell'elezione.

Trattasi di due passaggi argomentativi molto difficili da dimostrare e che, invece, la Corte risolve con (sorprendente) facilità.

Anche la violazione delle regole in tema di finanziamento è una motivazione scivolosa. Certamente in questo caso è più facile verificare un'inosservanza della legislazione in materia, ma ricollegarvi l'annullamento di un'intera elezione già svoltasi – per di più a soli due giorni dal secondo turno – è un salto concettuale drastico, nonché, come detto, non ben motivato dai giudici costituzionali rumeni.

Anche il passaggio sulla violazione della *par condicio* elettorale viene liquidato dalla Corte in poche righe, con formulazioni assertive. Né può sottacersi il fatto che, se ogni qual volta fosse accertata una violazione della pari concorrenza tra i candidati, si annullasse la relativa consultazione, allora il rischio che siano invalidate molte delle elezioni che periodicamente si tengono anche nelle democrazie più mature sarebbe enorme.

Non essendo allo stato dato sapere in che cosa siano esattamente consistite le presunte interferenze straniere nella campagna elettorale rumena, ad una prima lettura, la sentenza della Corte costituzionale appare, quindi, come una decisione radicale, che, pur muovendo da premesse condivisibili, si rivela foriera di più problematicità di quelle che si propone di risolvere.

L'annullamento di un'elezione già avvenuta è un fatto, infatti, di particolare gravità, che andrebbe assunto solo in casi-limite e con elementi inequivocabili a sostegno dell'invalidità del processo elettorale.

Ciò non significa affatto sminuire l'importanza dell'influenza del mondo digitale nella formazione del consenso. Al contrario, il caso della Romania dimostra tutta l'importanza di una regolazione attenta ed equilibrata di questi processi, che prevenga esiti così drammatici.

6. *Riflessioni conclusive*

La rivoluzione digitale pone una serie di sfide ed interrogativi in merito alla tenuta dei sistemi democratici.

In questo contesto, un ruolo decisivo è rivestito dalla formazione del consenso *online*: la profilazione, infatti, incide sulla possibilità di un'informazione libera del singolo cittadino-utente-elettore e, di conseguenza, sui presupposti stessi della rappresentanza e della partecipazione politica.

Dal tema della protezione dei dati personali degli utenti, alla creazione di *filter bubbles* ed *echo chambers*, all'emersione sulla scena pubblica di *leader* politici carismatici, nonché alla sempre maggiore influenza dei proprietari delle grandi piattaforme, innumerevoli sono le questioni di interesse per il diritto costituzionale. Ad essere toccate, alla radice, sono alcune delle fondamenta su cui i moderni ordinamenti democratici sono stati costruiti e plasmati nel corso del tempo.

Di fronte a queste sfide l'Unione europea, abbandonando un approccio iniziale fondato sull'auto-regolazione, ha dato vita, in breve tempo, ad un importante quadro normativo, approvando una serie di regolamenti particolarmente articolati. Essi rappresentano una prima risposta, parziale e tutta ancora da verificare, stante la necessità di un lungo processo di implementazione delle norme in questione e di adeguamento da parte dei grandi *gate-keepers*.

Trattasi di uno sforzo certamente lodevole, ma che lascia non pochi punti interrogativi aperti sul campo.

Ne è testimonianza quanto accaduto in Romania pochi mesi fa.

La decisione della Corte costituzionale di annullare l'esito di un'elezione già avvenuta sulla supposizione che la formazione consenso degli elettori sarebbe stata alterata, con la complicità di ingerenze straniere, da una campagna di disinformazione *online*, diretta a favorire un candidato e a distorcere il gioco democratico, dimostra tutta l'attualità e la serietà del tema.

Di qui, quindi, la necessità di aprire una riflessione sugli strumenti più adeguati per governare questi profondi fenomeni di trasformazione in corso, di modo da assicurare quanto più possibile un mercato della comunicazione *online* in cui sia preservato il discorso pubblico, inteso come "spazio istituzionale aperto a interazioni comunicative che, attraverso il conflitto tra opposte visioni del mondo, legittimano, sul piano sostanziale i meccanismi procedurali del circuito democratico-rappresentativo"[36].

Al fondo vi è la consapevolezza che, se tradizionalmente il costituzionalismo nacque con l'obiettivo di affermare i diritti e le libertà dei cittadini nei confronti del potere pubblico, oggi, nell'era digitale, le sfide più difficili riguardano, invece, la necessità che quegli stessi diritti, affinché possano dirsi effettivamente rispettati, siano garantiti nei confronti del potere, o meglio dei poteri, privati[37] da quelle stesse istituzioni pubbliche[38].

Il rischio è che, in assenza di interventi che individuino un bilanciamento tra interessi contrapposti, possano ripetersi anche in futuro esiti drastici come quello rumeno, in cui ad essere messa in dubbio è la stessa regolarità delle elezioni, quale momento fondante di ogni ordinamento democratico e rappresentativo.

---

[36] C. Caruso, *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, in *Quaderni costituzionali*, 3/2023, p. 544.

[37] Cfr. C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Milano, 1958, 29, nota 61.

[38] A. Barbera, *Articolo 2*, in G. Branca (a cura di), *Commentario della Costituzione. Artt. 1-12. Principi fondamentali*, Bologna-Roma, p. 50 ss.

Dati aperti e tutele collettive. Teorie e pratiche riequilibratorie delle asimmetrie

di **Luigi Prosia**

Abstract: I paradigmi sociali, etici e giuridici oggi dominanti si concentrano principalmente sugli interessi individuali e sui danni personali derivanti dalla violazione delle norme sulla protezione dei dati, risultando inadeguati a rimediare alle lesioni cagionate a gruppi omogenei di persone a seguito del trattamento massivo di grandi quantità di dati. La normativa europea più recente si sofferma sulle potenzialità connesse alla libera circolazione dei dati, nello specifico di quelli contraddistinti dalle cinque V (velocità, volume, varietà, veridicità, valore), non preoccupandosi *in toto* dei connessi profili di tutela. I big data analytics, invece, possono arrecare non solo un pregiudizio ai diritti fondamentali dei singoli, ma anche generare disparità di trattamento e discriminazioni indirette nei confronti di soggetti accomunati da caratteristiche simili, soprattutto per quanto concerne le pari opportunità di accesso all'istruzione e all'occupazione, nonché l'autodeterminazione nelle proprie abitudini di consumo. Essi toccano aspetti che vanno oltre le esigenze strettamente individuali tutelate dalle norme sulla protezione dei dati, rendendo necessaria, in tempi brevi, l'introduzione sia di meccanismi per riequilibrare le asimmetrie create dal e sul Web, sia di strumenti giurisdizionali per l'azione collettiva.

1. *Immersi nel ciberspazio, lì dove «information rules»*[1]

La digitalizzazione, con i suoi segnali, sensori e impulsi elettronici, sta comportando la messa in circolazione di un'incredibile quantità di dati che ci ri-

* Assegnista di ricerca in Filosofia del Diritto, Informatica giuridica, Biogiuridica – Università degli Studi di Roma Tor Vergata.

[1] Faccio mio il titolo di un libro degli economisti statunitensi Carl Shapiro e Hal Varian, che già nel 1999 rivelava il grande potere che di lì a poco avrebbe assunto il mondo dell'informazione.

guardano, ci descrivono e, in un certo senso, ci conoscono meglio di quanto immaginiamo, fino al punto di riuscire ad anticipare gran parte delle nostre decisioni quotidiane. Sono dati non solo precisi, intimi, correlabili e controllabili, ma anche così numerosi «da riempire tutte le biblioteche americane più di otto volte […] [mediante] un ciclo che si autoalimenta»[2]. Basti pensare che, per rappresentare la mole di contenuti attualmente disponibili sul Web, è necessario ricorrere allo zettabyte: un numero composto da un uno seguito da ventuno zeri. Tale cifra è destinata a crescere velocemente e senza interruzione a causa dello scambio giornaliero di informazioni, che si diffondono in forme eterogenee e provengono da fonti di diversa natura, seguendo spesso logiche frammentarie[3]. I sistemi integrati di telecomunicazione, del resto, intensificano la trasmissione, l'archiviazione e la ricerca di informazioni, tutte ormai potenzialmente pubblicabili, per giunta a costi relativamente contenuti. Ne deriva un flusso continuo di dati che plasma ogni livello della vita planetaria, condizionata sempre più «dalla velocità e dalla noncuranza dei frettolosi passaparola telematici»[4].

---

[2] L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017, p. 13. Sugli indiscutibili vantaggi dell'odierno sviluppo tecnico-scientifico, legati alla possibilità di processare una gran mole di dati senza dispendio di tempo e di energia, da un lato, e sulle istanze di tutela di nuovi diritti che questa elaborazione senza sosta inevitabilmente comporta, dall'altro, si veda A.C. Amato Mangiameli, *Intelligenza artificiale, big data e nuovi diritti*, in *Rivista italiana di informatica e diritto*, 1/2022, pp. 93-101.

[3] Per frammentazione si intende la dispersione delle informazioni personali di ogni utente sui social, che ogni clic, like o cuoricino contribuisce a spargere, da cui gli algoritmi ricavano automaticamente i suoi gusti commerciali e politici (cfr. M. Barberis, *Come Internet sta uccidendo la democrazia. Populismo digitale*, Milano, 2020, p. 159). Benché in questo libro si usino alternativamente le parole «dati» e «informazioni», sotto un profilo di stretta linguistica giuridica, va sottolineato che la prima ha un significato più ristretto, riferendosi a particelle elementari, non organizzate e non elaborate dall'uomo, pertanto non regolamentate e tutelate come le opere dell'ingegno (cfr. S. Aliprandi, *Open licensing e banche dati*, in *Informatica e diritto*, 1-2/2011, p. 26). Tuttavia, pur non presentandosi in sistemi strutturati, queste particelle ricevono lo stesso protezione, ma in forme certamente diverse dal paradigma della proprietà intellettuale.

[4] M.N. Campagnoli, *Informazione, social network & diritto*, *Dalle fake news all'hate speech online. Risvolti psicologici, profili giuridici, interventi normativi*, Milano, 2020, p. 78. Cfr. anche G. Granieri, *La società digitale*, Roma-Bari, 2006, pp. 28-29: «Al tempo dei media di massa e delle grandi distribuzioni editoriali […] era necessario effettuare una selezione dei contenuti prima di «investire» nella loro trasmissione […]. Oggi la società digitale ci sta mostrando un processo che si organizza su un principio esattamente contrario […] [e ciò] dal punto di vista della storia delle comunicazioni umane è una differenza di approccio paragonabile alla scoperta tolemaica in astronomia […] o all'accettazione del fatto che la terra sia rotonda e non piatta».

Tutto ciò rende le persone incredibilmente più esposte, dal momento che, pur di ottenere qualche like in più e sentirsi esistere come individualità assolute, rinunciano a custodire i propri segreti; inoltre, affidano la loro rappresentazione sociale a set di dati molteplici e diffusi, che ne modificano la stessa conoscenza e identità, tanto è vero che possiamo parlare di «corpo elettronico» contrapposto idealmente al «corpo fisico»[5]. Per opera delle Information and Communication Technologies (ICT), infatti, gli individui sperimentano inediti modelli esistenziali e mentali, che trasformano la realtà ultima delle cose, erodendo le barriere tra l'online e l'offline, e rendono l'«esserci» perfettamente sovrapponibile all'«essere connessi». Di conseguenza, la tecnologia cessa di essere un mero strumento (per calcolare, scrivere, archiviare, informare, educare) e diviene una «protesi che supera e perfeziona l'uomo e la natura»[6], visto che si vive, si cresce e si interagisce – con maggiore o minore successo e in modo più o meno sano – a seconda della conoscenza/informazione resa disponibile dai nuovi dispositivi: laptop, app e piattaforme che «oltrepassano la dialettica dei mezzi per raggiungere la retorica degli scopi»[7].

---

[5] Per una definizione di «corpo elettronico» (o «logico») generato dalle tante tracce lasciate in Rete dagli utenti, come pure dei rischi che esso solleva, si rimanda a S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, 2015, p. 270. Si parla anche di «datismo», una specie di religione che si giova della condivisione estrema di dati. Se, per l'umanesimo, le esperienze accadono dentro di noi, e proprio lì dovremmo trovare il significato di tutto quello che accade, per i «datisti», invece, le esperienze restano senza valore se non vengono condivise. «Vent'anni fa i turisti giapponesi erano lo zimbello del villaggio globale poiché andavano sempre in giro armati di macchine fotografiche e fotografavano qualunque soggetto gli capitasse a tiro. Ora tutti sono così […]. Il nuovo motto dice: "Se sperimentate qualcosa – registratelo. Se registrate qualcosa – caricatelo. Se caricate qualcosa – condividetelo"» (Y.N. Harari, *Homo Deus. Breve storia del futuro* (2016), trad. it., Milano, 2018, p. 472). Sulla Rete come ambiente geneticamente inadatto alla tenuta dei segreti, si vedano, di G. Ziccardi, *Diritti digitali. Informatica giuridica per le nuove professioni*, Milano, 2022, p. 81 e ss., e, per una trattazione ancora più ampia sul tema, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, 2015.

[6] I. Dionigi, *Osa sapere. Contro la paura e l'ignoranza*, Milano, 2019, p. 48. Secondo la teoria della mente estesa di A. Clark e D.J. Chalmers (*The Extended Mind*, in *Analysis*, vol. 58, 1/1998, pp. 7-19), i dispositivi tecnologici, come smartphone e computer, possono essere considerati persino parte integrante della nostra attività cerebrale. Integrandosi nei processi cognitivi, essi rendono sempre più sfumato il confine tra soggettività e ambiente digitale esterno, che amplifica la nostra percezione connettendoci costantemente a informazioni e reti globali.

[7] A.C. Amato Mangiameli, *Un nuovo bene: l'informazione*, in Ead., M.N. Campagnoli, *Strategie digitali. #diritto_educazione_tecnologie*, Torino, 2020, p. 32.

Al contempo, però, l'uomo è costantemente sfidato dal recupero e dall'elaborazione di dati tratti dalle proprie abitudini in Rete (dai siti Web visitati alle e-mail scambiate, dalle chat agli acquisti online), che possono essere registrate e computate con una precisione senza precedenti grazie all'azione di software così sofisticati da oltrepassare di gran lunga i limiti intellettuali e operativi propriamente umani[8]. L'obiettivo è senz'altro quello di raccogliere e immagazzinare quantità via via maggiori di informazione, per poi produrne di ulteriore e ancora più preziosa, poiché, come afferma Granger in *Fahrenheit 451*, a proposito delle attività di sorveglianza in una non meglio identificata società dispotica ove leggere o possedere libri è considerato reato, «non si sa mai quando l'essere a conoscenza di certi dati ti può essere utile!»[9]. E oggi, questa conoscenza risulta particolarmente utile alle aziende superstar della Silicon Valley, il cui modello economico-industriale «aspira a trasformare ogni gesto, ogni fiato, ogni relazione in un'occasione di profitto»[10].

All'orizzonte si profilano, allora, alcuni gravi rischi: se questa crescita esponenziale di dati, nelle mani di pochi giganti digitali, non viene accompagnata da una nostra altrettanto accresciuta attenzione – con cui evitare eccessi di fiducia e scelte sbagliate – le conseguenze, nonché le ripercussioni sulle nostre libertà e sui nostri diritti fondamentali, potrebbero essere spaventose. Sovraccaricando i nostri processi decisionali, l'opulenza informativa o «infobesità», ossia la costante e immensa disponibilità di informazioni sul Web, potrebbe paradossalmente mutare nel suo opposto, cioè nella drammatica scarsità di informazione, rendendoci, di fatto, indigenti. In mancanza di un'assidua dialettica fra attenzione sostenuta (su un determinato compito), selettiva (degli stimoli rilevanti) e suddivisa (fra più attività contemporaneamente), avere troppe informazioni equivale a non averne affatto. Si genera così l'illusione di conoscere quanto accade nel mondo e di prendere decisioni consapevoli mentre, in realtà, eventi di grande rilevanza – per esempio, in fatto di elezioni politiche, sicurezza nazionale o salute pubblica – si verificano quasi totalmente a nostra insaputa[11]. Insomma, troppa informazione, se recepita senza

---

[8] Su come le tecnologie digitali, al di là dei benefici apportati alle nostre vite, espongano a un potere incontrollabile, qual è quello della sorveglianza generalizzata, cfr. P. Tincani, *Controllo e sorveglianza*, in R. Brighi, S. Zullo (a cura di), *Filosofia del diritto e nuove tecnologie*, Roma, 2015, pp. 19-40; *Un altro dono dello spirito maligno. Nuova sorveglianza e comportamenti individuali*, in L. Pelliccioli (a cura di), *La privacy nell'età dell'informazione. Concetti e problemi*, Milano, 2016, pp. 19-63; *Sorveglianza e potere. Disavventure dell'asimmetria cognitiva*, in *Ragion pratica*, 1/2018, pp. 51-78.

[9] R. Bradbury, *Fahrenheit 451* (1953), trad. it., Milano, 1978, p. 175.

[10] É. Sadin, *La siliconizzazione del mondo. L'irresistibile espansione del liberismo digitale* (2016), trad. it., Torino, 2018, p. 13.

[11] Cfr. G. Saraceni, *Informational Opulence: Digital Divide and Poverty*, in

pensiero critico, non fa che generare confusione, arrivando persino a nascondere le questioni realmente fondamentali.

2. *Il concetto di identificazione/identificabilità*

Proiettando sempre più sé stesse nel mondo della Rete con le loro attività, interazioni e comunicazioni, le persone si ritrovano dunque «dataficate», cioè ridotte a una circolazione incessante di informazioni. Vivono vite da inforg, termine nato dalla fusione delle parole «informational» e «organism», che descrive la dimensione relazionale, sociale, comunicativa, economica e lavorativa degli individui dal punto di vista informazionale, ovvero come risultato dell'interazione tra la realtà materiale/analogica e quella immateriale/digitale, oltre che di una transizione continua dall'una all'altra. Tutto ciò avviene all'interno di un ambiente globale costituito da agenti biologici (noi), artefatti ingegneristici (le macchine) e appunto organismi interconnessi (noi + le macchine), che non rappresentano un'entità separata dall'uomo, bensì una sua vera e propria estensione tecnologica, capace di amplificare il corpo e i cinque sensi[12].

Se questo è il contesto di riferimento, l'individuazione della corretta nozione di dato personale diventa un nodo centrale per almeno due ordini di ragioni: teoriche, poiché gran parte della riflessione filosofica, politica, sociologica e giuridica gravita intorno alle tecnologie di trattamento dei dati, e pratiche, dal momento che l'applicazione della normativa europea a protezione dei dati personali non può prescindere dalla loro definizione[13]. Eppure, tale definizione, rinvenibile all'art. 4, punto 1, del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR), per cui è dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile (c.d. interessato)», appare fin trop-

---

Humanities and Rights Global Network Journal, vol. 3, 2/2021, pp. 179-198. Cfr. anche F. Rampini, *Rete padrona. Amazon, Apple, Google & co. Il volto oscuro della rivoluzione digitale*, Milano, 2014, p. 250, e G. Riotta, *Il Web ci rende liberi? Politica e vita quotidiana nel mondo digitale*, Torino, 2013, pp. 134-135: «La biblioteca del sapere online […] raddoppia in grandezza ogni undici ore. In una sola giornata Internet si moltiplica per due, in una settimana per quattordici. Trecento miliardi di e-mail, duecento milioni di tweet, due miliardi e mezzo di sms scambiati ogni giorno fanno rimbombare il tam-tam frenetico della tribù umana [eppure] […] la nostra saggezza non raddoppia in parallelo al Web e la nostra attenzione alle informazioni non cresce geometricamente».

[12] Ovvio qui il rimando a M. McLuhan, *Gli strumenti del comunicare* (1964), trad. it., Milano, 2023.

[13] Cfr. F. Cirillo, *La nozione di dato personale. Spunti di riflessione per un approccio interdisciplinare*, in *Ciberspazio e diritto. Rivista internazionale di informatica giuridica*, vol. 22, 1/2021, pp. 23-40.

po generica e onnicomprensiva. L'uso del termine «qualsiasi» è evidentemente finalizzato a scongiurare lacune nella tutela dei diritti e delle libertà inviolabili degli individui, nonché a garantire un adeguamento costante alla rapida evoluzione tecnologica[14].

La suddetta formulazione è tuttavia corredata da un elenco esemplificativo (non certo esaustivo) di possibili dati, che ne mitiga l'elevato coefficiente di astrazione e flessibilità: «si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online, o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». Sono tutti elementi, questi, da considerare *ex lege* dati personali. Un esempio di numero di identificazione offline è il codice fiscale, mentre un identificativo online può essere rappresentato dall'indirizzo IP[15].

Benché ogni rappresentazione di cose, fatti o persone, qual è per l'appunto l'informazione, possa potenzialmente ricadere nel campo di applicazione dell'art. 4 del GDPR, assurge al rango di dato personale soltanto quella specifica informazione concernente una persona fisica singolarmente individuata (distinguibile, non necessariamente da chiunque, ma almeno da qualcuno) o comunque

[14] È proprio questo l'assetto dell'intero impianto giuridico a tutela dei dati, scisso (ma in equilibrio) tra rigidità da una parte ed elasticità dall'altra, visto che poggia sulla congiuntura tra due differenti pilastri: «il primo, solido e fermo come una muraglia, e profondamente radicato nel tessuto normativo, mira a imporre regole uniformi e, soprattutto, ad assicurare l'attuazione delle medesime regole in tutta l'Unione; il secondo, mobile e flessibile come il braccio girevole di una gru o la piattaforma di un elevatore in movimento, assicura invece l'elasticità necessaria per trovare sempre il giusto punto di equilibrio con le tradizioni culturali dei diversi Paesi, con le caratteristiche dei loro ordinamenti giuridici, con le esigenze degli scambi internazionali», e consentire in ogni caso un livello di protezione «adeguato sia a garantire il diritto fondamentale dell'interessato che la tutela delle libertà in una società democratica» (F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, vol. II, Torino, 2016, p. 101 e ss.), nonché – aggiungerei – necessario a contrastare le continue derive dello sviluppo tecnologico in totalitarismo (e qualche volta in feticismo) dei dati.

[15] A tal proposito, il considerando 30 del GDPR specifica che «le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati (gli indirizzi IP), a marcatori temporanei (i cookie) o a identificativi di altro tipo (i tag di identificazione a radiofrequenza). Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle».

individuabile grazie all'ausilio di conoscenze aggiuntive. Ciò accade, per esempio, nell'ipotesi in cui il dato sia stato sottoposto a pseudonimizzazione (art. 4, punto 5, del GDPR). Quest'ultima, impedendo l'identificazione di una persona in assenza di specifiche chiavi di decodifica conservate separatamente e soggette a particolari misure di sicurezza, da una parte, riduce i rischi e le conseguenze negative per l'interessato e le sue libertà, dall'altra, aiuta titolari e responsabili del trattamento a rispettare gli obblighi di protezione dei dati[16]. Ciò nonostante, essendo la tecnica della pseudonimizzazione basata sulla semplice sostituzione di un dato identificativo con un «dato mascherato», dunque non immediatamente intelligibile, è soltanto reso più complesso il processo di identificazione univoca, ma resta sempre possibile risalire dal dato pseudonimo alla persona[17].

Il collegamento tra informazione e persona fisica su cui riposa il concetto di identificazione/identificabilità può, talvolta, essere stabilito con assoluta certezza, per esempio in presenza di un elemento altamente distintivo, che può essere diretto (il nome) o indiretto (il codice fiscale o l'indirizzo IP). Altre volte, invece, dipenderà da variabili contingenti, quali i costi e i tempi necessari per acquisire tanto le tecnologie disponibili al momento del trattamento, quanto quelle future che potrebbero consentire di forzare le misure di sicurezza a tutela dei dati e di sviluppare capacità di analisi, combinazione e raffronto tra plurime fonti informative, fino a raggiungere la totale identificazione dell'interessato. Si tratta di

[16] Cfr. considerando 28 del GDPR. In base all'art. 4, punto 7, dello stesso regolamento, il titolare è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali». Si tratta di una figura oggi centrale e strategica per assicurare una reale tutela del diritto fondamentale alla protezione dei dati personali, in qualsiasi contesto, sia esso reale o virtuale, dal momento che su di essa ricade la scelta, assolutamente discrezionale, delle modalità di attuazione dei principi e delle regole di fondo della normativa europea. Proprio il titolare, ai sensi e per gli effetti degli artt. 4, punto 8, e 28 del GDPR, può nominare, tramite contratto o diverso atto giuridico comunque di natura scritta, un responsabile che tratti i dati per suo conto, per esempio ai fini dell'erogazione di un servizio o a seguito di un appalto. Il titolare ha però la responsabilità di scegliere per tale incarico un soggetto/organismo che presenti garanzie sufficienti per mettere in atto le misure tecniche e organizzative prescritte dall'art. 32 del GDPR. Per un approfondimento dei concetti di titolare e di responsabile, nonché per individuarne i ruoli precisi, si vedano le *Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR* dell'European Data Protection Board adottate il 2 settembre 2020.

[17] Cfr. G. D'Acquisto, M. Naldi, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, 2017, p. 37 e ss.

casi in cui è ragionevolmente probabile che il titolare o un terzo adottino mezzi adeguati a conseguire tale identificazione[18].

Di converso, quando il rapporto di collegamento manchi *ab origine* oppure cessi successivamente, rendendo impossibile l'identificazione/identificabilità, il dato personale viene soppiantato dal dato anonimo o anonimizzato, che, non riferendosi più a una persona specifica o non avendo più alcuna connessione con essa, è privo delle garanzie giuridiche previste dal GDPR.

Va comunque rilevato che la linea di demarcazione fra dato anonimo e dato personale è mobile nel tempo, venendo condizionata (e tratteggiata volta per volta) da una molteplicità di fattori, primo fra tutti l'incessante avanzamento tecnologico, che offre strumenti sempre più performanti di identificazione, a discapito delle tecniche di «randomizzazione» e di «generalizzazione» comunemente adoperate per togliere valore personale ai dati. *Ergo*, l'esigenza di protezione degli individui sembra espandersi a dismisura, anche perché, in materia di trattamento dei dati, per darsi anonimato non è sufficiente l'assenza del nome anagrafico, come suggerirebbe l'etimologia del termine[19]. Si pensi al caso di un articolo di giornale che, pur omettendo nome e cognome per esteso di un soggetto coinvolto in una vicenda di cronaca, ne permetta comunque l'identificazione in ambito locale, tra le persone a lui vicine. D'altro canto, se la tutela venisse accordata sulla base della presenza del nome, si contraddirebbe l'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea, che riconosce il diritto alla protezione dei dati personali a ciascun individuo, senza esclusioni di sorta[20].

Malgrado la vasta portata del concetto di dato personale e della sua correlata tutela, qualcosa sembra sfuggire all'alveo della sua regolamentazione. Il riferimento è ai big data, ossia a tutte quelle informazioni (strutturate e non) provenienti dalle fonti più disparate (social media, portali di e-commerce, documenti elettronici, sensori, log di sistema, ecc.) e dal contenuto altamente eterogeneo (testuale, vocale, visivo, ecc.), che possono essere generate dal semplice agire

---

[18] Cfr. considerando 26 del GDPR e L. Bolognini, E. Pelino, C. Bistolfi, *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 43 e ss.

[19] Cfr. P. Bianchi, C. Cipolloni, *Anonimato* (voce), in A.C. Amato Mangiameli, G. Saraceni (a cura di), *Cento e una voce di informatica giuridica*, Torino, 2023, p. 25 e ss.

[20] «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

umano nella «datasfera»[21]. Problemi nell'applicazione dell'art. 4 del GDPR sorgono relativamente a questo ampio sciame informativo prodotto dai colossi del Web, a partire dal quale gli algoritmi compiono inferenze sulle qualità e sulle propensioni delle persone. Ne conseguono informazioni estremamente dettagliate, ma riferibili a un individuo specifico solo indirettamente, rendendo difficile la loro riconduzione alla definizione di dato personale con tutti gli annessi presidi giuridici. È esattamente questa la ragione che rende quanto mai opportuno ampliare l'orizzonte di tutela dei dati, concependo magari strumenti di ricorso collettivo, per evitare che questa tutela diventi sostanzialmente inefficace, e continuare a difendere gli individui da lesioni intime e significative del loro essere[22]. Dinanzi all'elaborazione di big dataset per rintracciare linee di tendenza riferibili a gruppi di individui con caratteristiche omogenee (per esempio, appassionati di running, frequentatori di una certa tratta aerea, abitanti di uno stesso quartiere, ecc.), è quasi inevitabile che la persona singola, come soggetto distinto da tutti gli altri, perda rilevanza e centralità.

3. *Dai monopoli agli «open big data»: una prima proposta di soluzione*

Volendo riflettere sulle possibili ricadute positive connesse all'odierna «protocollazione» della vita, misurata e quantificata in modo ubiquo attraverso il medium trasparente e affidabile dei dati, va sottolineato che questi, quando non vengono utilizzati per filtrare pregiudizi di natura emotiva o culturale, si stagliano come risorse essenziali e strategiche per generare progresso a ogni livello. Non è casuale che, di fronte alla riontologizzazione e riepistemologizzazione del mondo causata dall'avvento di Internet[23] (il mezzo di comunicazione più rapido, economico ed efficiente, ma non sempre il più sicuro), le big tech fondano i loro sistemi di business proprio sui dati, compiendo sforzi per assicurarsene il dominio esclusivo. Il loro valore, infatti, non si esaurisce con l'uso, anzi aumenta man mano che vengono utilizzati, grazie alle combinazioni sempre diverse rese possibili dalle inedite capacità di stoccaggio e analisi (o tecniche di data mining) degli algoritmi[24]. È come se durante il processo di knowledge discovery (o scoperta di

---

[21] Cfr. J.S. Bergé, S. Grumbach, V. Zeno-Zencovich, *The «Datasphere», Data Flows Beyond Control, and the Challenges for Law and Governance*, in *European Journal of Comparative Law and Governance*, vol. 5, 2/2018, pp. 144-178.

[22] Cfr. S. Rodotà, *Il diritto*, cit., p. 396.

[23] Cfr. L. Floridi, *Il verde e il blu. Idee ingenue per migliorare la politica*, Milano, 2020, p. 23 e ss.

[24] «Vere gemme intellettuali delle superstar digitali e dei loro incredibili ingegneri, una proprietà intellettuale che vale la pena custodire meglio di quanto il Cremlino

conoscenza) i dati si animassero, sprigionando tutta la loro ricchezza informativa in base all'ampiezza e alla velocità con cui vengono scambiati e riutilizzati in collegamenti dinamici capaci di oltrepassare barriere tecniche, giuridiche ed economiche[25]. Da questo punto di vista, la frequenta metafora dei dati come petrolio – estratti in forma grezza, lavorati e poi trasformati in altro – appare poco pertinente: l'informazione digitale non la si perde né distrugge con l'uso, essendo modulare e moltiplicabile in copie, oltre che ininterrottamente raffinabile. Sarebbe più corretto parlare di beni non rivali che, non consumandosi come il petrolio, possono essere adoperati contemporaneamente da più persone; non più solo quelle appartenenti ai ranghi del «big business» (il mercato tecnologico)[26] o alle strutture del controllo governativo, alcune volte persino in loro sottaciuta coalizione[27].

---

custodisca la salma di Lenin» (T. Ramge, V. Mayer-Schönberger, *Fuori i dati! Rompere i monopoli sulle informazioni per rilanciare il progresso* (2020), trad. it., Milano, 2021, p. 28), gli algoritmi consistono in espressioni matematiche e in precise istruzioni tra loro artatamente combinate per individuare associazioni e tendenze, ed estrarre dinamiche a partire dai dati inseriti in un sistema informatico. Nondimeno, su come celino meccanismi di alterazione dell'informazione e di condizionamento dell'azione, al punto da compromettere la tenuta dei sistemi democratici, soprattutto quando i dati di partenza sono poco chiari o errati, si rinvia a A.C. Amato Mangiameli, *Algoritmi e big data. Dalla carta sulla robotica*, in *Rivista di filosofia del diritto*, 1/2019, pp. 107-124.

[25] Quanto al profilo tecnico, il grado di interoperabilità dei dati è strettamente connesso alla loro classificazione secondo il modello «5 stars» di Tim Berners-Lee, il fondatore di Internet, che parte dai data raw (o dati grezzi) per arrivare ai linked open data, cioè svincolati dalla fonte, caratterizzati da elevata granularità, processabili automaticamente e contenenti addirittura link a ulteriori dati (cfr. T. Agnoloni, *Dall'informazione giuridica agli open data giuridici*, in G. Peruginelli, M. Ragona (a cura di), *L'informatica giuridica in Italia. Cinquant'anni di studi, ricerche ed esperienze*, Napoli, 2014, pp. 581-602). Relativamente alla dimensione giuridica ed economica, i dati possono essere utilmente rilavorati e ricombinati se rilasciati gratuitamente in formato non proprietario o con licenze di tipo aperto, come le Creative Commons, a parte qualche limitazione necessaria per motivi di privacy o sicurezza (cfr. B. Cunegatti, *Le licenze creative commons*, in G. Finocchiaro, F. Delfini (a cura di), *Diritto dell'informatica*, Torino, 2014, pp. 641-663).

[26] L'espressione è stata usata da Lawrence Lessig in un'intervista del 14 giugno 2013 su *billmoyers.com* dal titolo *Big Brothers's Prying Eyes*, e citata in G. Ziccardi, *Internet*, cit., p. 63 e ss.

[27] Ovvio è qui il rimando al Datagate, con cui Edward Snowden ha portato alla luce l'esistenza di accordi stipulati tra il Governo degli Stati Uniti e alcuni colossi privati (Google, Skype, Yahoo, ecc.) per scandagliare le enormi quantità di dati che transitano negli strumenti digitali di uso quotidiano e aumentare così la sicurezza dei cittadini, soprattutto dopo l'attentato dell'11 settembre. Questo ha comportato, in tal

Eppure, benché dai dati si possano estrarre di continuo nuove indicazioni e prospettive senza ridurne affatto la pregevolezza, queste attualmente si traducono in un vantaggio per i soli monopolisti digitali consolidati, a scapito di chi fornisce i dati intenzionalmente o inavvertitamente. Trattasi di una disparità che potrebbe essere superata rendendo il loro flusso libero e aperto a tutti (cittadini, Governi, organizzazioni internazionali, imprese, ecc.)[28]. In tal modo, specie quelli caratterizzati da grandi volumi, velocità, varietà e facile visualizzazione (i big data), potrebbero accrescere, accanto al profitto di pochi, il benessere di molti, configurando anche per i secondi un sicuro investimento in termini economici e sociali, senza dimenticare che

> le risultanze [del trattamento di dati] che oggi appaiono di nessuno o di scarso interesse potrebbero improvvisamente assumere importanza vitale […] in ragione di eventi futuri non prevedibili – come, ad esempio, una pandemia, un cataclisma naturale o uno stravolgimento delle borse – o di ulteriori sviluppi delle tecnologie informatiche[29].

La possibilità di ottenere dall'elaborazione dei dati previsioni sensate e statisticamente consistenti, sulle quali calibrare i vari processi decisionali, può essere di stimolo all'innovazione e alla crescita, tanto nel settore privato, quanto in quello pubblico. È qui che gioca un ruolo cruciale la trasformazione dei dati: da semplici simboli o segnali, privi di particolare utilità se considerati isolatamente, a «informazione semantica», ovvero dati dotati di senso. Questo processo si realizza quando i dati stessi vengono interpretati e contestualizzati in modo da acquisire significato e divenire strumenti validi per la comprensione dei fenomeni e il supporto alle decisioni, contribuendo così a ridurre il grado d'incertezza o il livello di sorpresa rispetto alla realtà[30].

---

caso, un controllo indiscriminato e, a tratti, inquietante delle autorità sui consociati. In altre ipotesi, invece, la conoscenza dei dati è divenuta uno strumento di esercizio della sovranità popolare, permettendo ai governati di scovare menzogne e segreti dei governanti (si veda il caso di WikiLeaks, un'organizzazione di attivisti che divulga documenti riservati, coperti da segreto di Stato, militare, bancario o industriale, per portare alla luce comportamenti eticamente scorretti di Governi o aziende).

[28] Cfr. V. Mayer-Schönberger, T. Ramge, *Reinventare il capitalismo nell'era dei big data* (2017), trad. it., Milano, 2018, tra le prime opere a promuovere la condivisione dei dati a tutti.

[29] G. Saraceni, *Big data* (voce), in A.C. Amato Mangiameli, Id. (a cura di), *Cento*, cit., p. 42.

[30] Sull'ampia varietà di teorie proposte nella ricerca filosofica per chiarire il concetto, ancora sfuggente, di informazione – alcune basate su un approccio puramente matematico alla codifica e trasmissione dei dati, altre incentrate sul loro valore

Nel primo ambito, i sistemi di analytics permetterebbero di ottimizzare le prestazioni, incrementare la produttività, abbassare i costi e, in generale, sviluppare forme di aziendalità più significative. L'art. 41 della Cost., dedicato all'iniziativa economica, compresa quella privata, non verrebbe violato dall'apertura generalizzata dei dati, rappresentando quest'ultima un'infrastruttura essenziale per garantire mercati concorrenziali e contendibili, come pure per scongiurare abusi di posizione dominante basati proprio sul possesso esclusivo dei dati, arrivando persino a obbligare i detentori a fornirli ai concorrenti[31]. Così facendo, cadrebbero le attuali disparità di azione, visto che non converrebbe più a nessuno accaparrarsi un accesso assoluto ai dati in un contesto economico partecipato e strumentale allo sviluppo di attività e applicazioni fruttuose per tutti.

La condivisione dei dati, *prima facie*, potrebbe configurare una perdita di potere economico per le grandi corporation, ma a ben guardare non ne contrasterebbe l'ascesa: le possibilità di guadagno sono in gran parte legate alle tecniche utilizzate per estrarre conoscenza dai dati, più che ai dati stessi. Per questa ragione, da un lato, il loro valore risulterebbe quasi nullo in mancanza di software in grado di processare in tempo ragionevole le molteplici informazioni racchiuse in essi; dall'altro, affinché la loro fruizione sia davvero diffusa e plurale, dovrebbe riguardare anche la conoscenza degli algoritmi sottesi alla loro analisi. Ma ciò, nella realtà dei fatti, si mostra di difficile realizzazione: i data baron ne rivendicano il diritto di proprietà esclusiva, trattandosi di un'area decisiva per il dominio tecnologico, perché frutto della genialità di quei data scientist che, prima di molti altri, hanno intuito le innumerevoli potenzialità insite nel processamento ininterrotto di masse sterminate di dati.

Inoltre, i meccanismi della Rete hanno l'effetto indiretto di favorire sistematicamente chi è già forte. È dimostrato, infatti, che per migliorare un determinato servizio, l'implementazione degli algoritmi dovrebbe andare di pari passo con l'incremento dei dati su cui vengono applicati, il che mette in difficoltà i nuovi entranti nel mercato, privi dei mezzi necessari per procurarsi un set di informazioni paragonabile a quello degli agenti dominanti[32]. Senza contare che gli utenti sono attratti da aziende già affermate, che sanno migliorare costantemente i loro servizi per adattarli alle esigenze dell'utenza stessa, scoraggiando in tal modo il

---

conoscitivo –, si veda L. Floridi, *Information: A Very Short Introducion*, Oxford, 2010, e *The Philosophy of Information*, Oxford, 2002.

[31] Cfr. V. Zeno-Zencovich, G. Giannone Codiglione, *Ten Legal Perspectives on the* «*Big Data Revolution*», in *Concorrenza e mercato*, 23/2016, p. 36 e ss.

[32] Cfr. M.F. De Tullio, *La privacy e i big data verso una dimensione costituzionale collettiva*, in *Politica del diritto*, 4/2016, p. 684 e ss.

passaggio verso nuovi operatori, i quali, peraltro, sono incapaci di sostenere i costi di switching (o transizione).

Nell'ambito pubblico, invece, la posta in gioco va oltre il mero potere economico e riguarda più da vicino valori preziosi quali la sicurezza dei cittadini, il contrasto alle discriminazioni, la prevenzione delle disuguaglianze, la salvaguardia della giustizia e dell'equità, lo sviluppo del sapere collettivo[33]. Indirizzando i dati verso il bene di tutti, numerosi comparti pubblici (sanità, trasporti, ambiente, energia, ecc.) potrebbero beneficiare di reali opportunità di cambiamento legate a una più efficiente e personalizzata fornitura dei servizi, a provvedimenti più accurati e tempestivi, come anche a un considerevole risparmio erariale[34].

Un uso sinergico di open data e big data, *rectius* di «open big data», potrebbe altresì aprire inediti scenari di trasparenza e collaborazione fra Stati, fra aziende e fra Stati e aziende, oltre a favorire una partecipazione consapevole, proattiva e reattiva da parte dei cittadini alla crescita sociale e civile del Paese, in direzione di una maggiore sussidiarietà orizzontale tra pubblico e privato[35]. Una volta diffusi, questi «super data» andrebbero incontro a una sorta di sanatoria (con concessione di licenza al loro riutilizzo) idonea a rafforzare il peso degli individui nelle decisioni che li riguardano[36]. L'accesso ai dati consentirebbe loro di organizzare più razionalmente la propria quotidianità: ad esempio, sarebbe più facile conoscere

---

[33] Sul punto, si rinvia a P. Lévy, *L'intelligenza collettiva. Per un'antropologia del cyberspazio* (1994), trad. it., Milano, 2002.

[34] Vedasi in tal senso l'Opinion dell'European Data Protection Supervisor dal titolo *Towards a New Digital Ethics: Data, Dignity and Technology*, n. 4 dell'11 settembre 2015. La convinzione dell'Unione circa le potenzialità economiche e sociali insite nei dati emerge anche da due comunicazioni della Commissione europea: *Dati aperti. Un motore per l'innovazione, la crescita e una governance trasparente*, n. 882 definitivo del 12 dicembre 2011; *Verso una florida economia basata sui dati*, n. 442 definitivo del 2 luglio 2014. Più di recente, l'ambizione dell'Ue di rendere la propria economia la più attrattiva, dinamica e sicura del mondo, promuovendo la riutilizzazione dei dati, potenziandone i meccanismi di condivisione e rafforzando la fiducia negli intermediari dei dati stessi, è emersa dalla comunicazione *Una strategia europea per i dati*, n. 66 definitivo del 19 febbraio 2020, sulla cui base è stato poi emanato il *Regolamento Ue n. 868/2022 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento Ue n. 1724/2018* (il c.d. Data Governance Act).

[35] Cfr. la comunicazione della Commissione europea *Costruire un'economia dei dati europea*, n. 9 definitivo del 10 gennaio 2017, che propone partenariati pubblico-privato per una cooperazione strategica sui dati, creando incentivi alla condivisione e agili meccanismi di trasferimento di tecnologie e conoscenze, collaborando a tal fine con istituti di ricerca e università.

[36] L'espressione «super data» è presa da M. Orefice, *I big data. Regole e concorrenza*, in *Politica del diritto*, 4/2016, p. 713.

il piano asili comunale, le strade chiuse al traffico o le linee tramviarie sospese. Tale accesso dovrà però rimanere uno strumento per informare o aiutare a capire. «Se così non sarà, i big data avranno sovvertito l'essenza stessa della natura umana, ovvero il pensiero razionale e la libera scelta»[37]. Ciò accade quando lo sviluppo tecnologico supera la nostra capacità di controllo, tradendo la promessa insita nell'espressione «società della conoscenza» incline all'ammirabile filosofia openness.

4. *Negoziazioni e tutele collettive come stretta definitiva*

Da quanto sopra esposto appare chiaro che soltanto conquistando il traguardo dell'universale condivisione dei dati e reimpostando, di conseguenza, i rapporti di potere, le istituzioni statali, le associazioni no profit e, nel complesso, la società civile potrebbero affrontare realmente le più diffuse problematiche ambientali, economiche, sociali e persino umanitarie. Viceversa, una distribuzione ineguale di informazioni/conoscenze sarà sempre di ostacolo all'avanzamento del progresso sociale, scientifico ed economico, inteso nell'ottica di uno sviluppo inclusivo, democratico e sostenibile. Del resto, se il Web rappresenta ormai lo spazio di tutte le cose, alimentato dai tanti dati immessi nel suo sottosuolo, è proprio da queste radici che in futuro potranno germogliare nuove piante del sapere.

Eppure, affinché la condivisione dei dati possa servire interessi generali e apportare un effettivo beneficio alla comunità, essa necessità di qualcosa di più: deve essere accompagnata da forme collettive sia di gestione dei dati stessi, sia di tutela dei relativi diritti. Ciò significa che ogni individuo dovrebbe essere messo concretamente nelle condizioni di partecipare, in maniera paritaria, alle negoziazioni relative alla circolazione, al trasferimento, alla redistribuzione e al riutilizzo dei dati, nonché di controllarne l'adempimento ed eventualmente denunciarne le violazioni[38]. Diversamente, le asimmetrie cognitive – manifeste nei tentativi di prevedere i comportamenti, nella ricomposizione della persona a partire da like e cookie, nelle trattazioni inique celate dietro richieste formali di consenso e di accettazione di condizioni generali – finirebbero per limitare la possibilità di autodeterminazione, non solo per il singolo interessato, ma anche per i membri del suo stesso gruppo sociale. Questi ultimi, infatti, potrebbero subire previsioni discriminatorie basate esclusivamente sull'appartenenza al gruppo, senza riconoscersi in esse. Presumere, come fanno i sistemi di IA, che gli individui rispondano ai medesimi stimoli e si comportino in modo identico per via della loro appar-

---

[37] V. Mayer-Schöngerger, K. Cukier, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e che già minaccia la nostra libertà*, trad. it., Milano, 2013, p. 261.

[38] Cfr. M.F. De Tullio, *La privacy*, cit., p. 675 e ss.

tenenza sociale, può portare a disparità di accesso (ad esempio, all'occupazione o all'istruzione) difficilmente contrastabili con i principi e gli strumenti del GDPR[39]. Questo vuoto di tutela potrebbe essere colmato dando rilievo, attraverso forme di collective redress, a interessi non immediatamente riferibili a persone determinate o determinabili nella loro univocità, ma comunque meritevoli di protezione.

Misure di questo tipo, che richiedono uno intervento legislativo specifico, potrebbero ispirarsi a quanto previsto dal diritto internazionale per la tutela delle minoranze, comportando diversi vantaggi in termini di identificazione e determinazione del danno. Ciò permetterebbe di superare le difficoltà legate al riconoscimento dei gruppi come soggetti giuridici autonomi, ivi compresa la loro legittimazione ad agire in sede giurisdizionale. Si pensi, per esempio, alle problematiche che potrebbero sorgere qualora un gruppo volesse presentare un ricorso per tutelare le proprie prerogative e, in assenza di un rappresentante legale precostituito, fosse necessario stabilire se debbano partecipare o meno in giudizio tutti i suoi membri. Questa difficoltà risulta particolarmente evidente per quei gruppi che non preesistono, ma si formano dinamicamente attraverso l'elaborazione algoritmica. Una possibile soluzione potrebbe essere rappresentata da organizzazioni indipendenti, designate preventivamente per intentare azioni legali nell'interesse di una pluralità di individui accomunati da certe caratteristiche. Tuttavia, tali enti dovrebbero essere privi di scopi di lucro, dotati di adeguate risorse finanziarie, competenze giuridiche e umane, e avere obiettivi statutari strettamente connessi alla tutela dei diritti violati[40].

---

[39] Per comprendere come l'abuso di big dataset possa indirettamente condurre a effetti discriminatori, si pensi al caso di un'impresa che indirizzi le proprie politiche di assunzione in base ai risultati di elaborazioni algoritmiche, che evidenziano un fatto: i dipendenti che vivono vicino al luogo di lavoro vi rimangono più a lungo rispetto a quelli che risiedono lontano. Una predizione, questa, che potrebbe entrare in conflitto con la parità di trattamento nell'offerta di lavoro, qualora le diverse zone di una città presentino composizioni etniche differenti.

[40] Sul punto, si rimanda a G.M. Ruotolo, *I dati non personali: l'emersione dei big data nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 1/2018, p. 109 e ss., il quale sottolinea come l'attenzione ai gruppi, sorta nel secondo dopoguerra per reagire ai regimi totalitari, sia via via passata in secondo piano nella prassi applicativa della Corte europea dei diritti dell'uomo, che, nel contesto dell'art. 8 posto dalla Convenzione europea dei diritti dell'uomo (CEDU) a tutela della vita privata, tende a scoraggiare i ricorsi di gruppi o persone giuridiche, nonostante l'art. 34 CEDU riconosca la legittimazione ad agire a «ogni persona fisica, ogni organizzazione non governativa o gruppo di privati che pretenda di essere vittima di una violazione da parte di una delle Alte Parti Contraenti dei diritti riconosciuti nella Convenzione o nei suoi protocolli». Si riscontra una timida apertura, e dunque una giurisprudenza residuale, nell'ipotesi in

Se, invece, l'autonomia contrattuale del singolo non venisse supportata – e, in alcuni casi, anche limitata – da negoziazioni e tutele di matrice collettiva, si rischierebbe il paradosso per cui la «massa cieca» finirebbe per dettare legge[41], senza che i dati fossero veramente accessibili a tutti. La comunità di riferimento rimarrebbe quasi sempre esclusa dalla loro gestione operativa e dal controllo strategico, perpetuando così le attuali disuguaglianze.

Allo stesso modo, per evitare che i dati, anziché rappresentare un supporto decisionale, diventino strumenti di controllo e repressione[42], il momento attuativo della loro apertura andrebbe affidato a un organo collegiale sovranazionale, equidistante sia dagli enti governativi (il settore pubblico), sia dai grandi giocatori dell'attuale mercato di Internet (il settore privato). Al contempo, dovrebbe essere garantita a chiunque la possibilità di appellarsi al potere giurisdizionale. Un tale approccio consentirebbe di vigilare su tutti coloro che potrebbero avere interesse a orientare il governo dei dati verso direzioni diverse da quelle facenti leva sulla condivisione, contribuendo, di riflesso, a un'inedita espansione del diritto alla conoscenza.

C'è bisogno, allora, di un accesso ai dati sempre più ampio, acefalo e acentrico, ovvero caratterizzato da una titolarità diffusa, con una gestione collettiva sia della loro disponibilità, sia della protezione dei diritti a essi correlati. Questo vuol dire che la capacità di disporre dei dati e di tutelarne l'uso non dovrebbe essere esclusivamente individuale, ma anche collettiva, fino al punto di poter sostituire o addirittura contrastare la volontà del singolo, laddove necessario[43]. L'intento è

---

cui gli interessi del ricorrente collidano con quelli del gruppo o della persona giuridica, oppure li inglobino. Diversamente, quando è stato presentato ricorso come semplici appartenenti al gruppo, e non anche come diretti interessati, la Corte ha sempre ribadito l'impossibilità di instaurare le cc.dd. *actio popolaris*, con cui proteggere gli interessi di altri o della persona giuridica nel suo complesso, rigettando o dichiarando inammissibile il ricorso stesso. Irricevibili sono anche i ricorsi che hanno per oggetto danni futuri o ipotetici (*in abstracto*), cioè quando esiste solo il rischio di essere colpiti dalla violazione contestata. Discorso a parte va fatto per i ricorsi cumulativi che, limitandosi a riunire più ricorrenti, ognuno dei quali invoca una propria posizione giuridica autonoma, seppure analoga a quella degli altri, sono certamente consentiti.

[41] Cfr. F. Faini, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Milano, 2019, p. 411.

[42] Cfr. M.F. De Tullio, *La privacy*, cit., p. 692.

[43] Questa necessità di protezione voluta ed esercitata dalla collettività a favore della collettività stessa, che viene raccomandata anche dall'European Data Protection Supervisor (opinion n. 8 del 23 settembre 2016, *The Coherent Enforcement of Fundamental Rights in the Age of Big Data*), emerge in qualche maniera anche dall'art. 80, par. 2, del GDPR, secondo cui gli Stati membri possono prevedere che un organismo, un'organizzazione o un'associazione, indipendentemente dal mandato dell'interessato, abbia il diritto di proporre reclamo all'autorità di controllo competente e di chiamare

ridurre l'attuale asimmetria informativa (e non solo) tra organizzazioni e aziende, individui e clienti, Stato e società, favorendo simultaneamente una corretta transizione al digitale basata sugli «open big data» per tutti, come l'Europa sostiene politicamente da alcuni anni. In questa direzione muovono le parole pronunciate nel febbraio 2020 dalla presidente della Commissione europea, Ursula von der Leyen, in occasione dell'apertura dei lavori dedicati alle iniziative di strategia digitale:

> vogliamo che i dati siano disponibili per tutti, sia pubblici sia privati, sia grandi che piccoli, siano essi startup o giganti del Web. […] Essendo parte in causa, i grandi attori digitali commerciali devono accettare la loro responsabilità, anche permettendo agli europei di accedere ai dati che raccolgono[44].

5. *Se il consenso non basta… perché non tornare alle origini?*

Oltre che come rimedio contro l'intrinseca natura predittiva dei big data, le negoziazioni e le tutele collettive potrebbero costituire una soluzione anche nei confronti dell'aggressività commerciale dei giganti della Rete, che spesso induce gli individui a barattare i propri dati per convenienza, mossi da egoismo individuale e non certo per utilità sociale. Ciò svuota di contenuto strumenti preventivi come l'informativa e il consenso, che la normativa europea affida agli individui stessi. È in questo modo che pochi soggetti privati aumentano sempre più il loro dominio, a discapito della parità contrattuale, fino al punto di riuscire a vincolare al proprio sistema di regole anche soggetti terzi non contraenti. Per esempio, se un utente è iscritto a un social e pubblica una foto con un'altra persona che non lo è, indicando dove sono stati e cosa hanno fatto, quest'ultima viene comunque coinvolta. Quando accederà a Internet, infatti, si troverà indirizzata, in conseguenza dell'incrocio dei dati, verso siti o contenuti richiamati da quella foto.

Questi pochi soggetti privati, in sostanza, arrivano a detenere un potere quasi normativo, ostacolabile in due modi: da un lato, vietando loro determinate operazioni lesive dei valori costituzionali, anche se vi è il consenso degli utenti (si pensi all'obbligo di iscrizione a una newsletter, alla sincronizzazione dei contatti o all'accettazione di e-mail pubblicitarie come condizione di accesso a un servizio); dall'altro, consentendo alcune altre operazioni in assenza di consenso,

---

in giudizio ora la stessa autorità (art. 78 del GDPR), ora il titolare o il responsabile del trattamento (art. 79), qualora ritenga che l'interessato sia stato leso nei suoi diritti a seguito di un trattamento illecito di dati.

[44] *Shaping Europe's Digital Future: Op-Ed by Ursula von der Leyen, President of the European Commission*, Bruxelles, 19 February 2020 (trad. mia).

quando queste siano giustificate da interessi pubblici, come la tutela della salute o della sicurezza, la lotta alla criminalità o il mantenimento dell'ordine costituito.

In effetti, ai sensi del GDPR, il marketing diretto e i trattamenti per finalità pubblicitarie sono permessi anche senza l'accettazione dell'interessato, sotto la copertura di «interessi legittimi» *ex* art. 6, par. 1, lett. *f*, purché «non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali» (considerando 47). Tuttavia, questa impostazione del GDPR risulta debole dal punto di vista della parità negoziale tra le parti, favorendo il contraente già più forte. Non deve quindi sorprendere se la libera, specifica, informata e inequivocabile espressione del consenso, anche quando è posta come condizione di accesso a una piattaforma o a un servizio di cui un utente ha bisogno, venga considerata unicamente in senso descrittivo e non anche prescrittivo, come suggeriscono il considerando 43 e l'art. 7, par. 4, che presumono il consenso non liberamente prestato se imposto come indispensabile per la stipula di un contratto senza esserlo realmente. Sarebbe invece più efficace vietare con norma cogente che i fornitori condizionino la fruizione di un servizio alla cessione di più informazioni di quante ne siano effettivamente necessarie.

Un catalizzatore fondamentale per garantire maggiore equità tra le parti può essere individuato nel recentissimo Regolamento Ue n. 2023/2854 (il c.d. Data Act), che rappresenta l'ultimo tassello dell'ampio quadro normativo volto a guidare la trasformazione digitale dell'Unione entro il 2030.

Benché non manchino le voci di dissenso di chi sostiene che, per frenare il potere dei giganti tecnologici statunitensi e cinesi, si stiano in realtà sovraccaricando di regole le piccole e medie imprese, questo nuovo intervento, deliberato con l'obiettivo di promuovere la condivisione dei dati tra individui, aziende e settore pubblico, potrebbe portare diversi benefici. Da un lato, consentirebbe ai consumatori di prodotti e servizi della società dell'informazione (come dispositivi IoT, macchinari industriali, veicoli smart, ecc.) di accedere a un numero maggiore di informazioni generate da ciò che utilizzano, e anche di comunicarle liberamente a terzi, nel rispetto dei segreti commerciali, preservando la riservatezza dei dati mediante misure specifiche, quali clausole contrattuali tipo, accordi o protocolli rigorosi, norme tecniche e codici di condotta (artt. 3 e 5); dall'altro, permetterebbe agli enti pubblici – ossia agli organismi dell'Unione e alle autorità nazionali, regionali e locali degli Stati membri – di sfruttare i dati detenuti dai grandi player della Silicon Valley per rispondere adeguatamente alle emergenze più disparate (art. 14). Si fa riferimento a situazioni eccezionali – come epidemie, calamità naturali, catastrofi di origine antropica e incidenti di cibersicurezza – che abbiano un impatto negativo sulle condizioni di vita della popolazione e sulla stabilità economica e finanziaria (art. 2, punto 29).

Per rendere l'accesso e la condivisione diritti effettivi, il Regolamento, oltre a invitare genericamente le autorità competenti a promuovere attività volte a

migliorare «l'alfabetizzazione in materia di dati»[45], impone che gli utenti-consumatori, prima di concludere un contratto (di acquisto, locazione o noleggio di un prodotto o fornitura di un servizio correlato), ricevano un'informativa chiara e dettagliata che li renda consapevoli del tipo, formato e volume stimato dei dati raccolti, nonché delle modalità di accesso, reperimento ed eventuale cancellazione dei dati stessi (art. 3, parr. 1 e 2)[46].

Specularmente al diritto di accesso degli utenti, sorge per i titolari l'obbligo di progettare e produrre prodotti connessi a Internet e servizi collegati che garantiscano tale diritto by design (per impostazione predefinita), come pure il suo esercizio in maniera facile, sicura, gratuita, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e, ove pertinente e tecnicamente possibile, in modo diretto (art. 3, par. 1). Se, nonostante l'impostazione predefinita, l'accesso risulta impossibile, i titolari, su semplice richiesta, devono mettere prontamente a disposizione i dati, affinché possano essere utilizzati senza indebito ritardo e «con la stessa qualità» con cui sono stati generati o elaborati, dunque senza degradazioni intenzionali o vincoli tecnici che ne limitino il valore (art. 4, par. 1); e questo, salvo limitazioni o divieti contrattuali, ad esempio per motivi di salute, sicurezza o protezione delle persone fisiche (art. 4, par. 2). Gli stessi requisiti valgono per la condivisione dei dati con terze parti, come i partner commerciali. L'obiettivo, in questo caso, è favorire la concorrenza, anche mediante accordi volontari tra imprese, scongiurando pratiche discriminatorie tra chi detiene i dati e chi li riceve, e massimizzando al contempo le possibilità di sviluppo legate proprio alla condivisione.

Tutto ciò potrebbe segnare il ritorno, se non all'Internet primitivo – inteso come una dimensione comunitaria e inclusiva, priva di rapporti proprietari –, almeno ai valori di libertà, cooperazione, neutralità e sperimentazione che ne avevano caratterizzato gli inizi e che ispirano tuttora la cultura hacker; valori che andrebbero volontariamente perseguiti dallo sforzo di una comunità sufficientemente compatta da approfittare in modo decentrato e creativo delle ancora inesplorate possibilità offerte dalla Rete e dalla messa in comune dei dati.

---

[45] Tale alfabetizzazione dovrebbe andare oltre il semplice apprendimento di strumenti e tecnologie, dotando cittadini e imprese della reale capacità di comprendere i vantaggi di un mercato dei dati inclusivo ed equo, come specificato nel considerando 19, e consolidando così il processo di innovazione dell'economia europea basata sui dati.

[46] Quanto alla tutela giudiziaria, le autorità responsabili del controllo dell'applicazione del GDPR, ivi compreso il Garante europeo della protezione dei dati, possono, nei limiti delle proprie competenze, infliggere sanzioni amministrative pecuniarie per la violazione degli obblighi relativi alla messa a disposizione o condivisione dei dati da impresa a consumatore e da impresa a impresa, oltre che al loro uso a vantaggio della collettività (art. 40, parr. 4 e 5).

La tutela della *privacy* alla prova degli usi militari dell'IA: riflessioni sul ruolo del diritto internazionale umanitario

di **Alice Civitella**

1. *Introduzione*

La raccolta e l'utilizzo di dati sono il centro di gravità dell'impiego dell'Intelligenza Artificiale (IA)[1]. È noto, infatti, come questa tecnologia necessiti di enormi quantità di dati al fine di essere addestrata, adattarsi, 'imparare' e, in ultima istanza, funzionare in modo adeguato[2]. La raccolta dei dati avviene in diversi modi: si pensi anzitutto a quelli generati dalla navigazione su Internet o dall'uso dei social media, ma anche a quelli acquisiti tramite sistemi di sorveglianza pubblica e privata o, più banalmente, attraverso i dispositivi intelligenti integrati in auto o abitazioni[3]. Essi possono essere raccolti, processati e immagazzinati anche per lunghi periodi di tempo, ponendo seri rischi per la privacy degli individui, specialmente in relazione all'impatto di attività quali sorveglianza, profilazione,

---

[1] E. Guild, *Mapping Limitations for State Surveillance through the UN Human Rights Instruments*, in *Privacy and Surveillance in a Digital Era: Challenges for Transatlantic Cooperation and European Criminal Law*, 2021, p. 218; C. Daelman, *AI Through a Human Rights Lens. The role of Human Rights in Fulfilling AI's Potential*, in *Artificial Intelligence and the Law*, Cambridge, 2021, p. 123

[2] EU, *Open data and AI: A symbiotic relationship for progress*, Sito web dell' Unione europea, disponibile a: https://data.europa.eu/en/publications/datastories/open-data-and-ai-symbiotic-relationship-progress

[3] Ad esempio, v.: D. Riebesehl, *AI in public and private forms of surveillance: Changing trust in the citizen-government relations*, in *Artificial intelligence and democracy: risks and promises of AI-mediated citizen-government relations*, Northampton, 2022

riconoscimento facciale e biometrico[4]. A fronte di ciò, sempre maggiore attenzione è stata data alle possibili conseguenze che l'utilizzo dell'IA può avere sul rispetto dei diritti umani.

Se tale attenzione ha visto un crescendo per le applicazioni dell'IA in ambito civile, lo stesso non può dirsi per quanto concerne le applicazioni in ambito militare. In questi contesti, l'IA è utilizzata per diversi fini: dalla sorveglianza alla logistica, dalla profilazione fino ad arrivare al supporto nell'identificazione di obiettivi militari e alla sua incorporazione all'interno di armi. Essa, dunque, è sempre più in grado di condizionare in modo diretto non solo la condotta delle ostilità, ma anche la vita degli individui. Numerose testimonianze in tal senso sono emerse in relazione alla raccolta e immagazzinamento dei dati biometrici di civili da parte delle autorità statunitensi nel corso delle operazioni militari in Iraq e Afghanistan, al fine di individuare potenziali affiliati a gruppi terroristici[5] e, più recentemente, nell'utilizzo di sistemi di sorveglianza di massa e per l'identificazione di obiettivi nel conflitto Israelo-Palestinese[6].

Muovendo da queste premesse, le pagine che seguono intendono offrire una prima riflessione circa l'applicazione del diritto alla privacy con riguardo alla raccolta e all'utilizzo dei dati da parte dell'IA nel contesto di conflitti armati, ponendo un accento particolare sulla relazione tra tale diritto fondamentale e il Diritto Internazionale Umanitario (DIU).

A tal fine, si procederà per gradi. Il secondo paragrafo sarà dedicato all'analisi di come la raccolta e l'utilizzo dei dati da parte degli algoritmi di IA viene rego-

---

[4] Report dell'Alto Commissariato per i diritti umani, *The right to privacy in the digital age*, 4 agosto 2022, A/HRC/51/17, p. 11; Sul punto, v. anche: M. Katrak, I. Chakrabarty, *Privacy, Political Participation and Dissent: Facial Recognition Technologies and Risk of Digital Authoritarism in the Global South*, in *Artificial Intelligence and Human Rights*, Oxford Academic, 2023, pp. 150-161; V. Golunova, *Artificial Intelligence and the Right to Liberty and Security*, in *Artificial Intelligence and Human Rights*, pp. 45-60; D. Riebesehl, *AI in public and private forms of surveillance: Changing trust in the citizen-government relations*, cit., p. 107; C. Garvie, *Face Recognition and the Right to stay Anonymous,* In *The Cambridge Handbook of Information Technology, Life Sciences and Human Rights*, Cambridge, pp. 139-152; OHCHR, *OHCHR and privacy in the digital age*, sito web delle Nazioni Unite, disponibile a: https://www.ohchr.org/en/privacy-in-the-digital-age; C. Daelman, *AI Through a Human Rights Lens. The role of Human Rights in Fulfilling AI's Potential,* cit., p. 126

[5] Sul punto v.: L. West, *Face Value: Precaution versus Privacy in Armed Conflicts*, in *The Rights to Privacy and Data Protection in Time of Armed Conflict*, ed. Buchan R. e Lubin A., NATO CCDCOE Publications, 2022, pp. 132-156; N. T. Djanegara, *Biometrics and Counter-Terrorism Case study of Iraq and Afghanistan*, Privacy international, 2021

[6] Y. Abraham, *'Lavender': The AI machine directing Israel's bombing spree in Gaza*, sito web di Magazine 972+, https://www.972mag.com/lavender-ai-israeli-army-gaza/

lata dal diritto internazionale dei diritti umani, soffermandosi sugli strumenti adottati a livello universale e nell'ambito regionale del Consiglio d'Europa[7]. Nel terzo paragrafo, poi, si fornirà una ricognizione delle diverse applicazioni dell'IA nei conflitti armati, analizzandone la regolamentazione nel DIU. Nel quarto paragrafo, ci si dedicherà dapprima all'interazione tra diritti umani e DIU, mettendo in risalto il ruolo del diritto alla privacy in questo senso, per poi analizzare il ruolo dell'Articolo 36 del Primo protocollo addizionale, che, imponendo agli Stati l'obbligo di assicurare la conformità di nuovi mezzi e metodi di guerra al diritto internazionale, ha una grande potenzialità nel ricondurre a sistema gli obblighi di diritti umani inerenti al rispetto della privacy con quelli derivanti dal rispetto del DIU. Il quinto paragrafo conclude.

Prima di procedere, si rende necessaria una precisazione in merito alla distinzione tra *data protection* e privacy. Di fatto, le due nozioni sono intimamente connesse, tanto che si discute della loro effettiva differenza. Secondo parte della dottrina, essa si sostanzierebbe nel fatto che il più ampio diritto alla privacy includerebbe anche la protezione di quelle informazioni non utilizzate esclusivamente per l'identificazione delle persone[8]. Sebbene quello del Consiglio d'Europa sia l'unico sistema in cui sia delineata una distinzione tra le due, anche nella giurisprudenza della Corte europea dei diritti umani (d'ora in avanti 'Corte EDU') il diritto alla protezione dei dati viene considerato derivante e parte del più generale diritto alla privacy, in quanto entrambi rientrano nel campo di applicazione del rispetto della vita privata e familiare[9]. Rifacendosi a tale interpretazione, nel corso della trattazione, si farà esclusivamente riferimento al diritto alla privacy, da intendersi ricomprendente anche il diritto alla protezione dei dati.

---

[7] La presente ricerca si incentra esclusivamente sul contesto regionale del Consiglio d'Europa, tralasciando il contesto Interamericano e Africano. L'esclusione di tali sistemi è dettata unicamente da necessità di ordine pratico, considerando l'ampiezza potenziale di una loro analisi esaustiva

[8] A. Zornetta, I. Cofone, *Data protection and the Right to privacy*, in *Artificial Intelligence and Human Rights*, 2023, p. 123

[9] J. Kokott, C. Sobotta, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, *International Data Privacy Law*, 2013, Vol. 3, No. 4, p. 223; Corte EDU, *Guide to the Case-Law of the of the European Court of Human Rights-Data protection*, aggiornata al 31 agosto 2024, p. 7; W. Schabas, *The European Convention on Human Rights: A Commentary*, Oxford Commentaries on International Law, 2015, p. 382

2. *La protezione dei dati e il diritto alla* privacy *nel diritto internazionale dei diritti umani*

Il diritto alla privacy è riconosciuto come un diritto fondamentale della persona, garantito in diversi strumenti internazionali. Il riconoscimento del diritto alla privacy come parte dei diritti umani si ritrova già all'articolo 12 della Dichiarazione universale dei diritti umani[10]. Non essendo la Dichiarazione uno strumento giuridico vincolante[11], è solo con la trasposizione dell'articolo 12 nell'articolo 17 del Patto sui diritti civili e politici del 1966 (d'ora in avanti 'il Patto')[12] che la tutela del diritto alla privacy ha trovato pieno riconoscimento.[13] L'articolo 17 del Patto, infatti, riprende in modo quasi del tutto identico l'articolo 12 della Dichiarazione, aggiungendo il divieto di «*unlawful interference*» nella protezione di tale diritto. Emerge sin da subito, dunque, una caratteristica fondamentale del diritto alla privacy, ossia la sua natura non assoluta. Come spiegato nel Commento generale n. 16[14], ciò implica che il diritto alla privacy sia suscettibile di limitazioni, sebbene esse debbano essere espressamente previste dalla legge, oltre che non arbitrarie[15].

La tutela del diritto alla privacy e dei dati personali, specialmente in relazione all'impiego di IA, è stata recentemente oggetto di attenzioni da parte delle Na-

---

[10] Dichiarazione Universale dei diritti umani, adottata dalla Risoluzione dell'Assemblea Generale delle Nazioni Unite 217 A, Parigi 10 Dicembre 1948

[11] La Dichiarazione è, infatti, una risoluzione dell'Assemblea Generale delle Nazioni Unite, e, dunque, priva di valore giuridicamente vincolante. V.: C. Focarelli, *Diritto Internazionale*, settima edizione, Vicenza, 2023, p. 422

[12] Patto sui diritti civili e politici, Nazioni Unite *Treaty Series*, vol. 999, p. 171

[13] Tale diritto è riconosciuto anche in altri trattati sui diritti umani, ad esempio: Convenzione americana sui diritti umani, *OAS Treaty Series* n. 36; Nazioni Unite *Treaty Series* Vol. 1144 p. 123, 1978, art 11; Convenzione sui diritti del fanciullo, Nazioni Unite *Treaty Seriers*, Vol. 1577 p. 3, 1990, art 16; Convenzione internazionale sui diritti dei lavoratori migranti e delle loro famiglie, Nazioni Unite *Treaty Series*, Vol. 2220 p. 3, 2003, art 14; Carta araba dei diritti dell'uomo, 12 Int'l Hum. Rts. Rep. 893, 2008, art. 16 e 21; Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, Nazioni Unite *Treaty Series* Vol. 2515 p. 3, 2008, art 22

[14] Alto Commissariato per i diritti umani, *ICCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 1988

[15] *O.c.*, § 3-4; Si pensi, ad esempio, alla normativa interna degli Stati sulle limitazioni a tale diritto fatte in nome della lotta al terrorismo o per il controllo dei confini. V.: E. Guild, *Mapping Limitations for State Surveillance through the UN Human Rights Instruments*, cit., p. 224

zioni Unite[16]. Si segnalano, in particolare, due documenti: il rapporto dell'agosto 2022 dell'Alto Commissariato sui diritti umani, *The Right to Privacy in the Digital Age*[17], e la recente risoluzione *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*, adottata dall'Assemblea Generale il 21 marzo 2024[18]. Due sono gli aspetti fondamentali che meritano di essere sottolineati. In primo luogo, il rapporto – nel mettere in luce i rischi associati alle attività di hackeraggio, limitazioni alla crittografia, sorveglianza e monitoraggio online operati dalle autorità statali – evidenzia la legittimità di tali attività qualora siano condotte nel rispetto dei diritti umani[19] e dei principi di necessità e di proporzionalità, quali principi generali del diritto internazionale[20]. Tutto ciò sembrerebbe estendersi anche alle attività di sorveglianza, intelligence e profilazione messe in atto dagli Stati attraverso l'uso di IA. In secondo luogo, il rispetto dei diritti umani è il punto cruciale di entrambi questi strumenti. A titolo esemplificativo, la risoluzione, riferendosi all'impiego dell'IA in tempo di pace[21], promuove il rispetto dei diritti umani e del diritto alla privacy in ogni fase della vita dell'IA, come anche la necessità di creare meccanismi volti alla protezione dei dati usati per il suo sviluppo e impiego[22]. La centralità del rispetto dei diritti umani e del diritto alla privacy si ritrovano, del resto, anche negli AI Principles[23] e nelle OECD Privacy Guidelines[24] dell'Organizzazione per la coo-

---

[16] *O.c.*, p. 230

[17] *Infra* nota 13. Questo Report è stato redatto in risposta della richiesta dell'Assemblea Generale espressa nella Risoluzione 68/167 del 18 dicembre 2013 di un Report da parte dell'Alto Commissariato per i diritti umani sulla protezione del diritto alla privacy nella sorveglianza sia a livello domestico che extraterritoriale, nell'intercettazione di comunicazioni digitali e nella raccolta di dati personali.

[18] UNGA, *Resolution adopted by the General Assembly on 21 March 2024 Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*, 78/265

[19] Report dell'Alto Commissariato per i diritti umani, *The right to privacy in the digital age*, cit. p. 13

[20] Ad esempio, v.: N. Menandez Gonzales, *The Rights to privacy and data Protection and Facial recognition Technology in the Global North*, cit., 2023, p. 146

[21] Res. 78/265 p. 2

[22] *O.c.* § 4(e) 3(J), 7

[23] OECD Legal Instruments, *Recommendation of the Council on Artificial Intelligence*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#mainText. Adottate nel 2019 e revisionate nel 2023 e 2024

[24] OECD Legal Instruments, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD/LEGAL/0188, adottata nel 1981 e revisionata nel 2013

perazione economica e lo sviluppo (OECD)[25]. Anche in questi casi, dunque, si sancisce espressamente l'obbligo di rispettare i diritti umani, inclusi la protezione dei dati e della privacy, e di adottare le garanzie necessarie alla loro protezione in ogni momento del ciclo della vita dell'IA.

Nel contesto del Consiglio d'Europa, tra i diritti umani garantiti dalla Convenzione europea dei diritti umani (CEDU), l'articolo 8 protegge il rispetto della vita privata e familiare. In risposta allo sviluppo e utilizzo di nuove tecnologie, la Corte EDU si è espressa sempre più frequentemente su questioni inerenti alla protezione dei dati[26]. Molti di questi casi hanno riguardato la raccolta e utilizzo dei dati ai fini di sorveglianza segreta e di massa; sorveglianza audio e video; geolocalizzazione di veicoli; conservazione dei dati personali e trasmissione dei dati ai fini di sicurezza nazionale[27]. L'articolo 8 assume importanza in quanto specifica in modo più dettagliato, rispetto agli strumenti sopra indicati, le circostanze in cui le restrizioni all'esercizio del diritto possono essere adottate, ad esempio per necessità derivanti dalla sicurezza nazionale o pubblica, incluso rispetto all'utilizzo dei dati biometrici[28].

Tra gli strumenti precipuamente volti alla tutela del diritto alla privacy e dei dati personali nel contesto del Consiglio d'Europa, si segnalano la Convenzione 108[29] del 1988, modernizzata tramite un apposito Protocollo di modifica (Convenzione 108+)[30], e la recente adozione da parte Consiglio dei ministri del Consiglio d'Europa della *Council of Europe Framework Convention on Artificial*

---

[25] Organizzazione intergovernativa fondata nel 1961 per la promozione dello sviluppo economico e della democrazia, https://www.oecd.org/

[26] Corte EDU, *Guide to the Case-Law of the of the European Court of Human Rights: Data protection*, 31 dicembre 2020, p. 7

[27] *O.c.,* pp. 30-76

[28] Art. 8(2) Convenzione europea dei diritti umani. Ai fini di determinare se questo articolo sia stato rispettato, si deve indagare se l'interferenza sia prevista e sia avvenuta nel rispetto della legge; se essa persegua un interesse legittimo; e, da ultimo, se l'interferenza sia necessaria in una società democratica. Sul punto v: R. Argren, *Protection of Biometric private life under the European Convention on Human Rights*, The Military Law and the Law of War Review, Vol. 62 no. 1, 2024, pp. 61-88, p.71; W. Schabas, *The European Convention on Human Rights: A Commentary,* cit., p. 384. Altri articoli della Convenzione simili sono il 9, 10 e 11

[29] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, Serie dei Trattati Europei, n. 108, 28 gennaio 1981

[30] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), CM (2018)2-final, 17-18 Maggio 2018

Intelligence and Human Rights, Democracy and the Rule of Law (*Framework Convention*), adottata nel maggio 2024 ed aperta alla firma il 5 settembre[31].

La Convenzione 108+ fornisce protezione agli individui in relazione al «*processing*»[32] dei propri dati personali, a garanzia del rispetto dei loro diritti umani e, in particolare, del diritto alla privacy[33] per tutti coloro che si trovano sottoposti alla giurisdizione degli Stati parte[34]. La *Framework Convention*, invece, ha lo scopo primario di protezione dei diritti umani, della democrazia e dello stato di diritto in ogni momento del ciclo di vita dell'IA, dal «*planning*» e «*design*» fino al «*retirement*»[35]. L'articolo 11, in particolare, sancisce la protezione del diritto alla privacy e dei dati per tutto il ciclo della vita dell'IA[36]. Per quanto significativa, la Convenzione ha, tuttavia, una portata limitata: da un lato, essa non trova applicazione nel caso in cui l'IA venga utilizzata a scopo di proteggere la sicurezza nazionale o la difesa dello Stato[37]; dall'altro, non è chiaro se tale divieto si estenda anche ai conflitti armati, restando così incerto il rapporto tra IA e privacy in tale contesto.

3. *Il diritto applicabile all'impiego dell'intelligenza artificiale nei conflitti armati*

La corretta selezione dei dati e il corretto funzionamento dell'IA nei contesti di conflitto armato sono requisiti essenziali per assicurare il rispetto del DIU[38]. Non essendo questa la sede per fornire una lista esaustiva di tutte le possibili applicazioni dell'IA nei conflitti armati, si cercherà di offrire una panoramica di quegli impieghi che paiono essere maggiormente problematici per il rispetto del diritto alla privacy e del DIU. Al fine di garantire una maggiore chiarezza esposi-

---

[31] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series - No. 225

[32] L'articolo 2(b) definisce il "data processing" come «*any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data*»

[33] Art. 1 Convenzione 108+

[34] *O.c.* Art. 3

[35] *Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, p. 4

[36] Art. 11 *Framework Convention*

[37] *O.c.* Art. 3(2) e (4)

[38] V. sul punto: L. West, *Face Value: Precaution versus Privacy in Armed Conflict*, cit., pp. 132-156

tiva, si propone qui una suddivisione dei diversi utilizzi dell'IA in tre diverse categorie, partendo da quegli utilizzi che hanno un impatto pressoché minimo sulla condotta delle ostilità, fino ad arrivare a quelli via via più rilevanti a tal riguardo. Infatti, è doveroso mettere in evidenza qui una caratteristica fondamentale, ma spesso trascurata, dell'IA, ossia che essa è a tutti gli effetti un «*enabler*», cioè una tecnologia che aiuta nello svolgimento di determinati incarichi, in precedenza svolte unicamente dagli esseri umani[39]. In questa prospettiva, non è necessario guardare alla tecnologia in sé e per sé, quanto piuttosto alle mansioni specifiche per le quali essa viene impiegata.

A fronte delle premesse appena fatte, si possono includere in una prima categoria tutti quegli impieghi dell'IA volti ad aiutare l'operatore umano nello svolgimento ed ottimizzazione di compiti inerenti alla logistica, all'addestramento delle forze armate, e alla velocizzazione delle comunicazioni[40]. Nella seconda categoria, invece, vanno inclusi tutti quegli utilizzi inerenti ad attività di maggiore rilievo per la condotta delle ostilità, ma che non sfociano nell'impiego diretto della forza armata. Tra queste si segnalano: analisi e definizione della priorità di obiettivi militari (ad esempio tramite l'analisi di sistemi audio-video); identificazione degli obiettivi militari tramite il riconoscimento di immagini e analisi dei dati; predisposizione di raccomandazioni inerenti alla scelta delle armi e delle linee d'azione; predizione e valutazione dei danni collaterali; analisi in tempo reale dei dati forniti dai sensori; identificazione e classificazione di dati e riconoscimento di *pattern* in essi, ad esempio per attività ostili; identificazione di individui e oggetti di interesse tramite dati derivanti dall'intero spettro elettromagnetico[41]. All'interno di questo gruppo vengono inclusi i c.d. *Decision Support Systems* (DSS), ossia sistemi computerizzati capaci di aiutare gli operatori umani nel prendere decisioni complesse utilizzati all'interno del processo del *targeting*[42].

---

[39] M. Sisson, *Multistakeholder Perspectives on the Potential Benefits, Risks, and Governance Options for Military Applications of Artificial Intelligence*, in Report *the Militarization of Artificial Intelligence*, 2020, p. 3

[40] *O.c.*, p. 4; S. Grand-Clément, *Artificial Intelligence Beyond Weapons. Application and Impact of AI in the Military Domain*, UNIDIR, 2023, pp. 14-20

[41] Tra gli altri: M. Sisson, *Multistakeholder Perspectives on the Potential Benefits, Risks, and Governance Options for Military Applications of Artificial Intelligence*, cit., p. 4

[42] Esempi sono il Project Maven statunitense e l'uso di Lavender e the Gospel da parte di Israele. Per un approfondimento sui DSS V.: A. Civitella, I*ntelligenza artificiale e diritto internazionale umanitario: l'uso di Lavender nel conflitto Israelo-palestinese*, SidiBlog, 2024, disponibile a: http://www.sidiblog.org/2024/06/03/intelligenza-artificiale-e-diritto-internazionale-umanitario-luso-di-lavender-nel-conflitto-israelo-palestinese/; D. Mauri, *Numeri, persone, umanità. Sistemi di supporto alle decisioni umane in campo militare da parte dell'IDF e diritto internazionale umanitario*, Diritti

Essi, infatti, sono in grado di fornire a livello tattico e strategico informazioni e suggerimenti immediati, ad esempio, sulle migliori modalità per effettuare un attacco e su quali armi utilizzare[43].

La terza categoria, infine, racchiude il più conosciuto impiego dell'IA all'interno di armi o, meglio, di sistemi d'arma in grado di operare in autonomia[44]. In questi casi, dunque, l'IA fornisce determinate potenzialità a tali sistemi d'arma ed alla loro capacità di operare autonomamente le c.d. fasi critiche del *targeting*. A differenza dei DSS, quindi, esse sono in grado di utilizzare direttamente la forza letale[45].

Al momento non esiste alcun tipo di disciplina sull'uso dell'IA nei conflitti armati[46]. Perciò, si dovrà procedere all'analisi delle norme pattizie e consuetudinarie del DIU per capire se e in che modo l'IA possa essere da esso disciplinata. Il punto cruciale, a tal riguardo, pare essere le finalità per le quali essa viene impiegata nei conflitti armati, ossia qualora l'IA venga utilizzata per attività disciplinate dal DIU. Più nel dettaglio, è cruciale determinare se essa venga usata in sistemi o attività parte dei mezzi e metodi di guerra[47]. È bene sottolineare che non esiste

---

Umani e diritto internazionale, Fascicolo 2, maggio-agosto 2024; D. Amoroso, *Sistemi di supporto alle decisioni basati sull'IA e crimini di guerra: alcune riflessioni alla luce di una recente inchiesta giornalistica*, Diritti umani e diritto internazionale, Fascicolo 2, maggio-agosto 2024; A.H, Michel, *Decisions, Decisions, Decisions: computation and Artificial Intelligence in military decision-making*, sito web del Comitato Internazionale della Croce Rossa, 2024

[43] CICR, Geneva Academy, *Artificial Intelligence and Related Technologies in Military Decision Making on the Use of Force in Armed Conflicts, Current Developments and Potential Implications*, Ginevra, 2024, p. 14

[44] Per un approfondimento sulle armi autonome e le loro caratteristiche, v.: M. Taddeo, A. Blanchard, *A Comparative Analysis of the Definitions of Autonomous Weapons Systems,* Science and Engineering Ethics, Vol 28, Issue 37, 2022; V. Boulanin, M. Verbruggen, *Mapping the Development of Autonomy in Weapon Systems*, SIPRI, 2017

[45] Su questa distinzione v.: CICR, *Artificial Intelligence and Machine learning in armed conflicts*, International Review of the Red Cross 102 (913), 2020, pp.467-469; CICR, Geneva Academy, *Artificial Intelligence and Related Technologies in Military Decision Making on the Use of Force in Armed Conflicts*, Current Developments and Potential Implications*,* cit.*,* p. 8

[46] Un tentativo di stabilire degli standard condivisi sull'impiego di IA a fini militari si è avuto con la *Political Declaration on Responsible Military use of Artificial Intelligence and Autonomy,* la quale, tuttavia non è uno strumento giuridico vincolante. V.: US Department of State, *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, 9 novembre 2023, cit.

[47] V.: CICR, Geneva Academy, *Artificial Intelligence and Related Technologies in*

una definizione univoca di armi, mezzi e metodi di guerra[48]. Infatti, se può facilmente definirsi cosa sia un'arma, ben più difficile è stabilire che cosa siano i mezzi e i metodi di guerra. In base al Commentario del Comitato Internazionale della Croce Rossa al Primo protocollo addizionale, con «*means and methods of warfare*» ci si riferisce alle armi nel senso più ampio e, con specifico riferimento ai metodi, al modo in cui vengono utilizzate[49]. Diverse definizioni si ritrovano anche in dottrina, dove alcuni autori promuovono un concetto più ampio di tale categoria, andando ad includere anche piattaforme ed equipaggiamenti militari non in grado di esercitare la forza e, quindi, di causare danni a persone/cose[50], mentre altri riconducono i mezzi di guerra alle sole armi o sistemi d'arma capaci, dunque, di infliggere forza armata[51].

Prendendo in questa sede come riferimento le definizioni più estensive di mezzi di guerra, in base alla classificazione effettuata, è possibile concludere che solo gli utilizzi dell'IA che ricadono nella seconda e terza categoria possono essere considerati come mezzi o metodi di guerra[52]. Conseguentemente, essi sono regolati dal DIU e devono rispettarne le norme rilevanti[53]. In diverse occasioni, infatti, è stato affermato che, per la loro capacità di impattare direttamente sulla condotta delle ostilità, anche i DSS debbano essere sottoposti alle norme che disciplinano la categoria dei mezzi e metodi di guerra[54]. Segnatamente, non solo

---

Military Decision Making on the Use of Force in Armed Conflicts, Current Developments and Potential Implications, cit., p. 9

[48] McClelland J., *The review of weapons in accordance with Article 36 of Additional Protocol I*, International Review of the Red Cross, Vol. 85 No 850, 2003, p. 404

[49] Commentario del 1987 all'articolo 35 del Primo Protocollo Addizionale, disponibile a: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-35/commentary/1987?activeTab=

[50] Ad esempio, v.: W.H. Boothby, *The Law of Targeting*, Oxford, 2012, p. 255; D. Fleck, *The Handbook of International Humanitarian Law*, Oxford, 2021, p. 129. Dinstein, ad esempio, distingue tra piattaforme che trasportano armi, da includere ella categoria dei mezzi di guerra, e quelle invece che, non trasportando armi, devono esserne escluse, Y. Dinstein, *The Conduct of Hostilities*, Cambridge, 2022, p. 82

[51] Ad esempio, v. N. Melzer, *Diritto Internazionale Umanitario. Un'ampia introduzione*, Comitato Internazionale della Croce Rossa, 2023, p. 120

[52] Secondo William Boothby, essi devono essere considerati come parte dei metodi di guerra. V. W. Boothby, *AI Warfare and the Law,* International law Studies, 2025, p. 138

[53] CICR, Geneva Academy, *Artificial Intelligence and Related Technologies in Military Decision Making on the Use of Force in Armed Conflicts, Current Developments and Potential Implications*, cit., p. 10

[54] Sul punto: N. Goussac, *Safety net or tangled web: Legal reviews of AI in*

essi non devono essere di natura indiscriminata[55] o provocare mali superflui, sofferenze inutili[56] o danni durevoli, estesi e gravi all'ambiente naturale[57], ma debbono altresì poter essere usati in modo tale da rispettare i principi di distinzione, precauzione e proporzionalità[58]. Come vedremo, tale conclusione ha un risvolto importante anche in relazione all'articolo 36 del Primo protocollo addizionale.

4. *La protezione dei dati ed il rispetto del diritto alla privacy nei conflitti armati*

Di per sé, il diritto alla privacy non trova protezione alcuna nel DIU[59]. Gli unici riferimenti che si ritrovano sono inerenti alla protezione della corrispondenza dei prigionieri di guerra, alla possibilità di sospendere i diritti concernenti le comunicazioni private, e, da ultimo, all'inviolabilità dei dati medici[60]. Un breve cenno viene fatto nella *Call to Action* adottata al *Responsible AI in the Military Domain Summit*, in cui si afferma la necessità di rispettare la normativa internazionale, regionale e nazionale in materia di protezione dei dati[61].

---

weapons and war-fighting, Blogs ICRC, disponibile a: https://blogs.icrc.org/law-and-policy/2019/04/18/safety-net-tangled-web-legal-reviews-ai-weapons-war-fighting/; CICR, Geneva Academy, *Artificial Intelligence and Related Technologies in Military Decision Making on the Use of Force in Armed Conflicts, Current Developments and Potential Implications*, *cit.,* p. 10; K. Klonowska, *Shifting the narrative: not weapons, but technologies of warfare*, ICRC Bogs, 2022, disponibile a: https://blogs.icrc.org/law-and-policy/2022/01/20/weapons-technologies-warfare/

[55] Art. 51(4) e (5)(a) Primo protocollo addizionale

[56] *O.c.* Art. 35 (2)

[57] *O.c.* Art. 35 (3)

[58] Rispettivamente, Art. 48, 57 e 51(5)(b) del Primo protocollo addizionale

[59] A. Lubin, *The Rights to Privacy and Data Protection under International Humanitarian law and Human Rights Law*, in *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspective,* Cheltenham, Northampton, 2022, p. 463

[60] Art. 76 della III Convenzione di Ginevra del 12 agosto 1949; art. 5 della IV Convenzione di Ginevra del 12 Agosto 1949; Commentario all'art. 34 della II Convenzione di Ginevra del 12 Agosto 1949, disponibile a: https://ihl-databases.icrc.org/en/ihl-treaties/gcii-1949/article-33/commentary/2017?activeTab=. Altri autori hanno considerato norme sul diritto alla privacy anche quelle inerenti al rispetto della proprietà privata, ad esempio v.: L. West, *Face Value: Precaution versus Privacy in Armed Conflict*, cit.

[61] *Responsible AI in the Military Domain Summit*, REAIM Call to Action, 15-16 Febbraio 2023, § 10

Di conseguenza, il fondamento giuridico del rispetto del diritto alla privacy nei conflitti armati deve essere ricercato nelle tutele previste nel diritto internazionale dei diritti umani. Tuttavia, anche in giurisprudenza nessun caso è emerso in merito all'applicazione della protezione dei dati e del loro utilizzo e, più in generale, del diritto alla privacy in tali contesti[62]. Infatti, sebbene la Corte EDU in più occasioni si sia espressa sulle violazioni dell'articolo 8 della CEDU in relazione alla protezione dei dati e informazioni personali, ciò non è mai avvenuto in relazione all'ambito di un conflitto armato. Esempi apparentemente isolati si ritrovano in alcune pronunce della Corte internazionale di giustizia (CIG): nel *Parere sulla Costruzione del muro in Palestina* del 2004 e nel più recente *Parere sulle conseguenze giuridiche derivanti dalle politiche e dalle pratiche di Israele nei territori palestinesi occupati, compresi quelli di Gerusalemme Est*, la CIG si è espressa in merito all'applicazione dell'art. 17 nel contesto di occupazione bellica e sulla sua violazione, senza però approfondire la portata dell'applicazione di questo diritto nei conflitti armati[63]. Dunque, la CIG in qualche modo dà per scontata la continuità dell'applicazione del diritto alla privacy in un contesto di occupazione bellica, in cui, come noto, si applicano norme specifiche del DIU.

A fronte di ciò, diventa necessario analizzare in quale modo il diritto alla privacy si applichi in tali contesti, indagando dapprima la relazione tra diritti umani e DIU e le sue conseguenze sull'applicazione del diritto alla privacy, e, successivamente, il rispetto del diritto alla privacy alla luce dell'obbligo sancito all'articolo 36 del Primo protocollo addizionale.

4.1 *La complessa relazione tra il diritto alla privacy e il DIU*

Il dibattito sulla relazione tra diritto internazionale dei diritti umani e DIU è risalente nel tempo. Sorvolando sulle iniziali interpretazioni del diritto internazionale dei diritti umani quale diritto applicabile esclusivamente in tempo di pace, è ormai pressoché universalmente accettato che i diritti umani continuino a trovare applicazione anche all'interno di un conflitto armato, sia esso di natura internazionale o non-internazionale[64]. Ciò è stato confermato in più occasioni

---

[62] A. Lubin, *The Rights to Privacy and Data Protection under International Humanitarian law and Human Rights Law*, cit., p. 465

[63] CIG, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, parere del 9 luglio del 2004, §128; CIG, *Legal Consequences Arising from the Policies and Practices of Israel in the Occupied Palestinian Territory*, Including East Jerusalem, parere del 19 luglio 2024, § 220

[64] Ad esempio v.: Comitato per i diritti umani, General Commment n. 29: '*States of Emergency*', 2001; Comitato per i diritti umani, General Comment n. 31 *'The Nature of the General Legal Obligation Imposed on States Parties to the Covenant'*, 2004.

dalla Corte internazionale di giustizia: nel *Parere sulla Liceità della minaccia e dell'uso delle armi nucleari* del 1996[65], nel *Parere sulle conseguenze giuridiche della costruzione del muro nei territori palestinesi occupati*[66], nella sentenza del caso *Congo c. Uganda* del 2005 relativa alle attività militari sul territorio del Congo[67]. Anche la Corte EDU ha sviluppato una giurisprudenza consolidata al riguardo, specialmente in relazione all'applicazione extraterritoriale della Convenzione[68].

Dunque, il nodo cruciale da sciogliere resta quale tipo di relazione sussista tra diritti umani e diritto umanitario e, nel nostro caso, tra il diritto alla privacy e le norme rilevanti del DIU.

Nel *Parere sulla Liceità e minaccia dell'uso delle armi nucleari* del 1996, la CIG, nell'esaminare la relazione tra diritti umani e diritto internazionale umanitario, ha fatto principalmente ricorso al criterio della *lex specialis*[69]*:* il diritto internazionale dei diritti umani, quale *lex generalis*, troverebbe continua applicazione anche all'interno dei conflitti armati insieme al DIU, che, in quanto *lex specialis*, avrebbe tuttavia la precedenza. Nel *Parere sulla Costruzione del Muro in Palestina*, la CIG riafferma l'applicazione di tale principio, senza però specificare in che modo tale principio regoli concretamente il rapporto tra DIU e diritti umani[70]. Volendo semplificare, si possono discernere tre diversi approcci al riguardo[71]. In base al primo, i diritti umani, pur applicabili, vengono messi da parte nei conflitti armati, dove solo il DIU verrà applicato, in quanto *lex specialis*. Questa è una posizione assolutamente minoritaria tanto tra gli Stati, quanto in giurisprudenza

---

[65] CIG, *Legality of the Use by a State of Nuclear Weapons in Armed Conflict*, Parere del 8 luglio 1996, §25

[66] CIG, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, *cit.,* §106

[67] CIG, *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v. Uganda), sentenza del 19 dicembre 2005 §216

[68] Ad esempio v.: *Loizidou c. Turchia*, 1995; *Bankovic e altri c. Belgio*, 2001; *Issa c. Turchia*, 2005; *Al Jedda c. Regno Unito*, 2007; *Al Skeini c. Regno Unito* 2011; *Hassan c. Regno Unito* 2014; *Georgia c. Russia* 2021

[69] *Infra* nota 67

[70] Secondo la GIC, possono delinearsi tre diverse situazioni: alcune ricadenti esclusivamente sotto i diritti umani; altre esclusivamente sotto il DIU; ed infine, altre che vedono l'applicazione di entrambi. Questo principio non viene però ripreso nel caso *Congo c. Uganda*, in cui la CIG si limita a sostenere l'applicabilità di entrambi, diritti umani e DIU (§216)

[71] M. Milanovic, *The Lost Origins of Lex Specialis. Rethinking the Relationship between Human Rights and International Humanitarian Law*, in *Theoretical Boundaries of Armed Conflict and Human Rights*, Forthcoming, 2014, 103 e ss.

e in dottrina, e non la si prenderà pertanto in considerazione[72]. Più complesso è il discorso inerente alle altre due interpretazioni. In base alla seconda, DIU e diritti umani sono entrambi direttamente applicabili e complementari; il principio della *lex specialis*, dunque, si configurerebbe come criterio di risoluzione di possibili antinomie tra norme del DIU e dei diritti umani, risultando nella temporanea disapplicazione di questi ultimi nel caso di specie[73]. In base all'ultima interpretazione, infine, il principio della *lex specialis* sarebbe da intendersi esclusivamente come metodo interpretativo[74]; così facendo, le norme del DIU dovranno interpretarsi anche alla luce dei diritti umani e viceversa[75].

Ciò detto, è bene chiedersi quali conseguenze abbia tutto ciò sull'applicazione del diritto alla privacy nei conflitti armati. Come si è visto, il diritto alla privacy non è di per sé oggetto di regolamentazione del DIU. Di conseguenza, il diritto internazionale dei diritti umani è il corpus giuridico che verrà in rilievo per la raccolta ed utilizzo dei dati per le IA, anche nel contesto di conflitti armati. Considerando l'applicazione di algoritmi di IA all'interno di mezzi e metodi di guerra, si prenderà qui in considerazione un caso particolare, ossia quello di un potenziale conflitto tra il diritto alla privacy e il principio di precauzione, *ex* articolo 57 del Primo protocollo addizionale[76]. In base all'articolo 57 del Proto-

---

[72] *O.c.,* p. 104-105; V. Koutroulis, *Are IHL and HRL still two distinct branches of public international law?*, in *Research Handbook on Human Rights and Humanitarian Law. Further Reflections and Perspectives*, p. 45

[73] M. Milanovic, *The Lost Origins of Lex Specialis. Rethinking the Relationship between Human Rights and International Humanitarian Law* , cit., p. 106; *O.c.*; P. Kilibarda, R. Kolb, *The International Court of Justice, international humanitarian law and human rights law*, in *Research Handbook on Human Rights and Humanitarian Law. Further Reflections and Perspectives*, Cheltenham, Northampton, 2022, p. 184; General Comment 31, cit., §11. V. A. Lubin, *The rights to privacy and data protection under international humanitarian law and human rights law*, cit., p. 480. Per critiche a questa interpretazione, v. Y. Shany, *Co-application and harmonization of IHL and IHRL: are rumours about the death of lex specialis premature?* in *Research Handbook on Human Rights and Humanitarian Law. Further Reflections and Perspectives*, pp. 9-29

[74] In linea con l'articolo 31 della Convenzione di Vienna sul diritto dei trattati, 1969

[75] M. Milanovic, *The Lost Origins of Lex Specialis. Rethinking the Relationship between Human Rights and International Humanitarian Law*, cit., p. 106; V. Koutroulis, *Are IHL and HRL still two distinct branches of public international law*?, cit. ,p. 45; P. Kilibarda, R. Kolb, *The International Court of Justice, international humanitarian law and human rights law*, *cit.,* p. 184; G. Oberleitner, *Complementarity: maximizing protection*, in *Human Rights in Armed Conflict: Law, Practice, Policy*, Cambridge, 2015, pp. 105-121

[76] Primo Protocollo Addizionale alle Convenzioni di Ginevra del 12 agosto

collo, ormai considerato di natura consuetudinaria[77], le parti in conflitto sono chiamate ad adottare tutti gli accorgimenti per loro possibili al fine di garantire il rispetto effettivo dei principi di distinzione e proporzionalità. Qualora, dunque, una parte in conflitto disponesse delle tecnologie in grado di reperire e analizzare dati ai fini di una migliore identificazione di potenziali obiettivi militari, il principio di precauzione le imporrebbe di usarla[78].

Se adottiamo la seconda accezione del principio della *lex specialis* sopra descritta, nel caso di specie, il principio di precauzione prevarrebbe, portando alla disapplicazione del diritto alla privacy degli individui i cui dati sono stati raccolti ed utilizzati. Infatti, nel caso specifico del *targeting* la norma rilevante sarebbe quella del DIU, mentre quelle dei diritti umani, e il diritto alla privacy in particolare, verrebbero messe da parte in nome delle esigenze derivanti dalla condotta delle ostilità. Se invece accettassimo la terza interpretazione, vale a dire quella della contestuale e complementare applicazione dei diritti umani nei conflitti armati, il principio di precauzione andrebbe interpretato alla luce del diritto alla privacy. La rilevanza di quest'ultimo, in tale prospettiva, andrebbe esclusa solo qualora si dimostrasse, nel caso specifico, un'assoluta incompatibilità tra diritto alla privacy e principio di precauzione.

Questa terza ipotesi ricostruttiva è, a nostro avviso, da preferire. Così facendo, diventa possibile garantire una, seppur minima, protezione del diritto alla privacy, non in modo dissimile rispetto a ciò che avviene per le limitazioni di tale diritto in tempo di pace in particolari casi di necessità.

Dunque, fatte salve le ipotesi in cui una Parte contraente si sia avvalsa di meccanismi di deroga di cui agli articoli 4 del Patto e 15 della CEDU[79], si esclude in questa sede una totale disapplicazione del diritto alla privacy nei contesti di conflitto armato. Si avanza, invece, la tesi per cui, anche in tali contesti, qualora necessario ai fini della condotta bellica, sia possibile per gli Stati limitare il

---

1949, relativo alla protezione delle vittime dei conflitti armati internazionali, adottato a Ginevra l'8 giugno 1977

[77] J-M Henckaerts e L. Doswald-Beck, *Customary International Humanitarian Law*, Volume 1: Rules, Comitato Internazionale della Croce Rossa, Cambridge, 2005, Regole dalla 15 alla 24

[78] Sul punto v, L. West, *Face Value: Precaution versus Privacy in Armed Conflict*, *o. c.* ; A. Lubin, *Lieber Studies Big Data Volume – Algorithms of Care: Military AI, Digital Rights, and the Duty of Constant Care,* Lieber Institute-West Point Articles of War, 13 febbraio 2024, disponibile a: https://lieber.westpoint.edu/algorithms-care-military-ai-digital-rights-duty-constant

[79] In base a questi articoli, gli Stati hanno la possibilità di derogare ufficialmente da alcuni diritti, incluso il diritto alla privacy. In ogni caso, le deroghe devono avvenire nel rispetto dei principi di necessità e proporzionalità

suddetto diritto. È intrinseca nella natura del diritto alla privacy la possibilità di retrocedere dinanzi alla necessità di tutelare altri interessi, quali, ad esempio, le esigenze di difesa e sicurezza nazionale[80]. Per quanto non sia specificato se tra le esigenze di sicurezza nazionale e di difesa dello Stato possano rientrare tutti i casi di conflitti armati, non pare illogico concludere che le possibili limitazioni a questo diritto possano effettuarsi anche in tali contesti[81]. Con ciò non si vuole suggerire che ci debba essere una prevalenza del diritto alla privacy rispetto al principio di precauzione; tale possibilità colliderebbe, infatti, con la salvaguardia dei civili dagli effetti delle ostilità. Si vuole invece avanzare l'ipotesi della possibilità di comprimere senza eradicare del tutto l'applicabilità del diritto alla privacy nell'impiego di mezzi e metodi di guerra dotati di IA[82].

Ciò deve essere fatto nel rispetto di talune garanzie. Lubin, in particolare, identifica cinque principi ricorrenti per garantire il rispetto del diritto alla privacy, anche quando questo viene limitato dalle autorità statali, applicabili anche al di fuori del territorio nazionale dello Stato: il principio di legalità, il principio di necessità, il principio di proporzionalità, la garanzia di adeguate misure di salvaguardia, e l'accesso ad un rimedio effettivo[83]. Sovente, infatti, la Corte EDU ha sottolineato il dovere per gli Stati di svolgere attività, quali la sorveglianza degli individui e la raccolta dei loro dati, e di impiegare tecnologie intrusive come il riconoscimento facciale, solo quando esplicitamente previsto dalla legge[84]; quando finalizzato ad un interesse legittimo per le società democratiche e quando proporzionato a tale interesse[85]; e, soprattutto, ponendo in essere garanzie per contrastare possibili azioni arbitrarie da parte delle autorità statali[86]. La protezione dei dati, inoltre, assume importanza particolare quando i dati sono "processati" in modo automatizzato con l'ausilio di tecnologie sempre più sofi-

---

[80] Nel caso dell'art. 8 della CEDU, la Corte EDU si è espressa al riguardo in diversi casi, ad esempio: T*aylor-Sabori c. Regno Unito*, 2002 (§§ 17-19); *Rotaru c. Romania* [GC], 2000 (§§ 36-44, 57-62); *Roman Zakharov c. Russia* [GC], 2015 (§ 238); *Glukhin c. Russia*, 2023, (§§ 65-73, 82-83); *Leander c. Svezia*, 1987, § 49; *K.U. c. Finlandia*, 2008, §§ 43-50; *Perry c. Regno Unito*, 2003, §§ 41-42

[81] Si vedano, ad esempio, i criteri stabiliti dalla Corte EDU nel caso *Weber e Saravia c. Germani*a e confermati dalla giurisprudenza successiva

[82] A. Lubin, *The rights to privacy and data protection under international humanitarian law and human rights law*, cit., p. 470

[83] *O.c.* pp. 468-470

[84] V., *Zòltan Varga c. Slovacchia*, 2021, § 151

[85] V., *Segerstedt-Wiberg e al. c. Svezia*, 2006, § 88; *Glukhin c. Russia*, 2023, § 86

[86] V., *Podchasov c. Russia,* 2024, § 62

sticate[87]. È dunque possibile ricostruire sulla vasta giurisprudenza presente quelli che dovrebbero essere gli obblighi per gli Stati che impiegano intelligenza artificiale nei conflitti armati, *adattandoli* alla particolarità di tali contesti, al fine non solo di garantire il rispetto del DIU, ma anche di non far venire meno le garanzie *minime* nella protezione della privacy degli individui. Nel nostro caso, sarebbe dunque doveroso per gli Stati adottare preventivamente norme apposite sulla limitazione del diritto alla privacy nell'impiego di sistemi di IA nei conflitti armati. Nella giurisprudenza della Corte EDU è richiesto che tali norme siano sufficientemente specifiche da indicare, tra le altre, le condizioni e le modalità in cui le autorità Statali possono adottare misure volte alla raccolta di dati, nonché le garanzie adottate al fine di evitare abusi da parte delle autorità, come ad esempio la natura, lo scopo e la durata di tali operazioni, e le autorità autorizzate a compierle[88]. Conseguentemente, gli Stati dovrebbero assicurare non solo il rispetto del principio di legalità, ma anche che limitazioni al diritto alla privacy avvengano in conformità con la necessità dello scopo da raggiungere nell'impiego di una determinata tecnologia, raccogliendo solo quei dati considerati strettamente necessari. Ad esempio, dovranno essere raccolti e processati solo quei dati essenziali per la corretta identificazione di combattenti al fine di salvaguardare i civili e, quindi, rispettare gli obblighi previsti dall'articolo 57 del Primo protocollo addizionale. Considerazione dovrà essere data anche al mantenimento della proporzionalità tra la limitazione del diritto e tale scopo, al fine di evitare ingerenze eccessive. In tal senso, accorgimenti potrebbero essere previsti in merito alla limitazione temporale di immagazzinamento dei dati raccolti, cosicché essi non siano conservati per periodi di tempo illimitati, anche in seguito alla conclusione delle ostilità. Inoltre, sarà dovere degli Stati che impiegano tali tecnologie adoperarsi al fine di assicurare la protezione di tali dati, proteggendoli da possibili attacchi o impedendone la diffusione a terze parti, se non in casi esplicitamente previsti e dettati da necessità inerenti alla condotta delle ostilità.

Tali sono solo esempi dei possibili accorgimenti che possono essere adottati dagli Stati nell'impiego dei suddetti sistemi al fine di garantire una protezione minima del diritto alla privacy nei conflitti armati, prendendo come modello di riferimento le limitazioni al diritto adottate già in tempo di pace. A ciò si deve aggiungere il ruolo dell'articolo 36 del Primo protocollo addizionale, che verrà di seguito analizzato.

---

87 V., *Catt c. Regno Unito*, 2019, § 114

88 V., *Shimovolos c. Russia*, 2011, § 68

4.2 *Il ruolo dell'articolo 36 del Primo protocollo addizionale alle Convenzioni di Ginevra*

In sede di negoziato del Primo Protocollo Addizionale, divenne evidente la necessità di trovare un modo per mettere concretamente in atto la proibizione o limitazioni dei mezzi/metodi di guerra rientranti nelle categorie previste dal Protocollo[89]. Dopo varie negoziazioni, dunque, nell'articolo 36 venne introdotto l'obbligo per le parti in conflitto di determinare la conformità di nuove armi, mezzi o metodi di guerra alle norme del Protocollo e, più in generale, del diritto internazionale, prima che essi vengano impiegati in contesti operativi.[90] Sono due gli aspetti dell'articolo 36 che lo rendono particolarmente rilevante ai fini di questa analisi. Il primo riguarda il fatto che non solo le armi, ma tutti i mezzi e metodi di guerra «debbano» essere inclusi nella revisione. Il secondo concerne la necessità che i nuovi mezzi e metodi di guerra siano conformi non solo al DIU, ma al diritto internazionale nel suo complesso, e quindi anche al diritto internazionale dei diritti umani[91]. Conseguentemente, si argomenterà in questa sede che quelle applicazioni dell'IA che possono essere incluse all'interno della categoria giuridica dei mezzi/metodi di guerra devono essere sottoposte alle revisioni previste *ex* articolo 36 e che anche il diritto alla privacy possa essere incluso tra le norme applicabili che devono essere rispettate prima dell'impiego di tali sistemi.

Per quanto concerne la prima argomentazione, è necessario richiamare l'analisi effettuata nel terzo paragrafo in merito alla classificazione di determinate applicazioni di IA come parte dei mezzi/metodi di guerra. Ci si riferisce in particolare all'uso di DSS per il *targeting* ed altri aspetti inerenti alla condotta delle ostilità e all'uso di armi autonome. Se, per quest'ultimo caso, pochi dubbi insorgono in merito alla necessità di revisionare tali sistemi d'arma *ex* articolo 36, meno im-

---

[89] Commentario del 1987 all'articolo 36 del primo Protocollo Addizionale. Disponibile a: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-36/commentary/1987

[90] Al momento, la natura consuetudinaria di questo obbligo è ancora soggetta a discussioni. Per una visione a favore della sua natura consuetudinaria CICR, *A Guide to legal review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, International Review of the Red Cross, Vol. 88 n. 864, 2006, p. 933 ; per una visione contraria, v. N. Jevglevskaja, *Weapons review obligation under customary international law*, International Law Studies, 2018, p. 209 ss

[91] Ad esempio, v. riferimento dello Human Rights Committe sulla necessità di tenere in considerazione il rispetto del diritto alla vita nella revisione di nuovi mezzi e metodi di guerra: Human Rights Committee, *General Comment No. 36 (2018) on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life*, 30 October 2018, UN Doc. CCPR/C/GC/36, § 65.

mediata pare l'estensione di tale obbligo ai DSS[92]. Come si è già avuto modo di sottolineare, infatti, i DSS non sono armi in senso stretto, sebbene possano avere effetti diretti e indiretti rilevanti ai fini della condotta delle ostilità. È opinione di chi scrive che tali impieghi di IA dovrebbero essere inclusi tra i mezzi e metodi di guerra da sottoporre a revisione. Tale necessità è stata espressa anche da parte della dottrina che si è occupata della materia[93]. Viene infatti riconosciuto come il loro impiego abbia inevitabili ripercussioni sull'uso della forza, incidendo dunque sulla pianificazione, tanto a livello operativo quanto tattico[94]. Essi, dunque, rientrerebbero nella definizione di mezzi di guerra data da Yoram Dinstein («*equipments modyfing military capabilities*»)[95]e in quella di mezzi e metodi di guerra fornita da Justin McClelland («*[…] items of equipment which, whilst they do not constitute a weapon as such, nonetheless have a direct impact on the offensive capability of the force to which they belong*»)[96]. Tale approccio sembra confermato anche dalla *US Political Declaration*, nella quale, al punto B, si esprime la necessità di assicurarsi, anche tramite le revisioni, che i sistemi di IA impiegati operino in conformità con il diritto internazionale[97].

---

[92] Ad esempio, v.: N. Jevglevskaja, *Challenges to Article 36 Reviews Posed by Autonomous Weapons Systems (AWS*), In *International Law and Weapons Review: Emerging Military Technology under the Law of Armed Conflict*, Cambridge, 2021, pp. 207-238

[93] CICR, *Artificial Intelligence and Machine Learning in armed conflicts: a human centred approach,* International Review of the Red Cross, cit., p. 464; K. Klonowska, *Shifting the narrative: not weapons, but technologies of warfare*, *o.c.* ; J. McClelland, *The review of weapons in accordance with Article 36 of Additional Protocol I*, cit., ; V. Boulanin, D. Lewis, *A Responsible reliance concerning development and use of AI in the military domain,* cit., p. 8; K. Klonowska, *Article 36: Review of AI Decision Support Systems and other Emerging Technologies of Warfare*, cit.

[94] CICR, Geneva Academy, *Artificial Intelligence and Related Technologies in Military Decision Making on the Use of Force in Armed Conflicts, Current Developments and Potential Implications,* cit.

[95] Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict,* cit., p. 115

[96] J. McClelland, *The review of weapons in accordance with Article 36 of Additional Protocol I*, cit., p. 401

[97] US Department of State, *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, 9 novembre 2023, cit. Sul punto: S. Steene, C. Jenks, *The Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, Lieber Institute Westpoint Articles of war, 13 novembre 2023, disponibile a: https://lieber.westpoint.edu/political-declaration-responsible-military-use-artificial-intelligence-autonomy/

Tale inclusione non è fine a sé stessa. Essa, infatti, ci conduce al secondo aspetto di questa analisi, vale a dire la necessità per gli Stati vincolati dall'articolo 36, di considerare nella loro valutazione dei mezzi/metodi di guerra sopra descritti anche le norme inerenti alla protezione del diritto alla privacy e dei dati personali. Bisogna però fare una precisazione: raramente le norme sui diritti umani sono state considerate dalla dottrina tra le norme di diritto internazionale applicabili *ex* articolo 36[98]. Infatti, nelle linee guida stilate dal Comitato Internazionale della Croce Rossa, non viene fatto riferimento alle norme sui diritti umani, ma solamente alle norme del diritto internazionale che riguardano la disciplina di armi specifiche, piuttosto che norme rilevanti del diritto penale internazionale[99]. Tuttavia, si vogliono sottolineare qui due elementi fondamentali. Il primo riguarda la già descritta applicabilità del diritto internazionale dei diritti umani nei contesti di conflitto armato[100]; il secondo, l'assoluta novità che l'impiego di IA nei mezzi/metodi di guerra rappresenta, nonché le implicazioni che tale impiego comporta per il rispetto dei diritti umani e del diritto alla privacy. In considerazione di questi elementi, emerge la necessità di far fronte alle sfide poste dall'impiego dell'IA nei conflitti armati ampliando l'interpretazione dell'articolo 36 fino ad includere la protezione del diritto alla privacy. Con ciò non si vuole suggerire che un sistema d'arma autonomo o un DSS possa essere proibito a causa dell'incapacità di rispettare il diritto alla privacy; una tale ipotesi sembra irragionevole, specialmente qualora tali sistemi rispettino tutti i requisiti previsti dal DIU. Tuttavia, dato il sempre più evidente impatto dell'IA sulla privacy e sulla vita degli individui i cui dati vengono utilizzati nella fase di addestramento ed impiego di questi sistemi, tramite gli obblighi imposti dall'articolo 36 maggiore attenzione potrebbe essere data nel verificare se e come nel loro normale utilizzo di questi sistemi il diritto alla privacy ed alla protezione dei dati vengano compromessi e, in caso, mettere in essere determinati parametri o regolamentazioni per limitarne l'impatto[101]. Ad esempio, gli Stati potrebbero adottare accorgimenti finalizzati ad evitare che i dati siano raccolti ed immagazzinati senza limiti di tempo, o, ancora,

---

[98] Ad esempio, v. S. Casey-Maslen, N. Corney e A. Dymond-Bass, *The review of weapons under international humanitarian law and human rights law*, in *Weapons under International Human Rights Law*, Cambridge, 2014, pp. 411-447; H. M. Laufe, *War, weapons and watchdogs: an assessment of the legality of new weapons under international human rights law*, Cambridge International Law Journal, Vol. 6 No. 1, pp. 62-74

[99] CICR, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare Measures to Implement Article 36 of Additional Protocol I of 1977*, sito web del Comitato Internazionale della Croce Rossa, 2006, pp. 10-19

[100] *Infra* § 4.1

[101] S. Casey-Maslen, N. Corney e A. Dymond-Bass, *The review of weapons under international humanitarian law and human rights law*, cit., p. 421

che siano raccolti dati non strettamente necessari allo scopo per il quale viene impiegato il sistema. Ciò permetterebbe di creare un bilanciamento tra le necessità di efficienza del sistema d'arma o dei DSS e il diritto alla privacy degli individui i cui dati e le cui informazioni vengono utilizzate dalle varie applicazioni di IA.

5. *Riflessioni conclusive*

L'analisi effettuata ha voluto mettere in luce le criticità legate all'impiego dell'IA nei conflitti armati in relazione alla tutela del diritto alla privacy. L'importanza del rispetto di tale diritto non può essere sottovalutata. Dato il sempre crescente impiego dell'IA, il diritto alla privacy inevitabilmente ricopre una posizione centrale tra i diritti umani potenzialmente colpiti dall'impiego di tale tecnologia. Ciò è vero sia in tempo di pace, che in tempo di guerra. La sempre maggiore possibilità di sorveglianza, profilazione, identificazione e nonché di immagazzinare informazioni biometriche anche nel lungo periodo possono avere conseguenze sulla tutela di diversi diritti umani, come quello di non discriminazione, della libertà di espressione o assemblea nel breve e nel lungo periodo[102]. Non a caso, dunque, è stato affermato come il rispetto del diritto alla privacy possa fungere da scudo anche nella protezione e nel godimento di questi diritti. Ciononostante, si è cercato di mettere in evidenza una generale mancanza di attenzione, sia da parte della dottrina che da parte degli Stati, in merito all'importanza della tutela della privacy degli individui nei contesti di conflitto armato. Il tutto aggravato dal fatto che poca – se non nessuna- considerazione alla tutela della privacy viene data dalle norme del DIU. Sebbene, come si è visto, il diritto alla privacy continui ad applicarsi nei contesti di conflitto armato, anche la mancanza di giurisprudenza sul punto e la complessa relazione tra diritti umani e DIU contribuiscono a rendere sfocata l'effettiva rilevanza di tale diritto in situazioni di conflitto armato, specialmente in merito all'utilizzo dell'IA nei mezzi e nei metodi di guerra.

Tuttavia, in sede di conclusione, vi sono due elementi che si vogliono sottolineare. Il primo riguarda la possibilità di non disapplicare del tutto questo diritto anche nel caso in cui si verifichi un contrasto con norme specifiche del DIU e, nel dettaglio, col principio di precauzione. Infatti, tramite l'adozione di regolamentazioni specifiche, sarebbe possibile porre degli accorgimenti al fine di mantenere una, seppur minima, continuità nella protezione della privacy in con-

[102] Ad esempio v: M. Warthon, *Artificial Intelligence and Freedom of Assembly*, in *Artificial Intelligence and Human Rights*, pp. 91-103; L. Koen, K. Mufamadi, *Artificial Intelligence and Racial Discrimination*, in *Artificial Intelligence and Human Rights,* pp. 195-206

siderazione della possibilità di apporre apposite restrizioni qualora necessario. Il secondo concerne le potenzialità intrinseche dell'articolo 36 del Primo protocollo addizionale di aprire uno spiraglio verso l'inclusione di accorgimenti specifici per la tutela della privacy nello studio, sviluppo o acquisto di mezzi e metodi di guerra che impiegano algoritmi di IA.

Sebbene entrambi questi aspetti necessitino e meritino ulteriori ricerche, essi potrebbero garantire il mantenimento di, almeno, un livello minimo di protezione di un diritto spesso dato per scontato.

La persona vulnerabile ai tempi dell'IA: emozioni, diritti fondamentali e forme di tutela rafforzata

di **Sabrina Akram Ibrahim El Sabi**

1. *Premessa*

L'espansione delle tecnologie digitali ha reso l'impiego dei sistemi di IA[1] sempre più pervasivo nella vita quotidiana e nei rapporti sociali[2], ponendo nuove sfide in termini di tutela[3].

---

[1] Cfr. E. Calzolaio, *I Dispositivi medici «intelligenti»: spunti di comparazione giuridica*, in *Il Foro Italiano*, 2, 2022, p. 75 ss.

[2] T. Evas, *The EU Artificial Intelligence Act: Advancing Innovation for Trustworthy AI*, in *AIRe*, 1, 2024, p. 99 ss.; O. Lobel, *The Law of AI for Good*, in *Florida Law Review*, 75, 6, 2023, p. 1139; G. Cerrina Feroni, *AI e diritto: "L'umanesimo digitale diventa concreto solo con le regole"*, *Garante per la Protezione dei dati personali*, 2024, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9977187; D. Castro, *The EU's AI Act Is Premature, Says ITIF*, 2023, https://itif.org/publications/2023/12/08/the-eu-ai-act-is-premature/; G. Scorza, *Scorza: AI Act è a rischio, ecco le regole che servono - Intervento di Guido Scorza*, *Garante per la protezione della privacy*, 2023, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9960565; L. d'Avack, *Intelligenza artificiale e diritto: problematiche etiche e giuridiche*, in *Diritto di Famiglia e delle Persone (II)*, 4, 1, 2023, p. 1710 ss.

[3] A. Mantelero, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template*, in *Computer Law & Security Review*, 54, 2024, p. 1; V. Zeno-Zencovich, *Artificial Intelligence, Natural Stupidity and Other Legal Idiocies*, in *MediaLaws*, 2024, https://www.medialaws.eu/rivista/artificial-intelligence-natural-stupidity-and-other-legal-idiocies/; D.U. Galetta, *Human-stupidity-in-the-loop? Riflessioni (di un giurista) sulle potenzialità e i rischi*

Esaminando il quadro giuridico delineatosi recentemente in Europa, è interessante soffermarsi sulle principali problematiche causate dalla proliferazione delle tecnologie di IA utilizzate per regolare e implementare determinati settori (si pensi, ad esempio, a quelle che si occupano della cura, dell'assistenza e del benessere di specifici gruppi di soggetti vulnerabili[4]), mirando all'individuazione di strumenti di tutela che possano essere utilizzati dall'utente in caso di discriminazione algoritmica e violazione dei diritti fondamentali[5].

L'uso dei sistemi di IA, dunque, solleva questioni significative relative ai dati, ai *bias* algoritmici[6], all'esclusione digitale e alle possibili lesioni ad altri diritti fondamentali tra cui quello alla non discriminazione, oltre che alla dignità e all'autodeterminazione di un individuo vulnerabile[7].

Pertanto, con l'evoluzione di questa tecnologia trasformativa, acquista rilievo l'analisi dell'impatto dell'IA sui soggetti più fragili della società (in cui rientrano diversi gruppi tra cui i minori, gli anziani, i disabili, gli immigrati ecc..).

La ricerca mira ad indagare le questioni giuridiche generate dagli emergenti sistemi di IA, con particolare riferimento ai sistemi di rilevamento delle emozioni degli utenti, partendo dalla creazione e dallo sviluppo responsabile di tali tecnologie, per poi concentrarsi sulle problematiche connesse alla tutela del diritto di non discriminazione degli individui che utilizzano questi dispositivi. Si esploreranno, infine, le possibili soluzioni normative e i meccanismi di protezione (in cui rientrano strumenti di prevenzione come il *Fundamental Rights Impact Assessment*[8]) disponibili per gli utenti vulnerabili in caso di pregiudizi e violazione dei diritti fondamentali[9].

---

dell'Intelligenza Artificiale, in *federalismi.it*, 5, 2023, 4 ss., https://www.federalismi.it/nv14/editoriale.cfm?eid=665.

[4] C. Equizi, *Il limite delle risorse disponibili nella tutela dei diritti delle persone vulnerabili*, in *Dirittifondamentali.it*, 2, 2023, p. 690 ss.; V. Lorubbio, *La tutela dei soggetti vulnerabili*, in *DPCE online*, 1, 2020, p. 661 ss.; R. Calo, *Privacy, Vulnerability and Affordance,* in *DePaul Law Review*, 66, 2017, p. 592.

[5] A. Astone, *Sistemi intelligenti e regole di responsabilità*, in *Persona e Mercato*, 3, 2023, p. 485 ss.

[6] S. Santini, *IA emotiva e bias algoritmici. L'impatto nel settore sanitario*, in *AgendaDigitale*, 2024, https://www.agendadigitale.eu/sanita/ia-emotiva-e-bias-algoritmici-limpatto-nel-settore-sanitario/.

[7] Cfr. C. Irti, *L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano*, in *Persona e Mercato*, 1, 2023, p. 47 ss.

[8] V., *infra*, par. 3.1.

[9] European Union Agency for Fundamental Rights, *Getting the future right– Artificial intelligence and fundamental rights*, 2020, https://fra.europa.eu/en/

2. *IA e rilevamento delle emozioni: opportunità, rischi e implicazioni*

In questo contesto, caratterizzato dalla diffusione delle innovazioni tecnologiche[10], è opportuno fare delle valutazioni sulle conseguenze giuridiche (negative e positive) derivanti dall'evoluzione del settore dell'IA emotiva[11].

Trattasi di tecnologie la cui disciplina è stata inserita all'interno dell'AI Act[12] e che sono classificate come sistemi di IA "ad alto rischio[13]" i quali, sebbene perseguano interessi generali volti a migliorare la qualità della vita di diverse categorie di soggetti/utenti, non offrono sicura tutela all'autodeterminazione informativa e alla privacy[14] dei medesimi.

Questa particolare categoria di sistemi – un sottoinsieme dell'IA che misura, comprende, simula e reagisce alle emozioni umane, nota come *Emotion Recognition Technology* (ERT[15]) – si è sviluppata negli ultimi tempi ed è strettamente connessa all'ambito del c.d. *Affective Computing*[16].

---

publication/2020/artificial-intelligence-and-fundamental-rights.

[10] H. Hyden, *AI, Norms, Big Data, and the Law*, in *Asian Journal of Law and Society*, 7, 3, 2020, p. 409 ss.

[11] Per un'analisi dei dispositivi di riconoscimento emozionale sia consentito rinviare a S. El Sabi, *IA e Data Protection nei dispositivi elettronici: riconoscimento delle emozioni e prospettive di tutela per i soggetti vulnerabili*, in *DPCE online*, 64, 2, 2024, p. 1049 ss.; E.M. Incutti, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale*, in *Giustiziacivile*, 2022, p. 515 ss.

[12] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), pubblicato in Gazzetta ufficiale il 12.7.2024.

[13] Cfr. Allegato III AI Act.

[14] A. Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI*, Asser Press-Springer, 2022, *passim*.

[15] K. McInerney and O. Keyes, *The Infopolitics of feeling: How race and disability are configured in Emotion Recognition Technology*, in *New Media & Society*, 2024, https://journals.sagepub.com/doi/full/10.1177/14614448241235914.

[16] P. Ekman and W.V. Friesen, *The Reportoire of Nonverbal Behaviour: Categories, Origins, Usage and Coding*, in *Semiotica*, 1, 1969, p. 49 ss.; *Id.*, *Constans Across Cultures in the Face and Emotion*, in *Journal of Peronality and Social Psycholy*, 17, 2, 1971, p. 124 ss.; R. Picard, *Affective Computing*, in *MIT Media Laburatory Percetual Computing Section Technical Report*, 1995; A. Häuselmann, *Fit for Purpose? Affective Computing Meets EU Data Protection Law*, in *International Data Privacy Law*, 11, 3, 2021, p. 245 ss.

In linea generale, tali tecnologie[17], basate su procedimenti automatizzati[18], alimentano la loro operatività con un'immissione continua ed esponenziale di dati[19] (relativi alla salute, biometrici, emotivi, ecc..) e combinano tra loro distinti elementi di psicologia, scienza cognitiva[20] e informatica, al fine di creare sistemi capaci di comprendere e simulare le risposte emotive umane.

Tali dispositivi, dunque, sono progettati per dedurre lo stato emotivo dell'individuo, a partire dall'analisi delle sue espressioni facciali (pensiamo alle tecniche per il riconoscimento facciale TRF[21]), dal tono di voce, dai movimenti del corpo e da altri dati biometrici e non, utilizzando modelli di *machine learning*[22] e algoritmi di *deep learning*[23].

I sistemi di IA emotiva sono tra le applicazioni tecnologiche in più rapida diffusione, con utilizzi molto diversi per settore (quello del *marketing*, della pubblicità, della salute mentale o di quello sanitario più in generale), obiettivi, intensità, incidenza e rischi connessi[24]. La riflessione sulla loro regolamentazione – che

---

[17] E. Steindl, *Does the European Data Protection Framework Adequately Protect Our Emotions? Emotion Tech in Light of the Draft AI Act and Its Interplay with the GDPR*, in *European Data Protection Law Review*, 8, 2, 2022, p. 312 ss.; M. Purdy, J. Zealley e O. Maseli, *The Risks of Using AI to Interpret Human Emotions*, in *Harvard Business Law Review*, 2019, https://hbr.org/2019/11/the-risks-of-using-ai-to-interpret-human-emotions; H. Devlin, *AI Systems Claiming to 'Read' Emotions Pose Discrimination Risks – Expert Says Technology Deployed is Based on Outdated Science and therefore is Unreliable*, in *The Guardian*, 2020, https://www.theguardian.com/technology/2020/feb/16/ai-systems-claiming-to-read-emotions-pose-discrimination-risks.

[18] G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del diritto*, 2, 2019, p. 199 ss.

[19] N. Daga and P. Mehta, *Risk of Using Artificial Intelligence to Interpret Emotions*, in *Indian Journal of Integrated Research Law*, 3, 5, 2023, p. 12.

[20] L. Floridi and A.C. Nobre, *Anthropomorphising Machines and Computerising Minds: The Crosswiring of Languages between Artificial Intelligence and Brain & Cognitive Sciences*, in *Minds and Machines*, 34, 5, 2024, https://link.springer.com/article/10.1007/s11023-024-09670-4.

[21] V. *European Data Protection Supervisor* (EDPS), *Tech Dispatch on Facial Emotion Recognition*, 2021, p. 1 ss.

[22] A. Alslaity and R. Orji, *Machine Learning Techniques for Emotion Detection and Sentiment Analysis: Current State, Challenges, and Future Directions*, in *Behaviour & Information Technology*, 43, 1, 2024, p. 139 ss.

[23] G. Mosca, *Deep learning: cos'è, come funziona e applicazioni*, in *Agenda Digitale*, 2023, https://www.agendadigitale.eu/cultura-digitale/deep-learning-cose-come-funziona-e-applicazioni/.

[24] M.D. Fenwick, W.A. Kaal and E.P. Vermeulen, *Regulation Tomorrow: What Happens When Technology is Faster Than the Law?*, in *American University Business*

avrebbe come principale scopo quello di migliorare l'interazione umana con i dispositivi digitali – solleva aspetti problematici che meritano di essere segnalati, soprattutto facendo riferimento all'IA Act[25].

In proposito, l'art. 3, par. 39) dell'AI Act definisce un "sistema di riconoscimento delle emozioni" come quel «sistema di IA finalizzato all'identificazione o all'inferenza di emozioni o intenzioni di persone fisiche *svolta solamente*[26] sulla base dei loro dati biometrici»[27].

Tra i molteplici aspetti positivi dell'uso di tali dispositivi – che se adeguatamente progettati offrono notevoli possibilità di avanzamento della società e del

Law Review, 6, 3, 2017, p. 591 ss.

[25] A. Orlando, *La regolamentazione delle tecnologie di riconoscimento facciale nell'UE e negli USA: alea IActa est?*, in *DPCE online*, 64, 2, 2024, https://www.dpceonline.it/index.php/dpceonline/article/view/2186.

[26] Corsivo mio.

[27] Nonostante non sia questa la sede per discutere in maniera approfondita sul tema, è necessario segnalare le criticità che la nozione di "dati biometrici" ha di recente sollevato, con particolare riferimento ai sistemi di IA per il riconoscimento delle emozioni. In proposito, la definizione di dati biometrici fornita dal GDPR (art. 3, par. 33), che li qualifica come «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», sembrerebbe adottare termini indefiniti, lasciando spazio a interpretazioni più o meno restrittive. Il riferimento ai dati biometrici del GDPR avrebbe reso la disciplina incompleta e particolarmente limitata. Difatti, interpretando rigorosamente la definizione del GDPR, il rinvio alla nozione di dati biometrici, operato nella precedente versione dell'AI Act, finiva per limitare significativamente ciò che era ricompreso nel concetto di riconoscimento delle emozioni, poiché l'operazione, in tali ipotesi, non necessariamente consente l'identificazione univoca del soggetto interessato. Di qui la necessità di introdurre nel Regolamento una nuova nozione di dato biometrico, escludendo ogni riferimento all'identificazione univoca. E, dunque, ai sensi dell'art. 3, par. 34) dell'AI Act, sono dati biometrici «i dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali l'immagine facciale o i dati dattiloscopici». L'eliminazione del riferimento all'identificazione allarga l'ambito di applicazione, permettendo l'inclusione in tale nozione di sistemi fondati su dati relativi alla pressione sanguigna o al battito cardiaco, al respiro, alla temperatura corporea, all'attività elettrica cerebrale. Dubbi persistono, tuttavia, sull'inclusione in questa più ampia nozione – quindi nella categoria di dato biometrico e, conseguentemente, di quella di riconoscimento delle emozioni – software che rilevano le emozioni dell'utente da un testo scritto, attraverso l'analisi dell'impostazione e della scelta delle parole, a meno che non venga interpretata in modo particolarmente ampio la nozione di dato personale attinente «alle caratteristiche (…) comportamentali di una persona fisica» (art. 3, par. 34).

mercato digitale – si rammentano quelli che possono essere utilizzati per il monitoraggio dello stato di salute e di benessere di un soggetto[28],

(dalla sperimentazione clinica virtuale, all'individuazione di soggetti fortemente a rischio di contrarre determinate patologie), così come per il suo benessere psicologico, consentendo una migliore comprensione delle condizioni emotive[29] del paziente-utente e facilitando la diagnosi di disturbi psicologici[30].

Il graduale ed esponenziale ingresso dell'IA in ambito sanitario, con particolare riferimento ai dispositivi medici[31], ha portato le istituzioni europee a promuovere e implementare un quadro normativo[32] idoneo a favorire l'attuazione di progetti multinazionali necessari per la trasformazione digitale dell'Ue, innovando, in questo modo, il settore della produzione di *device AI-based* in medicina e in quello dell'assistenza e del benessere delle persone[33].

---

[28] V.E. Gutierrez Maestro, T.R. De Almeida, E. Schaffernicht and Ó. Martinez Mozos, *Wearable-Based Intelligent Emotion Monitoring in Older Adults during Daily Life Activities*, in *Applied Sciences*, 13, 9, 2023, p. 1 ss.

[29] Y. Cai, X. Li and J. Li, *Emotion Recognition Using Different Sensors, Emotion Models, Methods and Datasets: A Comprehensive Review*, in *Sensors*, 23, 2023, p. 2455 ss., chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10007272/pdf/sensors-23-02455.pdf; J.S. Bard, *Developing Legal Framework for Regulating Emotion AI*, in *Boston University Journal of Science & Technology Law*, 27, 2, 2021, p. 272 ss.

[30] L. Montalbano, *Brain-Machine Interfaces and Ethics: A Transition from Wearable to Implantable*, in *Journal of Business & Technology Law*, 16, 2, 2021, p. 191 ss. Si pensi, ad esempio, all'utilizzo delle piattaforme connesse ai *wearable devices* o, ancora, a talune applicazioni diffuse negli USA, come *SimSensei*, utilizzate per migliorare l'umore dei pazienti. Sul punto, D. Devault, R. Artstein, G. Benn, T. Dey *et al.*, *SimSensei Kiosk: A Virtual Human Interviewer for Healthcare Decision Support, Conference: Proceedings of the 2014 International Conference on Autonomous Agents and Multi-agent Systems*, 2014, p. 1061 ss.

[31] E. Giusti, *La sanità elettronica: dati sanitari relativi alla salute, applicazioni e rischi*, in *Rivista italiana di medicina legale*, 1, 2023, p. 86 ss.

[32] Cfr. A. Fiorentini, *Salute digitale nell'Unione europea: tra innovazione ed equo accesso all'assistenza sanitaria*, in V. Salvatore (a cura di), *Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea*, Torino, 2023, 3-4 ss. Si consulti altresì la Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio del 14 dicembre 2022, con cui è stato istituito il programma strategico per il decennio digitale 2030, GUUE L 323, 2022, 4-26. Tale decisione fa seguito alla comunicazione COM(2021)118 final del 9 marzo 2021, "Bussola per il digitale 2030: il modello europeo per il decennio digitale".

[33] 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. 370 ss.

L'impiego di dispositivi tecnologici, previsto per assicurare una migliore tutela della salute degli individui (specialmente quella dei soggetti più fragili), diventa un ulteriore strumento a garanzia di un elevato livello di protezione della salute psico-fisica umana[34]. Monitorando gli stati emotivi degli utenti, gli operatori sanitari possono personalizzare il loro approccio per migliorare i risultati e fornire un'assistenza mirata.

Si assiste, pertanto, ad una vera e propria rivoluzione che presenta numerose sfide ed elevati rischi, considerando la sensibilità dei dati relativi alla salute degli individui, le esigenze di tutela della riservatezza, nonché le possibili distorsioni cognitive dovute ad assunzioni errate nel processo di apprendimento automatico.

L'ulteriore applicazione nel campo dell'*Affective Computing* e, quindi, dei sistemi di IA emotiva riguarda proprio il settore commerciale, con particolare riferimento agli strumenti di *marketing*[35] (o *neuromarketing*[36]), con cui si cerca di

---

[34] Cfr. art. 35 della Carta dei diritti fondamentali dell'Unione europea.

[35] R. Calo, *Digital Market Manipulation*, in *George Washington Law Review*, 82, 2014, p. 995 ss.; V. Marda and E. Jakubowska, *Emotion (Mis)Recognition: is the EU missing the point?*, in *European Digital Rights (EDRi)*, 2023, https://edri.org/our-work/emotion-misrecognition/. In tema di strategie aggressive di *marketing* digitale e di manipolazione, si veda, inoltre, V.V. Cuocci, *La protezione dei dati personali dei soggetti vulnerabili nella dimensione digitale – Uno studio di diritto comparato*, Bari, 2022, p. 11 s., la quale precisa che «Il *marketing* digitale si basa essenzialmente sulla raccolta dei dati e sul costante monitoraggio dei soggetti e della loro attività *online*. I dati raccolti ed integrati in una rete sofisticata di altoparlanti intelligenti, elettrodomestici intelligenti, sorveglianza, app hanno lo scopo di rendere i consumatori ricettivi alle tecniche di *marketing* digitale. L'ultima frontiera al centro di una strategia pubblicitaria mirata è la creazione di "profili di persuasione" personalizzati in combinazione con una strategia di *targeting* adattivo che trasmette il messaggio giusto al posto giusto, nel tempo e nel luogo per il consumatore giusto. Queste strategie sono basate su dati come l'età o il sesso, o su elementi ancor più dettagliati di *targeting* (ad esempio, corrispondenza delle caratteristiche demografiche con il comportamento osservato) fino a forme molto più raffinate e complesse di *targeting* psicografico, che si basano su elementi psicologici ed emozionali, sulla personalità e sul comportamento di un consumatore, sui suoi valori, opinioni e interessi. Il pericolo relativo alle tecniche manipolative e di *targeting* è ulteriormente acuito dall'utilizzo dell'intelligenza artificiale che si 'nutre', appunto, di dati personali. Sul punto può osservarsi che il *targeting* comportamentale si compone di tre fasi: raccolta dei dati personali, analisi e valutazione dei dati formulata dall'algoritmo in chiave predittiva. Il risultato porta non solo alla conoscenza dei gusti e delle preferenze di un soggetto, ma anche dei punti di debolezza del soggetto».

[36] V.J.C. Cerro Rodrìguez, A. Antonovica and D.L. Sutil Martìn, *Consumer Neuroscience on Branding and Packaging: A Review and a Future Research Agenda*, in *International Journal of Consumer Studies*, 2023, p. 1 ss.

comprendere le reazioni dei consumatori-utenti[37] digitali e che determinano la progressiva erosione degli spazi di autonomia della decisione dell'individuo (oltre che a sollevare questioni legate soprattutto alle ipotesi di manipolazione e sfruttamento delle emozioni degli utenti).

Le istanze di tutela dei diritti della persona, che l'impiego dei dati personali per alimentare il funzionamento e l'implementazione delle tecnologie di IA ha portato alla luce, si pongono in diretta continuità con questo nuovo ambito giuridico, recentemente sorto nel contesto della disciplina sull'IA[38]. Le ulteriori tecnologie che fanno uso delle emozioni per catturare i gusti degli utenti e che hanno richiesto tale intervento giuridico a tutela della persona sono le c.d. neurotecnologie[39], quelle tecnologie in grado di codificare in modo più diretto e dettagliato il contenuto degli stati mentali di un individuo, compresi quelli comunicati tramite il linguaggio verbale, i testi scritti e il comportamento osservabile[40].

La tutela del singolo, nel nuovo scenario digitale, consiste nella necessità di garantire all'individuo un potere di controllo sulla massa di dati che lo riguardano e che vengono quotidianamente acquisiti e gestiti da terzi.

In tale settore, l'individuo, ai fini delle proprie decisioni d'acquisto, è scrutato a partire dal proprio linguaggio del corpo che un tempo si riteneva non essere codificabile in termini economici, e che, invece, ora si declina in un'ingente quantità di dati costituti non solo dalla lettura della voce e del relativo tono, ma anche dai movimenti facciali, dal tempo che l'utente impiega a leggere o ad interagire con un annuncio pubblicitario[41]. «I dati così raccolti permettono alle imprese di studiare le abitudini, ma soprattutto, di prevedere la risposta emotiva dell'utente digitale, divenuto immediatamente raggiungibile tramite i medesimi

---

[37] M. Goncalves, Y. Hu, I. Aliagas and L.M. Cerdá, *Neuromarketing algorithms' consumer privacy and ethical considerations: challenges and opportunities*, in *Cogent Business & Management*, 11, 1, 2024, p. 5 ss.

[38] S. Trozzi, *Il principio della finalità del trattamento dei dati personali alla prova dei recenti sviluppi in tema di intelligenza artificiale: il caso ChatGPT e la neuroprivacy*, in *federalismi.it*, 1, 2024, p. 197 ss.

[39] P.M. Oliveira, J. Guerreiro e P. Rita, *Neuroscience Research in Consumer Behavior: A Review and a Future Research Agenda*, in *International Journal of Consumer Studies*, 2022, p. 2041 ss.

[40] Cfr. ancora S. Trozzi, *Il principio della finalità del trattamento dei dati personali alla prova dei recenti sviluppi in tema di intelligenza artificiale: il caso ChatGPT e la neuroprivacy*, cit., p. 197 ss.

[41] G. Scorza, *Neuroverso. Il cervello è nudo. Quale impatto sulle nostre vite, diritti e libertà*, Milano, 2023, *passim*; J.R. Flahaux, B.P. Green and A.G. Skeet, *Ethics in the Age of Disruptive Technologies: An Operational Roadmap*, Markkula Center for Applied Ethics Santa Clara University, 2023, *passim*.

strumenti impiegati per targhettizzarlo (smartphone, tablet, computer, dispositivi *IoT*, smartwatch)»[42].

È infatti noto che l'applicazione di tali dispositivi al *marketing* mira allo sfruttamento delle emozioni per fini commerciali. L'IA emotiva facilita la raccolta di reazioni[43] e permette di personalizzare (ma anche di tracciare e manipolare) ulteriormente le comunicazioni commerciali e di ottimizzare le campagne di *marketing* in tempo reale[44]. Per tale ragione, gli interpreti si sono interrogati sulla necessità di introdurre una disciplina più adeguata, volta a prevenire o a far cessare le crescenti pratiche di manipolazione da parte degli algoritmi, poiché l'attuale panorama normativo parrebbe non essere in grado di accogliere adeguatamente tali sviluppi[45].

In proposito, è bene concentrare l'attenzione sul quadro normativo europeo e sull'impiego delle emozioni umane per scopi commerciali *business-to-consumer* (B2C), ma anche nel contesto di altri usi altamente rilevanti dell'IA emozionale[46].

L'adozione in diverse aree del diritto comunitario e nazionale di norme tradizionali a tutela dei consumatori per la limitazione delle forme di manipolazione e sfruttamento nei rapporti tra imprese e parti deboli del rapporto risulta insufficiente e non è più in grado di fornire una risposta esaustiva alle questioni sorte nella società algoritmica.

Pertanto, è fondamentale che «la progettazione e l'uso di software persuasivi e di algoritmi di tecnologie dell'informazione e della comunicazione (TIC) o di IA rispettino pienamente la dignità e i diritti umani di tutti gli utenti, in particolare di quelli più vulnerabili, come gli anziani[47] o le persone con disa-

---

[42] S. Trozzi, *Il principio della finalità del trattamento dei dati personali alla prova dei recenti sviluppi in tema di intelligenza artificiale: il caso ChatGPT e la neuroprivacy*, cit., p. 224.

[43] D. Clifford, *The Legal Limits to the Monetisation of Online Emotions*, Tesi di dottorato, KU Leuven, Faculty of Law 2019, p. 103 ss.

[44] C. Burr, N. Cristianini and J. Ladyman, *An Analysis of the Interaction between Intelligent Software Agents and Human Users*, in *Minds and Machines*, 2018, p. 735; C. Burr and N. Cristianini, *Can Machines Read Our Minds?*, in *Minds and Machines*, 29, 2019, p. 461.

[45] P. Valcke, D. Clifford and V.K. Dessers, *Constitutional Challenges in the Emotional AI Era*, in H-W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor and G. De Gregorio (eds), *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2021, p. 63.

[46] *Ibid.*, p. 57 ss.

[47] C. Bozzaro, J. Boldt and M. Shweda, *Are Older People a Vulnerable Group? Philosophical and Bioethical Perspectives on Ageing and Vulnerability*, in *Bioethics*, 32, 4,

bilità[48]». In effetti, i processi di *machine learning* conferiscono a queste tecnologie una capacità di autoapprendimento che consente loro di operare con un elevato grado di autonomia, nonostante la loro persistente opacità, generando potenziali pregiudizi (si pensi, ad esempio, agli errori di profilazione) per le libertà e i diritti fondamentali.

Per tale ragione, il legislatore europeo e le istituzioni hanno evidenziato l'urgente necessità di progettare le nuove tecnologie al fine di preservare la dignità e l'autonomia umana, fisica e psicologica.

2.1 Bias *algoritmici e discriminazione dei soggetti vulnerabili. Un fenomeno complesso*

Uno dei principali rischi associati all'IA e, in particolare, all'*Emotional AI*, è che, accanto ai molti utilizzi benefici, tali sistemi possano essere utilizzati impropriamente, conducendo spesso a risultati discriminatori[49], escludendo determinati gruppi di individui e violando principi fondamentali come il diritto alla

---

2018, p. 233 ss., i quali in proposito sostengono la tesi della vulnerabilità dell'anziano intesa in senso "posizionale" e non quale categoria vulnerabile *tout court*. La vulnerabilità delle persone anziane, difatti, dipenderebbe dalle azioni poste in essere dallo stesso una volta calato in un determinato contesto (come ad esempio, la dimensione digitale). V., ancora, V.V. Cuocci, *La protezione dei dati personali dei soggetti vulnerabili nella dimensione digitale – Uno studio di diritto comparato*, cit., p. 185, «la scarsa dimestichezza dell'anziano con le tecnologie, oltre che le ridotte capacità cognitive e fisiche legate al fisiologico invecchiamento determinano una difficoltà per quest'ultimo». Appare, di conseguenza, infruttuosa, nell'ambito della dimensione digitale, la distinzione tra anziano non autosufficiente o affetto da patologie capaci di minarne l'autonomia, e anziano autosufficiente, privo di patologie. Sull'anziano vulnerabile, v. C.M. Cascione, *Il lato grigio del* diritto. Invecchiamento della popolazione e tutela degli anziani in prospettiva comparatistica, Torino, 2022, *passim.* Ancora, F. Macioce, *La vulnerabilità di gruppo*, Torino, 2021, p. 66 s. «Così, ad esempio, gli anziani non sono collocabili in un gruppo vulnerabile con caratteristiche identitarie (come se l'anzianità fosse un dato determinante l'identità di una persona); ciò non significa che l'anzianità non possa anche divenire, seppur raramente, un fatto utilizzabile in politiche dell'identità, significa tuttavia che questo approccio non è essenziale al fine di determinare le caratteristiche e i meccanismi alla base della vulnerabilità di tale gruppo di persone. Questa, piuttosto, dipende dal posizionamento comune delle persone anziane […]»

[48] Cfr. punto 9.1.5., Parliamentary Assembly, Council of Europe, Committee on Culture, Science, Education and Media, *Technological Convergence, Artificial Intelligence and Human Rights*, Report 2017, https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23726&lang=en.

[49] C. Nardocci, *Artificial Intelligence-based Discrimination: Theoretical and Normative Responses. Perspectives from Europe*, in *DPCE online*, 3, 2023, p. 2371 ss.

dignità, alla non discriminazione e ai valori di uguaglianza e giustizia. A ciò si aggiunge il rischio che tali sistemi, possano alimentare pratiche di manipolazione[50], sfruttamento e controllo sociale[51].

In proposito, uno dei principali obiettivi dell'AI Act è quello di garantire un elevato livello di protezione dei diritti fondamentali, promuovendo un'IA *human-centred* e affidabile[52].

Le istituzioni europee sembrerebbero aver acquisito maggior consapevolezza delle insidie che si celano dietro i sistemi di decisione algoritmica e dei *bias* algoritmici, cercando di contrastarli attraverso misure in grado di comprendere le decisioni prese dall'algoritmo come il c.d. *human oversight*[53] o come il modello della *Explainable AI*[54],che permette agli individui di comprendere le decisioni o le previsioni dell'algoritmo. Ciò nonostante, la discriminazione algoritmica è, in termini fattuali, un fenomeno più complesso di quanto lascia supporre, generando problematiche che vanno oltre la singola decisione automatica che discrimina un individuo[55].

A ben vedere, i rischi indotti dai sistemi di *algorithmic decision-making*[56] includono anche altri scenari in cui le dinamiche di tipo discriminatorio, favorite

---

[50] T. Cohen, *Regulating Manipulative Artificial Intelligence*, in *SCRIPTed: A Journal of Law, Technology and Society*, 20, 1, 2023, p. 203 ss.

[51] A. Gentili, *La vulnerabilità sociale. Un modello teorico per il trattamento legale*, in *Rivista critica del diritto privato*, 2019, p. 41 ss.

[52] Considerando 1 AI Act. Cfr., inoltre, E. Battelli, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona*, in *Diritto di famiglia e delle persone*, 3, 2022, p. 1096 ss.

[53] S. Sterz, K. Baum, S. Biewer, H. Hermanns, A. Lauber-Rönsberg *et al.*, *On the Quest for Effectiveness in Human Oversight: Interdisciplinary Perspectives*, in *Information & Communications Technology Law*, 32, 2, 2023, p. 170 ss.; R. Koulu, *Proceduralizing Control and Discretion: Human Oversight in Artificial Intelligence Policy*, in *Maastricht Journal of European and Comparative Law*, 27,6, 2020, p. 720 ss.

[54] C. Panigutti, R. Hamon, I. Hupont, D. Fernandez Llorca, D. Fano Yela *et al.*, *The Role of Explainable AI in the Context of the AI Act*, in *FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, 2023, p. 1129 ss.; D. Gunning and D. Aha, *DARPA's Explainable Artificial Intelligence (XAI) Program*, in *AI magazine*, 40, 2, 2019, p. 44 ss.; B. Goodman and S. Flaxman, *European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"*, in *AI magazine*, 38, 3, 2017, p. 50 ss.; U. Peters, *Explainable AI Lacks Regulative Reasons: Why AI and Human Decision-Making are not Equally Opaque*, in *AI and Ethics*, 3, 2023, p. 963 ss.

[55] G. Caparezza Figlia, *Decisioni algoritmiche tra diritto alla spiegazione e divieto di discriminare*, in *Persona e Mercato*, 4, 2023, p. 639 ss.

[56] B. Lepri, N. Oliver, E. Letouzé, A. Pentland and P. Vinck, *Fair,*

dalle macchine, investono più soggetti spostandosi dal piano squisitamente individuale a quello collettivo e sociale (per esempio, gli algoritmi che selezionano i contenuti sui social media, svolgono un ruolo fondamentale nella diffusione di stereotipi e modelli culturali, creando discriminazioni a livello collettivo)[57].

La questione si è inasprita con l'introduzione dell'IA emotiva, capace di influenzare i comportamenti e le decisioni di persone vulnerabili, sfruttando i loro dati emotivi per manipolarne la volontà. Se non progettata e gestita correttamente, l'*Emotional AI* può avere effetti dannosi, mettendo a rischio la dignità e l'autonomia dell'individuo. Spesso può accadere che gli utenti più vulnerabili diventino dipendenti dalle tecnologie che li assistono, le quali potrebbero ridurre la loro capacità di interagire in modo critico con il sistema, aumentando il rischio di manipolazione e sfruttamento emotivo[58].

Si discute, pertanto, delle nuove forme di discriminazione oggi generate dall'ingresso di sistemi algoritmici di IA[59] all'interno di processi decisionali che incidono sugli interessi giuridicamente rilevanti degli individui. In ipotesi simili, è stata ravvisata la compressione di due garanzie fondamentali offerte dalla CEDU, consistenti, rispettivamente, nel riconoscimento del diritto alla vita privata e nel divieto di discriminazione[60].

L'IA emotiva raccoglie ed elabora dati personali particolarmente sensibili e ha il potenziale per manipolare e influenzare i processi decisionali di determinati gruppi di soggetti. Per tale motivo, se non progettata, gestita e supervisionata correttamente, la stessa può causare gravi danni e sottoporre gli utenti a rischi notevoli.

I profili principali della riflessione giuridica riguardano essenzialmente la violazione del trattamento dei dati personali particolari – specialmente quelli emotivi – le possibili discriminazioni algoritmiche, nonché le manipolazioni della volontà che l'impiego di tali tecnologie determina nei confronti dei gruppi di soggetti particolarmente vulnerabili[61].

Transparent, and Accountable Algorithmic Decision-Making Processes, in *Philosophy & Technology*, 31, 4, 2018, p. 611 ss.

[57] N. Lettieri, *La discriminazione nell'era delle macchine intelligenti. Modelli possibili di analisi, critica e tutela*, in *GenIUS*, 2022, p. 5 s.

[58] T. Balduzzi, *I sistemi biometrici vietati(1): riconoscimento delle emozioni e categorizzazione biometrica*, in A. Mantelero, G. Resta and G.M. Riccio (eds), *Intelligenza artificiale. Commentario*, Milano, 2025, in fase di plubblicazione.

[59] E. Falletti, *Discriminazione algoritmica. Una prospettiva comparata*, Torino, 2022, p. 250 ss.; G. Gaudio, *Le discriminazioni algoritmiche*, in *Lavoro Diritti Europa*, 1, 2024, p. 2 ss.

[60] V. artt. 8 e 14 CEDU.

[61] E. Calzolaio, *I Dispositivi medici «intelligenti»: spunti di comparazione giuridica*, cit., p. 80 ss.

Nonostante i potenziali benefici, questi sistemi presentano limiti significativi anche in termini di accuratezza e interpretazione culturale delle emozioni. Ciò viene meglio specificato nel considerando 44 dell'AI Act all'interno del quale il legislatore ha evidenziato le «serie preoccupazioni *che sussistono* in merito alla base scientifica dei sistemi di IA volti a identificare o inferire emozioni, perché l'espressione delle emozioni varia notevolmente in base alle culture, alle situazioni e persino in relazione a una stessa persona […]». In particolare, tra le principali carenze di tali sistemi figurano la limitata affidabilità e generalizzabilità, nonché la mancanza di specificità. 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 ed essere invasivi dei diritti e delle libertà delle persone interessate. Tali tecnologie potrebbero, dunque, determinare un trattamento pregiudizievole o sfavorevole di talune persone fisiche o di interi gruppi. È pertanto opportuno vietare l'immissione sul mercato 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. Divieto, questo, da non estendersi ai sistemi di IA immessi sul mercato esclusivamente per motivi medici o di sicurezza, come quelli destinati all'uso terapeutico.

Inoltre, la raccolta e l'analisi delle emozioni personali possono essere interpretate come una violazione della privacy e della sicurezza dei dati[62] dell'utente, sollevando preoccupazioni sui potenziali effetti negativi derivanti dalla manipolazione delle loro emozioni[63] (ad esempio, il naturale decadimento delle facoltà cognitive degli anziani, li rende più inclini a sviluppare una dipendenza dalla macchina, dal sistema che li assiste e si prende cura di loro).

In taluni casi, è stato osservato che gli utenti-pazienti, soprattutto quelli privi di assistenza[64], possono sviluppare un eccessivo affidamento alle *chatbot*[65], considerandole, alle volte, come sostituti dell'interazione umana.

---

[62] D.U. Galetta, *Human-stupidity-in-the-loop? Riflessioni (di un giurista) sulle potenzialità e i rischi dell'Intelligenza Artificiale*, cit., p. 4 ss.

[63] S. Santini, *IA emotiva e bias algoritmici. L'impatto nel settore sanitario*, cit., https://www.agendadigitale.eu/sanita/ia-emotiva-e-bias-algoritmici-limpatto-nel-settore-sanitario/.

[64] Cfr. M. Michilli, *Anziani e tecnologia, non grandi tasti ma più competenze: le azioni urgenti da attuare*, in *Agenda Digitale*, 2022, https://www.agendadigitale.eu/cultura-digitale/anziani-e-tecnologia-non-grandi-tasti-ma-piu-competenze-le-azioni-urgenti-da-attuare/.

[65] A. Rodríguez-Martínez, T. Amezcua-Aguilar, J. Cortés-Moreno and J.J. Jiménez-Delgado, *Qualitative Analysis of Conversational Chatbots to Alleviate Loneliness in Older Adults as a Strategy for Emotional Health*, in *Healthcare*, 12, 1, 62, 2024, p. 9 ss.

Ciò può comportare problemi di perdita di autonomia e difficoltà nella comprensione del funzionamento delle tecnologie e del trattamento dei propri dati[66].

Quanto alle preoccupazioni che l'impiego dell'IA emotiva solleva circa la possibilità di manipolare le emozioni dei vulnerabili, occorre porre l'accento sugli obblighi di informazione e di trasparenza per gli utenti esposti a tali tecnologie[67].

Trattasi di applicazioni che necessitano, sin dalla loro creazione, di determinati elementi: il rispetto dei principi di *privacy by design* e *privacy by default*[68]; la tutela del trattamento dei dati personali comuni e particolari; la coerenza dell'applicazione dei dati biometrici per il riconoscimento delle emozioni; l'adeguata trasparenza[69] da fornire all'utente; particolari controlli e un apposito meccanismo legato alla valutazione di impatto[70] preventiva che possa concretamente verificare l'intelligibilità del sistema di IA, oltre che ad una preventiva valutazione dell'impatto sui diritti fondamentali.

In effetti, ogni sistema di IA (robot assistivi, dispositivi domotici, *wearable devices*[71]), volto a interagire con soggetti vulnerabili, è chiamato a svolgere un compito alquanto delicato, prestando particolare attenzione alle capacità cognitive e agli aspetti psico-emotivi dei soggetti in questione.

In simili ipotesi, non può prescindersi dall'individuazione di misure volte a sviluppare strumenti di controllo preventivo e di *accountability* per il monitoraggio di tali tecnologie. Sul punto l'AI Act parrebbe dotarsi di norme specifiche volte a disciplinare un uso consapevole di questi dispositivi, prediligendo impostazioni meno invasive per la privacy. Trattasi di disposizioni che dovrebbe-

---

66 J. Stypinska, *AI Ageism: A Critical Roadmap for Studying Age Discrimination and Exclusion in Digitalized Societies*, in *AI & Society*, 38, 2023, p. 669 ss.

67 Cfr. P. Kulurkar, C.K. Dixit, V.C. Bharathi *et al.*, *AI Based Elderly Fall Prediction System Using Wearable Sensors: A Smart Home-Care Technology with IOT*, in *Sensors*, 25, 2023, p. 3 ss.

68 V. art. 10 AI Act che introduce un approccio che sembra riflettere in parte il principio di *privacy by design* e *by default* di cui all'art. 25 GDPR.

69 V. art. 13 AI Act.

70 In tema di DPIA si vedano D. Wright, *The State of the Art in Privacy Impact Assessment*, in *Computer Law & Security Review*, 28, 1, 2012, p. 54 ss.; D. Wright, M. Friedewald and R. Gellert, *Developing and Testing a Surveillance Impact Assessment Methodology*, in *International Data Privacy Law*, 5, 1, 2015, p. 40 ss.

71 Sui *wearable devices* si consultino, P. Stanzione, *"Dispositivi indossabili: rischi per la privacy. Che fine fanno le informazioni raccolte?" - Intervista a Pasquale Stanzione*, 2021, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9552323; L. Tirabeni, *I dispositivi indossabili per il benessere*, in *Il Mulino*, 3, 2022, p. 119 ss.

ro tutelare i soggetti vulnerabili, al fine di prevenirne abusi o discriminazioni[72]. Specifici gruppi di soggetti devono essere resi edotti riguardo al trattamento e all'elaborazione dei propri dati personali e, in particolare, sui controlli posti in essere per garantire il corretto funzionamento dei dispositivi.

In tale ottica, parrebbe dirimente la realizzazione di una comunicazione preventiva, chiara ed efficace[73] rivolta agli utenti, finalizzata alla comprensione del loro funzionamento e delle loro caratteristiche, che consenta, soprattutto ai più vulnerabili, di non aderire a condizioni pregiudizievoli. In effetti, gli obblighi di trasparenza e di notifica sono prescritti al fine di prevenire i rischi e rimuovere gli effetti negativi che determinati sistemi di IA potrebbero generare.

In sintesi, risulta cruciale accertarsi che le leggi applicabili in ogni fase del ciclo di vita di un sistema di IA siano in grado di garantire il trattamento conforme ed etico dei dati personali, perseguendo uno scopo ben definito, chiaro, legittimo e delineato all'inizio del progetto.

La via intrapresa, tuttavia, consente di rilevare che dall'analisi dell'AI Act[74] non si rinvengono nuovi strumenti che la persona, individualmente o collettivamente organizzata, possa utilizzare per rendere la tutela effettiva o più efficace.

Le numerose preoccupazioni suscitate dal trattamento dei dati personali, dai rischi derivanti dalla manipolazione delle emozioni e dalla discriminazione di specifici gruppi sociali, portano a chiedersi se, nella pratica, i sistemi di IA – soprattutto quelli di futura progettazione – possano essere disciplinati sulla base di una regolamentazione ancora considerata sufficientemente generica[75], rischiando di non stare al passo con gli sviluppi del settore.

---

[72] *European Council, Report CAHAI(2020)23 Ad hoc Committee on Artificial Intelligence* 2020, 2 ss., www.coe.int/cahai; *Parliamentary Assembly, Preventing discrimination caused by the use of artificial intelligence, Resolution 2343/2020*, https://pace.coe.int/en/files/28807/html.

[73] Art. 1, lett. d) AI Act.

[74] B. Calderini, *AI Act, il punto su risultati raggiunti e i dubbi sul futuro*, in *Agenda Digitale*, 2023, https://www.agendadigitale.eu/sicurezza/privacy/ai-act-raggiunto-un-equilibrio-instabile-ecco-perche/; G. Resta, *Cosa c'è di 'europeo' nella Proposta di Regolamento UE sull'intelligenza artificiale?*, in *Diritto dell'Informazione e dell'Informatica*, 2, 2022, p. 323 ss.

[75] L. Colonna, *Artificial Intelligence in the Internet of Health Things: Is the Solution to AI Privacy More AI?*, in *Boston University Journal of Science & Technology Law*, 27, 2, 2021, p. 329 ss.; T.R. Mosley, *AI Isn't Great at Decoding Human Emotions. So Why are Regulators Targeting the Tech?*, in *MIT Technology Review*, 2023, https://www.technologyreview.com/2023/08/14/1077788/ai-decoding-human-emotions-target-for-regulators/.

L'esito cui si giunge è che l'IA emotiva, essendo spesso costruita su basi discriminatorie e pseudo-scientifiche, rischia, ancora per molto tempo, di rimanere scientificamente discutibile e giuridicamente opaca[76].

3. *Basi giuridiche e specificità dei rimedi. Un nuovo paradigma?*

I processi di digitalizzazione della società algoritmica, assieme all'impiego dei sistemi di IA, hanno accentuato i dubbi sulla protezione delle persone vulnerabili, con notevoli difficoltà nella percezione dei rischi derivanti dallo sfruttamento o dalla manipolazione delle informazioni. A ciascun individuo, infatti, dovrebbe essere garantito il controllo delle propri dati e un adeguato esercizio dei diritti ad esse correlati. Per tale ragione, nel caso in cui ad un soggetto vulnerabile (e perciò incapace di esprimere un consenso consapevole) non venissero accordate tali garanzie, sarebbe necessario intervenire con misure protettive adeguate, al fine di salvaguardarne la dignità umana e prevenire l'uso improprio dei dati che potrebbe causare danni o discriminazioni[77].

In tal senso, si cerca di rafforzare la tutela dei soggetti più fragili salvaguardando l'affidabilità di tali tecnologie e subordinando la possibilità di utilizzo di dispositivi di IA emotiva alla predisposizione di un'apposita certificazione (rilasciata all'esito di un procedimento che verifichi anche idoneità, correttezza e rappresentatività dei *training data* sui quali l'IA è stata addestrata)[78]. Una simile soluzione andrebbe a rimuovere gli ostacoli volti ad impedire la più ampia diffusione dell'IA e dei sistemi di *autonomous decision-making* nei settori ritenuti ad "alto rischio".

In tale ottica, è fondamentale comprendere se le normative attuali possano offrire soluzioni adeguate o se sia necessaria una revisione della disciplina per garantire la protezione dei diritti fondamentali sul piano dello sviluppo tecnologico[79]. Occorre, inoltre, interrogarsi sul modo in cui il diritto può conformare i

---

[76] V. Marda and E. Jakubowska, *Emotion (Mis)Recognition: is the EU missing the point?*, cit., https://edri.org/our-work/emotion-misrecognition/.

[77] G. Malgieri and B. Kusters, *Pricing Privacy – The Right to Know the Value of Your Personal Data*, in *Computer Law & Security Review*, 2018, p. 294 ss.

[78] S. Trozzi, *Il principio della finalità del trattamento dei dati personali alla prova dei recenti sviluppi in tema di intelligenza artificiale: il caso ChatGPT e la neuroprivacy*, cit.

[79] A. Orlando, La regolamentazione delle tecnologie di riconoscimento facciale nell'UE e negli USA: alea IActa est?, cit., https://www.dpceonline.it/index.php/dpceonline/article/view/2186; E.C. Raffiotta, *Dalla self-regulation allaover-regulation in ambito digitale: come (e perché) di un necessario cambio di prospettiva*, in *Osservatorio delle fonti*, 2, 2023, p. 246 ss.; A. Bradford, *Digital empires: The global battle to regulate*

rimedi e le tutele dinanzi all'aumento esponenziale dei rischi derivanti dall'ambiente digitale.

Uno dei principali rimedi previsti dall'AI Act attiene alla centralità del principio di trasparenza, che impone un'informativa chiara e completa soprattutto per determinati gruppi di utenti. Tale principio è determinante per il corretto funzionamento dei sistemi di *Emotional AI*, come previsto dall'art. 50, co. 3, dell'AI Act, sugli obblighi di trasparenza per i fornitori e i *deployers* dei sistemi di riconoscimento delle emozioni[80]. In tema di trasparenza, occorre, inoltre, soffermare l'attenzione sull'obbligo di notifica che sopraggiunge nel momento in cui gli utenti interagiscono con sistemi di IA. In proposito, una notifica esplicita è obbligatoria in caso di impiego di tecnologie di IA per il rilevamento delle emozioni, trattandosi, appunto, di sistemi ad alto rischio. Nell'attuare tale obbligo, si dovrebbe inoltre prestare attenzione alle caratteristiche delle persone fisiche appartenenti a gruppi vulnerabili[81]. Ciò garantirebbe agli utenti piena consapevolezza di come le loro emozioni vengano rilevate e trattate, rispondendo alla necessità di trasparenza. A questo proposito, l'art. 13 stabilisce, in senso più ampio, che i sistemi di IA ad alto rischio devono essere progettati e sviluppati in modo da garantire un grado sufficiente di trasparenza, affinché i *deployers* possano interpretare l'*output* di un sistema e utilizzarlo correttamente. In particolare, dovranno fornirsi per tali sistemi istruzioni chiare, pertinenti, accessibili e comprensibili, agevolando agli utenti l'interpretazione dei risultati[82].

Un altro aspetto di particolare rilievo concerne l'abuso emotivo delle tecnologie di IA.

Sul punto, l'AI Act vieta due categorie di sistemi: da un lato, quelli che utilizzano metodi subliminali o tattiche manipolative per alterare il comportamento degli utenti, impedendo di operare scelte consapevoli e causando danni significativi[83]; dall'altro, quelli per il riconoscimento delle emozioni in contesti educativi e lavorativi, ad eccezione delle esigenze di assistenza sanitaria o di sicurezza[84].

Il tema della manipolazione emotiva[85] non concerne soltanto la questione di influenzare le scelte individuali, ma riguarda anche il modo in cui queste scelte vengono indotte attraverso il *targeting* delle emozioni, sfruttando la vulnerabilità

---

technology, Oxford, 2023, *passim*.

[80] Cfr. sul punto anche il considerando 69 AI Act.

[81] Cfr. considerando 132 e art. 52 AI Act.

[82] Cfr. il considerando 93 AI Act.

[83] Art. 5, co. 1, lett. a) AI Act.

[84] Cfr. art. 5, co. 1, lett. f) AI Act.

[85] M. Ienca, *On Artificial Intelligence and Manipulation*, in *Topoi*, 42, 2023, p. 833 ss.

di chi interagisce con tali sistemi (l'IA emotiva ha il potenziale di manipolare le emozioni rendendo gli individui più suscettibili a scelte pregiudizievoli, con implicazioni che vanno dalla perdita di autonomia alla manipolazione dei comportamenti sociali)[86].

La manipolazione emotiva, dunque, agisce più direttamente sull'individuo, sfruttando la sua vulnerabilità psicologica e sociale.

A questo punto, senza pretese di esaustività e rinviando ad altra sede una più puntuale trattazione, sul tema dell'IA emozionale e della discriminazione algoritmica è interessante il parallelismo con gli Stati Uniti[87], dove l'approccio normativo è più frammentato e *business friendly* rispetto all'Europa.

Invero, il differente *modus operandi* nella predisposizione di modelli regolatori da parte dell'Ue e degli USA, rileva soprattutto ai fini di una valutazione sull'ERT.

Nonostante i sistemi di IA basati sul riconoscimento emozionale siano già presenti sul mercato statunitense, attualmente non vi è una specifica regolamentazione di tali tecnologie.

Pertanto, sulla questione è stata rilevata la necessità di introdurre disposizioni mirate mettendo in luce i rischi connessi al rilevamento delle emozioni

---

[86] L. Kempe, *The Price of Emotion: Privacy, Manipulation, and Bias in Emotional A*I, in *Amercan Bar Association – Business Law Section*, 2024, https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-september/price-emotion-privacy-manipulation-bias-emotional-ai/#:~:text=Emotional%20AI%2C%20a%20subset%20of,investigations%2C%20and%20class%20action%20lawsuits.

[87] Cfr. A. Alù, *I differenti approcci regolatori in materia di intelligenza artificiale tra evoluzione tecnologica e risvolti applicativi*, in *Diritto di Famiglia e delle Persone (II)*, 3, 1, 2023, p. 1127 ss.; S. Aceto di Capriglia, *Intelligenza artificiale: una sfida globale tra rischi, prospettive e responsabilità. Le soluzioni assunte dai governi unionale, statunitense e sinico. Uno studio comparato*, in *federalismi.it*, 9, 2024, p. 24 ss.; P. Cihon, M.M. Maas and L. Kemp, *Should Artificial Intelligence Governance be Centralised? Six Design Lessons from History*, Atti della Conferenza AAAI/ACM su *AI, Ethics, and Society*, New York, 2020, p. 228 ss.; R. Wyden, press releases, *EU Restrictions on AI Emotion Detection Products*, 2023, https://www.wyden.senate.gov/news/press-releases/eu-restrictions-on-ai-emotion-detection-products; A. Mantelero, *AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment*, in *Computer Law & Security Review*, 34, 2018, p. 754 ss.; G. Capuzzo, *A Comparative Study on Algorithmic Discrimination between Europe and North-America*, in *Comparative Law Review*, 10, 2, 2019, p. 125 ss.; E. Stradella, *Le fonti nel diritto comparato: analisi di scenari extraeuropei (Stati Uniti e Cina)*, in *DPCE online*, 51, 1, 2022, p. 219 ss., https://www.dpceonline.it/index.php/dpceonline/article/view/1569/1551; B. Marchetti e L. Parona, *La regolazione dell'intelligenza artificiale: Stati Uniti e Unione europea alla ricerca di un possibile equilibrio*, in *DPCE online*, 1, 2022, p. 244, spec. nt. 26-27.

e ritenendo esemplare la scelta dell'Ue di agire contro l'uso improprio di tali tecnologie.

Tra le più rilevanti iniziative normative emerse a livello federale, merita particolare menzione il *Blueprint for an AI Bill of Rights*[88], introdotto dall'amministrazione Biden.

L'*AI Bill of Rights*, ha posto la necessità di regolamentare l'IA non solo per garantire la protezione della privacy degli utenti, attraverso l'adozione di forme di limitazione al trattamento dei dati personali, ma soprattutto per prevenire forme di discriminazione algoritmica[89].

Difatti, una delle sfide principali per i sistemi di IA mira ad impedire che gli stessi rafforzino i pregiudizi esistenti nei confronti di particolari gruppi di individui. Per contrastare tale fenomeno, si rende necessario sviluppare strategie incentrate sulla creazione di set di dati diversificati e inclusivi, al fine di individuare e mitigare i pregiudizi oltre a garantire la trasparenza e l'intelligibilità dell'IA.

A livello federale, nonostante non esista attualmente una specifica disciplina sull'IA emozionale, la *section* 5 del *Federal Trade Commission Act* (FTCA)[90] vieta atti o pratiche sleali o ingannevoli e prevede la possibilità di adottare apposite misure in caso di pregiudizi generati dall'IA. Un'ulteriore attività legislativa si è registrata, a livello statale, in Colorado, dove nel maggio 2024 è stata promulgata la prima legge statale in tema di *Consumer Protections for Artificial Intelligence. Concerning consumer protections in interactions with artificial intelligence systems*[91], che affronta la discriminazione nell'IA e si applica agli sviluppatori e agli utilizzatori di sistemi di IA ad alto rischio operanti in Colorado.

Tale legislazione sofferma l'attenzione sulla protezione dei consumatori più vulnerabili e sui rischi associati all'uso di sistemi di IA che potrebbero portare a discriminazioni algoritmiche, introducendo una serie di misure volte a garantire che i sistemi di IA ad alto rischio siano sviluppati, distribuiti e gestiti con un

---

[88] The White House, *Blueprint for an AI Bill of Rights - Making Automated Systems Work for the American People*, 2022, https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[89] M. Lopez, *Reevaluating Human Values for Patient Care in the Age of Artificial Intelligence: A Human-Centred Approach to Mobile Digital Health Technology Regulation in the United States*, in *AIRe*, 1, 2024, p. 58; E. Kiesow Cortez and N. Maslej, *Adjudication of Artificial Intelligence and Automated Decision-Making Cases in Europe and the USA*, in *European Journal of Risk Regulation*, 14, 2023, p. 460.

[90] Section 5(a) FTCA (15 USC §45) «prohibits unfair or deceptive acts or practices in or affecting commerce», chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.federalreserve.gov/boarddocs/supmanual/cch/200806/ftca.pdf.

[91] Cfr. SB24-205 *Consumer Protections for Artificial Intelligence - Concerning consumer protections in interactions with artificial intelligence systems*, 2024, https://leg.colorado.gov/bills/sb24-205.

elevato livello di responsabilità, trasparenza e rispetto per i diritti fondamentali dei consumatori-utenti.

In particolare, sono previsti specifici obblighi[92] sia per gli sviluppatori di sistemi di IA ad alto rischio – il cui compito è quello di garantire che i loro prodotti non causino discriminazioni, potendolo verificare attraverso una valutazione dell'impatto che il sistema avrà sui diritti fondamentali degli utenti – sia per i distributori di tali tecnologie. Tali soggetti, agendo con «*reasonable care*[93]», devono adottare misure preventive per proteggere i consumatori da qualsiasi rischio noto o prevedibile di discriminazione.

Ne discende che, sebbene il quadro giuridico europeo, a differenza di quello statunitense, offra una base per il trattamento dell'IA emozionale, vi è comunque la necessità di adottare determinate strategie che possano garantire una regolazione più incisiva e specifica, capace di adattarsi alle peculiarità di tali sistemi, con particolare attenzione alla protezione dei diritti fondamentali e alla tutela dei soggetti vulnerabili e che funga da modello per l'ordinamento statunitense.

3.1 *Il* Fundamental Rights Impact Assessment *(FRIA)*

In un'ottica di prevenzione delle violazioni dei diritti fondamentali degli individui derivanti dall'utilizzo dei sistemi di IA - e al fine di garantire un adeguato equilibrio tra progresso tecnologico e tutela giuridica - merita particolare attenzione il meccanismo introdotto dall'AI Act: il *Fundamental Rights Impact Assessment* (c.d. FRIA). Trattasi di uno strumento, impiegato dal *deployer*, finalizzato a individuare preventivamente i potenziali rischi per i diritti fondamentali, così da scongiurare abusi e impatti negativi connessi all'impiego dei sistemi di IA.

A riguardo, il considerando 96 del regolamento sottolinea che per garantire una tutela efficace dei diritti fondamentali, gli operatori di sistemi di IA ad alto rischio dovrebbero effettuare tale valutazione prima di mettere in uso i sistemi.

Invero, l'approccio basato sul rischio dell'AI Act stabilisce controlli procedurali da attuare a partire dalla fase di progettazione della tecnologia, prima dell'im-

---

[92] Sez. 6-1-1702 *Consumer Protections for Artificial Intelligence*; G. Olivato, *Colorado – SB 24/205, Act Concerning consumer protections in interactions with artificial intelligence systems: norme per lo sviluppo e per l'implementazione di sistemi di AI ad alto rischio*, in *BioDiritto*, 2024, https://www.biodiritto.org/AI-Legal-Atlas/AI-Normativa/Colorado-SB-24-205-Act-Concerning-consumer-protections-in-interactions-with-artificial-intelligence-systems-norme-per-lo-sviluppo-e-per-l-implementazione-di-sistemi-di-AI-ad-alto-rischio.

[93] V. sez. 6-1-1703,1 e sez. 6-1-1703, 1, *Consumer Protections for Artificial Intelligence*, *Colorado General Assembly*, https://leg.colorado.gov/bills/sb24-205.

missione sul mercato del dispositivo. Sebbene tale approccio sia ampiamente utilizzato nella regolamentazione industriale, principalmente in ambito di sicurezza e protezione, esso trova applicazione anche in relazione ai diritti fondamentali e a questioni sociali più ampie[94].

In particolare, l'art. 27, par. 1 dell'AI Act introduce l'obbligo di una valutazione di impatto (prognostica) sui diritti fondamentali per i sistemi di IA ad alto rischio, stabilendo che, prima dell'utilizzo di tali sistemi, i *deployer* – siano essi organismi di diritto pubblico o enti privati – devono effettuare una valutazione dell'impatto sui diritti fondamentali che l'uso di tali sistemi può produrre.

Tale valutazione concerne: una descrizione dei processi in cui il sistema di IA ad alto rischio sarà impiegato, in linea con lo scopo previsto; una descrizione del periodo e della frequenza di utilizzo; l'identificazione del contesto e delle categorie di persone fisiche o di gruppi coinvolti nell'utilizzo del sistema; i rischi specifici di danno per questi soggetti, in considerazione delle informazioni date dal fornitore del sistema; una descrizione dell'attuazione di misure di controllo umano; e, infine, le misure da adottare in caso di materializzazione dei rischi.

Il FRIA rappresenta un risultato importante raggiunto dal Parlamento europeo rispetto a una proposta della Commissione che, pur ponendo l'accento sull'uomo e sulla protezione dei diritti fondamentali, non aveva implementato adeguatamente un modello di regolazione basato sul rischio[95]. Peraltro, considerato quale strumento obbligatorio da adottare prima di impiegare un sistema di IA ad alto rischio, il FRIA segue una metodologia generale di gestione dei rischi, che include una procedura sull'identificazione, l'analisi e la prevenzione o la mitigazione dei medesimi.

Questa valutazione non può essere considerata soltanto come un controllo finale, ma deve influenzare la progettazione stessa del sistema di IA evitando pregiudizi[96].

A causa del legame intrinseco tra rischio potenziale e progettazione del sistema, si raccomanda che la valutazione venga effettuata fin dalle prime fasi di definizione della strategia dell'operatore per l'uso di un dato sistema di IA e che venga ripetuta ogni volta che si apportano modifiche significative alla distribuzione del sistema[97].

---

[94] A. Mantelero, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template*, cit., p. 2 ss.; A. Wernick, *Impact Assessment as a Legal Design Pattern—A "Timeless Way" of Managing Future Risk*, in *Digital Society,* 3, 2, 2024, p. 29 ss.

[95] A. Mantelero, *o.c.*, p. 2 ss.

[96] *Ibid.*, p. 4, spec. 8.

[97] Considerando 96 AI Act.

Sebbene il FRIA rappresenti uno strumento di valutazione utile per promuovere sia la responsabilità che la trasparenza, è ancora necessario sviluppare un approccio metodologico più solido per valutare l'impatto dell'IA sui diritti fondamentali[98], essendo ancora poco approfondite le indicazioni fornite dall'AI Act su come condurre la valutazione[99]. Ciò è imprescindibile per supportare gli operatori di IA nello sviluppo e nell'implementazione dei loro sistemi in modo affidabile e incentrato sulla tutela dell'individuo.

4. *Alcune osservazioni conclusive*

Abbiamo cercato di mettere in luce le problematiche generate dall'impiego dei sistemi di IA (soprattutto emotiva) che incidono su interessi giuridicamente rilevanti di particolari gruppi di individui, riflettendo sul modo in cui il diritto affronta e concettualizza il fenomeno, nonché sulle strategie regolative proposte per contrastarlo.

Con riguardo al primo dei due aspetti, è emersa l'urgenza di ripensare la discriminazione mediata dai sistemi di IA, riconoscendo la necessità di affrontare questo fenomeno in modo specifico, tenendo conto delle sue peculiarità tecnologiche[100]. Il secondo aspetto attiene, invece, alla scarsa efficacia dei rimedi giuridici tradizionali rispetto ai fenomeni generati dalla discriminazione algoritmica, al fine di esplorare approcci normativi innovativi[101].

La rapida evoluzione dell'IA solleva due problematiche significative per i soggetti vulnerabili: una legata alla discriminazione, l'altra alla privacy.

L'obiettivo è verificare se le legislazioni nazionali e sovranazionali siano in grado di elaborare una risposta comune per una circolazione responsabile dei dati personali e uno sviluppo dell'IA che rispetti pienamente i diritti fondamentali.

---

[98] C. Novelli, F. Casolari, A. Rotolo, M. Taddeo and L. Floridi, *Taking AI Risks Seriously: A New Assessment Model for the AI Act*, in *AI & Society*, 39, 2023, p. 2494.

[99] G. De Gregorio, M. Fasciglione, F. Paolucci and O. Pollicino, *Compliance through Assessing Fundamental Rights: Insights at the Intersections of the European AI Act and the Corporate Sustainability Due Diligence Directive*, in *MediaLaws*, 2024, https://www.medialaws.eu/compliance-through-assessing-fundamental-rights-insights-at-the-intersections-of-the-european-ai-act-and-the-corporate-sustainability-due-diligence-directive/#:~:text=on%20fundamental%20rights.-,The%20Fundamental%20Rights%20Impact%20Assessment,27%20para.

[100] N. Lettieri, *La discriminazione nell'era delle macchine intelligenti. Modelli possibili di analisi, critica e tutela*, cit., 2022, p. 15.

[101] J. Kleinberg, J. Ludwig, S. Mullainathan and C.R. Sunstein, *Algorithms as discrimination detectors*, in *Proceedings of the National Academy of Sciences*, 117, 48, 2020, p. 30096 ss.

Sebbene siano previsti specifici requisiti di trasparenza per limitare i rischi e prevenire gli effetti negativi di alcuni sistemi di IA, è emerso che l'attuale quadro normativo sulla protezione dei dati non è sufficiente a regolamentare le tecnologie emergenti, potendo non essere adeguato per la tutela di gruppi di persone particolarmente vulnerabili.

Per tale ragione, nonostante gli esiti positivi perseguiti, persiste la preoccupazione che i sistemi di IA — in particolare quelli futuri — possano essere disciplinati da norme ancora troppo generiche, non in grado di adattarsi rapidamente agli sviluppi tecnologici del settore.

Nonostante le attuali disposizioni in materia di IA propongano di offrire un'adeguata protezione alle persone più vulnerabili, vi è un bisogno urgente di potenziare il quadro normativo esistente, implementando gli strumenti regolatori tradizionali e riconoscendo maggiore attenzione alle esigenze dei gruppi vulnerabili. Ciò potrebbe, infatti, favorire un utilizzo più responsabile e inclusivo dell'IA, rafforzando al contempo la tutela del benessere e dei diritti fondamentali di tali soggetti.

Il problema centrale riguarda l'efficacia dei rimedi giuridici tradizionali, che faticano a rispondere in modo adeguato a fenomeni tanto rapidi e complessi, alimentati da infrastrutture tecnologiche poco trasparenti e inaccessibili.

In quest'ottica, una delle principali sfide riguarda la regolazione della trasparenza algoritmica. Nonostante le norme sulla privacy, la loro attuazione risulta spesso insufficiente – soprattutto per quanto riguarda i sistemi di IA emotiva, che trattano dati particolarmente sensibili[102] – e produttiva di una serie di pregiudizi.

Per contrastare tali rischi, sarebbe necessaria una vigilanza rigorosa nonché la predisposizione di misure di salvaguardia per proteggere la privacy degli utenti e prevenirne la manipolazione emotiva.

Tuttavia, sul piano normativo e istituzionale, in particolare, si evidenzia la carenza di strumenti adeguati, necessari per tutelare al meglio gli individui particolarmente vulnerabili nelle ipotesi di opacità delle macchine algoritmiche.

Una possibile soluzione, potrebbe consistere nell'assicurare un duplice livello di protezione per i soggetti vulnerabili[103]: da un lato, attraverso l'inquadramento di più mirate normative che prevedano misure di tutela adeguate; dall'altro, mediante una protezione (preventiva) che si fondi non più (e soltanto) sulla valutazione di impatto sulla protezione dei dati (DPIA) e sulla costruzione di mi-

---

[102] A. Lombardi, *Disciplina della tutela dei dati personali e regolazione dell'intelligenza artificiale: rapporti, analogie e differenze tra GDPR e AI Act*, in *EJPLT*, 2, 2023, p. 251 s.

[103] V., ancora, V.V. Cuocci, *La protezione dei dati personali dei soggetti vulnerabili nella dimensione digitale – Uno studio di diritto comparato*, cit., p. 205 s.

sure di *privacy by design*, ma soprattutto su una valutazione di impatto sui diritti fondamentali di questo specifico gruppo di individui.

In quest'ottica, appaiono auspicabili misure di salvaguardia volte a tutelare la privacy, prevenire la manipolazione e lo sfruttamento emotivi e affrontare i pregiudizi che possono emergere dall'impiego degli algoritmi di rilevamento delle emozioni.

Lo scopo finale è quello di garantire un utilizzo controllato e contingentato di sistemi di *Emotional AI*, preservando i diritti fondamentali degli individui più fragili[104] e prevedendo, nel contempo, idonee procedure di valutazione e controllo da adattare alle attuali esigenze, al fine di assicurare il rispetto degli standard di qualità e sicurezza e mitigare il rischio di esporre gli utenti a conseguenze estremamente dannose[105].

[104] L. Ruggeri, *Ambiente e tecnologie: nuove sfide per la tutela della persona*, in *AmbienteDiritto.it*, 3, 2023, p. 2 ss.; G. Sartor, *Human Rights and Information Technologies*, in R. Brownsword, E. Scotford and K. Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology*, Oxford, 2017, p. 424 ss.

[105] E. Calzolaio, *I Dispositivi medici «intelligenti»: spunti di comparazione giuridica*, cit., p. 75 ss.

Tutela del diritto all'istruzione dei migranti nell'era degli algoritmi: strumenti e limiti

di **Salvatore Amato**

1. *Il diritto all'istruzione dei soggetti migranti maggiorenni: meritevole di tutela o pretesa priva di rilievo?*

Nonostante l'art. 34 cost.[1], da un lato, affermi espressamente «la scuola è aperta a tutti», indicando, per l'appunto, il principio base in tema di istruzione che dovrà orientare l'intera interpretazione della disciplina di settore[2] e, dall'altro lato, ai sensi del comma 3, delinei un criterio «soggettivo»[3] per l'accesso ai più

---

[1] Per un'analisi circa la natura del principio di cui all'art. 34 cost. si veda U. Pototschnig, *Istruzione (diritto alla)* [XXIII, 1973], in «Enciclopedia del diritto»; F. Angelini, *La scuola nella Costituzione: bilancio e letture prospettiche*, in «Diritto Costituzionale», n. 3, 2021, pp. 11-46; E. Rossi, P. Addis, F. Biondi Dal Monte, *La libertà di insegnamento e il diritto all'istruzione nella Costituzione italiana*, in «AIC», n. 1, 2016. Si veda altresì F. Fracchia, *"Costituzione scolastica": bilancio e letture prospettiche*, in «Diritto Costituzionale», n. 3, 2021, laddove qualifica l'art. 34 non solo come diritto ma altresì come un dovere all'istruzione.

[2] M. Benvenuti, *L'istruzione come diritto sociale*, in F. Angelini, M. Benvenuti (a cura di), *Le dimensioni costituzionali dell'istruzione*, *Atti del Convegno di Roma, 23.24 gennaio 2014*, Jovene Editore, Napoli 2014; M. Benvenuti, *"La scuola è aperta a tutti"? Potenzialità e limiti del diritto all'istruzione tra ordinamento statale e ordinamento sovranazionale*, in «federalismi.it», 4 settembre 2018, pp. 99-126. Si veda, altresì, F. Biondi Dal Monte, S. Frega, *Per l'uguaglianza sostanziale tra i banchi di scuola*, Franco Angeli, Milano 2023; A. De Fusco, *Sul diritto all'istruzione come veicolo di integrazione delle seconde generazioni dell'immigrazione in Italia*, in «AIC», febbraio 2018.

[3] M. Benvenuti, *L'istruzione come diritto*, cit., p. 180. Per un'analisi fornita

elevati gradi dell'istruzione, per cui «i capaci e meritevoli, anche se privi di mezzi, hanno diritto di raggiungere i gradi più alti degli studi», l'art. 38 del D.lgs. 25 luglio 1998, n. 286 (T.U.I.) in tema di immigrazione comporta una limitazione, laddove considera meritevole di tutela assoluta esclusivamente la figura del minore straniero presente sul territorio italiano, dedicando al comma 5 solo una breve specificazione in favore della figura dello straniero (migrante) adulto, per cui «le istituzioni scolastiche, nel quadro di una programmazione territoriale degli interventi, anche sulla base di convenzioni con le Regioni e gli enti locali, promuovono: a) l'accoglienza degli stranieri adulti regolarmente soggiornanti mediante l'attivazione di corsi di alfabetizzazione nelle scuole elementari e medie; b) la realizzazione di un'offerta culturale valida per gli stranieri adulti regolarmente soggiornanti che intendano conseguire il titolo di studio della scuola dell'obbligo».

Al comma 6, inoltre, la disposizione in discorso aggiunge che «le regioni, anche attraverso altri enti locali, promuovono programmi culturali per i diversi gruppi nazionali, anche mediante corsi effettuati presso le scuole superiori o istituti universitari», introducendo dunque solo in via d'eccezione il diritto all'istruzione del soggetto migrante maggiorenne e tacendo tuttavia in ordine allo specifico diritto del migrante di accedere ad una istruzione universitaria.

In altre parole, nonostante la qualificazione in termini di diritto fondamentale del diritto all'istruzione[4], da intendere come un diritto da generalizzare a tutti gli

---

dalla Corte costituzionale in tema di diritti sociali dei soggetti migranti si segnalano tra le più rilevanti le pronunce n. 120/1967, 104/1969, 54/1979, 62/1994, 198/2000 e 252/2001. In tema di diritti fondamentali dei soggetti migranti si veda altresì M. Immordino, *La salute degli immigrati irregolari tra "certezza" del diritto e "incertezza" della sua effettività*, in «Nuove Autonomie», n. 2-3, 2013, pp. 202-203, laddove focalizza l'attenzione non sulle disposizioni formali contenute in Costituzione bensì sulle parole contenute all'interno delle disposizioni «*come "uomo", "dignità umana", "libertà", "solidarietà", "uguaglianza", "inclusione", "non discriminazione", "universalità dei diritti", "inviolabilità";* concetti e valori caratterizzanti la «persona» in quanto tale, prescindendo dalla cittadinanza; P. Morozzo Della Rocca, *Diritto alle cure mediche e prestazioni di assistenza sociale connesse alla salute dello straniero irregolarmente soggiornante*, in «Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)», n. 2, 2015; A. Zito, *Beni primari, diritti sociali degli immigrati e ruolo delle pubbliche amministrazioni*, in «Nuove Autonomie», n. 2-3, 2013; A. RUGGERI, *Cittadini, immigrati e migranti al bivio tra distinzione e integrazione delle culture (note minime su una spinosa e ad oggi irrisolta questione)*, in «Dirittifondamentali.it», n. 3, 2021, pp. 393-412; V. Caracciolo La Grotteria, *Immigrati e istruzione*, in «Amministrazione e Contabilità dello Stato. Degli enti pubblici», www.contabilita-pubblica.it, 04 luglio 2022, pp. 1-11

[4] L'art. 34 cost. non è il solo a evidenziare la portata e la meritevolezza di tutela del diritto all'istruzione. In primo luogo, la Dichiarazione Universale dei diritti dell'uomo del 10.12.1948, all'art. 26, prevede il diritto di ogni persona di accedere all'istruzione,

individui, in quanto diritto ancorato direttamente all'esplicazione della persona umana, il T.U.I. – se in un primo momento, attraverso, da un lato, la disposizione di cui all'art. 2 comma 1, affermi che agli stranieri, *latu sensu* intesi, sono riconosciuti i diritti fondamentali della persona umana, in conformità con la normativa di diritto interno, le convenzioni internazionali in vigore e i principi di diritto internazionale generalmente riconosciuti e, dall'altro lato, mediante il comma 5 della stessa norma, sancisca la parità di trattamento dello straniero *latu sensu* inteso con il cittadino, nell'accesso ai pubblici servizi nei limiti e nei modi previsti dalla legge – differenzia, all'interno della categoria dei non cittadini, i soggetti minori dai maggiorenni[5]. Difatti, come già detto, tutte le disposizioni

---

laddove afferma che «1) Ogni individuo ha diritto all›istruzione. L›istruzione deve essere gratuita almeno per quanto riguarda le classi elementari e fondamentali. L›istruzione elementare deve essere obbligatoria. L›istruzione tecnica e professionale deve essere messa alla portata di tutti e l›istruzione superiore deve essere egualmente accessibile a tutti sulla base del merito. 2) L›istruzione deve essere indirizzata al pieno sviluppo della personalità umana ed al rafforzamento del rispetto dei diritti umani e delle libertà fondamentali. Essa deve promuovere la comprensione, la tolleranza, l›amicizia fra tutte le Nazioni, i gruppi razziali e religiosi, e deve favorire l›opera delle Nazioni Unite per il mantenimento della pace». Sul punto S. Marchisio, *Diritto all'istruzione e integrazione dei rifugiati*, in «Ordine internazionale e diritti umani», n. 3, 2018. Inoltre, anche il Patto internazionale relativo ai diritti economici, sociali e culturali adottato a New York in data 16.12.1966, all'art. 13, riconosce «a ogni persona» il diritto di accedere e ottenere una istruzione al fine di sviluppare a pieno la personalità umana, la dignità della medesima e rafforzare il rispetto dei diritti dell'uomo e delle libertà fondamentali aggiungendo, al comma 2 lett. c), che «l'istruzione superiore deve essere resa accessibile a tutti su un piano d'uguaglianza, in base alle attitudini di ciascuno, con ogni mezzo a ciò idoneo»; la CEDU, all'art. 2 Prot. 1, afferma, inoltre, che il diritto all'istruzione non può in nessun caso essere negato e, da ultimo, l'art. 14 della Carta dei diritti fondamentali dell'UE, rammenta che «ogni individuo ha diritto all'istruzione e all'accesso alla formazione professionale e continua». Il diritto ad ottenere l'istruzione, a valle degli obiettivi cui tendono le «Carte» dei principi fondamentali, appare preordinato alla tutela del diritto, da riconoscersi ad «ogni individuo», di partecipare liberamente alla vita culturale degli Stati (art. 27 della Dichiarazione e art. 15, comma 1, lett. a) del Patto), così come anche evidenziato dall'art. 9 cost., nella parte in cui tutela e garantisce lo sviluppo della cultura, qualificando tale bene come irrinunciabile dall'ordinamento, in quanto avente valore primario e assoluto.

[5] Emblematico sul punto l'art. 45, d.p.r. 31 agosto 1999, n. 394, recante «norme di attuazione del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero», che parifica esclusivamente il minore straniero al cittadino italiano, prevedendo che «i minori stranieri presenti sul territorio nazionale hanno diritto all'istruzione indipendentemente dalla regolarità della posizione in ordine al loro soggiorno, nelle forme e nei modi previsti per i cittadini italiani. Essi sono soggetti all'obbligo scolastico secondo le disposizioni vigenti in materia. L'iscrizione dei minori

inerenti il diritto all'istruzione dei non cittadini concentrano l'attenzione sulla figura del minore straniero, abbozzando[6] una disciplina «residuale» per lo straniero maggiorenne esclusivamente all'interno del comma 5 dell'art. 38 T.U.I., a mente del quale l'istruzione per gli stranieri maggiorenni risulta riservata esclusivamente ai non cittadini regolarmente soggiornanti, così come l'istruzione universitaria, il cui accesso, ai sensi dell'art. 39 T.U.I. è subordinato all'ottenimento di regolare permesso di soggiorno. In particolare, ai sensi dell'art. 5, comma 1, T.U.I., hanno diritto di soggiornare in Italia gli stranieri entrati regolarmente all'interno del territorio e, pertanto, il percorso universitario del non cittadino maggiorenne viene subordinato dai limiti e dai modi stabiliti per gli stranieri regolarmente soggiornanti.

Ciò, tuttavia e alla luce delle criticità legate alla disciplina in ordine al rilascio dei permessi di soggiorno, appare in contrasto con la definizione di principio fondamentale del diritto all'istruzione. Inoltre, il permesso di soggiorno (per motivi di studio) non appare in grado, di per sé, di soddisfare le esigenze collegate al diritto allo studio dei non cittadini.

È, dunque, possibile affermare che nel sistema delineato è presente una vistosa lacuna, laddove il diritto all'istruzione, qualificato quale diritto fondamentale della persona, non trova adeguata tutela in ordine alla figura del non cittadino maggiorenne[7], a cui la soddisfazione di tale diritto fondamentale viene subordinata all'ottenimento di un titolo amministrativo abilitante, a dire il vero, di difficile ottenimento. È pur vero che il riconoscimento del diritto all'istruzione non può giungere a divenire il varco per l'accesso incondizionato e illimitato all'ordinamento nazionale, necessitando, il sistema di accesso, di un meccanismo votato ai principi di ragionevolezza e di bilanciamento di interessi già sottolineati dalla Corte Cost.[8], nonché

---

stranieri nelle scuote italiane di ogni ordine e grado avviene nei modi e alle condizioni previsti per i minori italiani».

[6] Si veda A. De Fusco, *Sul diritto all'istruzione come*, Op cit., p. 9 ss.

[7] P. Bonetti, *L'insostenibilità costituzionale delle recenti norme sugli stranieri. I limiti all'ingresso e al soggiorno che violano i diritti fondamentali e il sistema delle fonti del diritto non assicurano sicurezza, né alcuna disciplina efficace dell'immigrazione*, in «Diritto Pubblico», n. 3, 2019, pp. 651-673; C. Di Maio, *Intercultura e diritto all'istruzione. Obiettivi e criticità dei processi di integrazione degli stranieri nelle scuole italiane*, in S. Gambino (a cura di), *Diritti sociali e crisi economica. Problemi e prospettive*, Giappichelli, Torino, 2015

[8] Corte Cost. sentenza 27 febbraio 2015, n. 22. Per un'analisi della pronuncia, M. Pipponzi, *Stranieri e prestazioni assistenziali: il punto della situazione dopo le pronunce della Corte costituzionale sull'art. 80, co.19, l. n. 388 del 2000*, in «Diritto immigrazione e cittadinanza», n. 1, 2015. In tema O. Spataro, *I diritti degli immigrati nella giurisprudenza della Corte Costituzionale*, in «Nuove Autonomie», n. 2-3, 2013.

dalla giurisprudenza della Corte di Strasburgo[9] in tema di uguaglianza sostanziale[10]. Difatti, non si intende censurare la già sostenuta esistenza di una stretta correlazione tra ingresso e soggiorno[11], sebbene non possa non affermarsi come tale correlazione sembrerebbe comprimere eccessivamente l'accesso all'istruzione dei soggetti migranti maggiorenni, soprattutto alla luce delle criticità discendenti dall'utilizzo delle nuove tecnologie di cui si dirà più avanti.

2. *Ulteriori limiti discendenti dal diritto UE: la Direttiva UE/2016/801*

Nonostante l'UE abbia già realizzato talune spinte verso un efficientamento del diritto allo studio[12] inteso quale strumento di integrazione dei cittadini migranti di Stati terzi nella società europea[13] (di talché si inizia a parlare di status

[9] Corte Edu sentenza 10 settembre 2020, G.L. c. Italia (n. 59751/2015). Sul punto, M. Ikonomu, *Diritto all'istruzione e principio di non discriminazione, la Corte di Strasburgo condanna l'Italia*, in «Questione Giustizia», questionegiustizia.it, 15 settembre 2020.

[10] La Corte afferma che l'art. 14 Cedu non vieta allo Stato membro di trattare i gruppi in modo diverso al fine di correggere «disuguaglianze di fatto», essendo, in alcune circostanze, necessario il trattamento differente per tutelare i diritti fondamentali. In tema si veda M. Nino, *Corte europea dei diritti umani, divieto di discriminazione e diritto all'istruzione della minoranza rom*, in «Diritti umani e diritto internazionale», n. 2, 2013; A. Lauro, *Un "devoir de justice": le sfide dell'uguaglianza nel diritto all'istruzione, scolastica*, in «Costituzionalismo.it», n. 1/2023; A. Albanese, *Non discriminazione, uguaglianza e ragionevolezza nella garanzia dei diritti sociali degli immigrati. L'approccio della Corte Edu e della Corte Costituzionale*, in F. Astone, R. Cavallo Perin, A. Romeo, M. Savino, *Immigrazione e Diritti Fondamentali*, Unito, Torino, 2019. In tema anche F. Fracchia, *Integrazione, eguaglianza, solidarietà*, in «Nuove Autonomie», n. 2-3/2013 ove si incentra l'attenzione sul fenomeno della «globalizzazione dei diritti» e, in particolare, del fenomeno dell'allargamento dell'area dei diritti fondamentali. Si veda altresì G. Moschella, *La legislazione sull'immigrazione e le prospettive della tutela dei diritti fondamentali: l'ordinamento europeo e l'esperienza italiana,* in «Ordine Internazionale e diritti umani», n. 3, 2019.

[11] P. Morozzo Della Rocca (a cura di), *Immigrazione, asilo e cittadinanza*, Maggioli Editore, Rimini, 2018, pp. 15 ss.

[12] Sul punto F. Esteve Garcia, *El régimen europeo de estudiantes e investigadores extracomunitarios en España*, in A. Solanes Corella, E. La Spina (coor.), *Políticas migratorias, asilo y derechos humanos. Un cruce de perspectivas entrela Unión Europea y España*, n. 04, 2014, pp. 121-148.

[13] A. Pitrone, *La recente disciplina europea sulla migrazione qualificata: tra promozione della migrazione circolare e politiche di integrazione*, in «Freedom Security

privilegiato dello studente – anche - non cittadino[14]), le misure poste in essere non risultano ancora del tutto adeguate alla soddisfazione del diritto fondamentale.

Spunti critici discendono, in particolare, dalla Direttiva 2016/801/UE[15], la cui interpretazione estensiva da parte della giurisprudenza ha incontrato i favori della dottrina[16] e per cui gli unici vincoli che lo Stato membro può frapporre a studenti non cittadini che intendono accedere all'interno dello spazio UE per motivi di studio vengono tassativamente enunciati negli artt. 6 e 7 della stessa Direttiva, non potendosi in alcun caso enucleare condizioni aggiuntive[17].

Benché esista una impossibilità per gli Stati membri di coniare ulteriori condizioni di ingresso e di rilascio dell'«autorizzazione», di per sé gli artt. 6 e 7 contengono delle aporie, laddove, da un lato, l'art. 6 afferma che lo Stato membro non può limitare l'ingresso a studenti non cittadini per motivi di studio, salvo che lo stesso ritenga che i non cittadini non «hanno o [non] avranno un rapporto di lavoro» mentre, dall'altro lato, l'art. 7, par. 1, lett. a), delinea la necessità per il cittadino studente di paese terzo di «presentare un titolo di viaggio valido come definito a norma del diritto nazionale e, se necessario, una domanda di visto o un visto valido oppure, se del caso, un permesso di soggiorno valido o un visto valido per soggiorno di lunga durata».

Inoltre, ulteriori requisiti vengono richiesti dal par. 1, lett. e) dell'art. 7, il quale richiede all'interessato l'esibizione di «prove richieste dallo Stato membro interessato per dimostrare che il cittadino di paese terzo disporrà, durante il soggiorno programmato, di risorse sufficienti per provvedere al suo sostentamento senza ricorrere al sistema di previdenza sociale dello Stato membro, e al suo ritorno»

Justice: European Legal Studies», n. 1, 2018, p. 91.

S. Sani, *Il sistema scolastico italiano e le politiche di integrazione promosse dall'Unione Europea*, in «History of Education & Children's Literature», XVII, n. 2, 2022.

[14] A. Pitrone, *La circolazione degli "studenti" nell'Unione Europea: cittadini privilegiati?,* in A. Di Stasi, M.C. Baruffi, L. Panella (a cura di), *Cittadinanza europea e cittadinanza nazionale*, Editoriale Scientifica, Napoli, 2023.

[15] Relativa alle condizioni di ingresso e soggiorno dei cittadini di paesi terzi per motivi di ricerca, studio, tirocinio, volontariato, programmi di scambio di alunni o progetti educativi, e collocamento alla pari (attuata con D.Lgs. 11 maggio 2018 n. 71). Per un'analisi H. Calers, *The Student and Researchers Directive: Analysis and Implementation Challenges*, in T. De Lange, P. Minderhoud (eds.), *The Students & Researchers Directive: Central Themes, Problem Issues and Implementation in Selected Member States*, Wolf Productions, Nijmegen, 2020.

[16] S. Amadeo, F. Spitaleri, *Il diritto dell'immigrazione e dell'asilo dell'Unione Europea*, Giappichelli, Torino, 2019, p. 191.

[17] *Ibidem.*

(così come, del resto, richiesto dall'art. 14, par. 1, lett. c) del Cod. dei Visti), mentre il par. 7 della medesima disposizione conclude aggiungendo che «non sono ammessi i cittadini di paesi terzi che si considera presentino una minaccia per l'ordine pubblico, la sicurezza pubblica o la sanità pubblica».

A ben vedere, tali limiti possono considerarsi di portata elastica in quanto privi di effettive condizioni stringenti per lo Stato membro, il quale risulta privo di reali vincoli e di conseguenza, continua a vantare una discrezionalità assoluta[18] in tema di ingresso e soggiorno. Dunque, al fine di evitare «l'eclissi dei diritti»[19] dei migranti, occorre delineare uno strumento che possa garantire il diritto all'istruzione (qualificato alla stregua di diritto fondamentale) anche a coloro i quali risultano privi di autorizzazione amministrativa relativamente ad ingresso e soggiorno e, soprattutto, al fine di rimediare alla criticità legata alla discrezionalità priva di limiti dello Stato.

Emblematica la Raccomandazione (UE) 2020/1364[20], la quale, con riferimento all'istruzione universitaria, afferma che «gli Stati membri dovrebbero valutare la possibilità di migliorare l'accesso alle università per i giovani che necessitano di protezione internazionale, consentendo loro di qualificarsi come studenti, tenendo conto delle loro esigenze specifiche»[21].

Pertanto, nonostante il diritto allo studio venga qualificato come diritto fondamentale della persona umana e quindi da garantire a «chiunque», anche la disciplina UE abbozza[22] una normativa in ordine agli studenti non cittadini UE interessati ad accedere al sistema di formazione europeo; normativa che, tuttavia, sembra mal conciliarsi con la categoria dei soggetti migranti. I vincoli indicati e le prerogative statali delineate dalla Direttiva UE/2016/801 sembrano ridurre eccessivamente le possibilità di accesso dei non cittadini e, anzi, sbarrare l'accesso degli studenti migranti richiedenti protezione. In particolare, la disposizione secondo cui la direttiva non incide sul diritto di uno Stato membro di determinare il volume di ingresso dei cittadini di paesi terzi «ad eccezione degli studenti, qualora lo Stato membro interessato ritenga che tali cittadini hanno o avranno

---

[18] E. Minniti, *"Sicurezza Pubblica": la discrezionalità degli Stati nazionali in merito all'ingresso dei non cittadini per motivi di studio*, in «DPCE on line», n. 3, 2017, p. 728.

[19] R. Niro, *Spunti sul diritto speciale dei migranti e l'eclissi dei diritti*, in «Giurisprudenza Costituzionale», n. 1, 2021.

[20] Si veda il Considerando 2, per cui «la presente raccomandazione mira a sostenere gli sforzi costantemente profusi dagli Stati membri per aprire e rafforzare canali legali e sicuri».

[21] Raccomandazione (UE) 2020/1364, considerando 20.

[22] A. De Fusco, *Sul diritto all'istruzione come*, cit., p. 9.

un rapporto di lavoro» (art. 6), nonché le «condizioni generali» di cui all'art. 7, sembrano limitare eccessivamente i soggetti migranti richiedenti protezione dalla possibilità di giungere alla soddisfazione del diritto fondamentale.

Dunque, il permesso di soggiorno per motivi di studio se, da un lato, appare uno strumento astrattamente in grado di assicurare il diritto allo studio, dall'altro lato, tuttavia, appare allo stesso modo caratterizzato da una procedura farraginosa e comunque in mano agli Stati membri che, per le ragioni sopra espresse, riservano una discrezionalità pressocché assoluta e priva di reali limiti in ordine alla decisione circa l'ingresso e il soggiorno di non cittadini per motivi di studio. Tale discrezionalità, unitamente alla previsione specifica (anch'essa priva di reale circoscrizione) di cui al par. 6 dell'art. 7 della Direttiva UE/2016/801 e soprattutto all'idea, nonostante tutto, attuale che il migrante costituisca, in sé, un problema di sicurezza pubblica[23], porta a riflettere sui meccanismi ad oggi presenti nell'ordinamento, in grado di tutelare i diritti degli stessi soggetti e, soprattutto, ai possibili strumenti di futura tutela.

3. *L'impatto dell'intelligenza artificiale sul diritto all'istruzione dei soggetti migranti*

Occorre ora comprendere come, in un contesto particolarmente limitante come quello sopra delineato, l'impatto delle nuove tecnologie e di intelligenza artificiale possa modificare la condizione certamente precaria dei soggetti migranti.

I meccanismi di intelligenza artificiale[24] possono essere qualificati come strumenti informatici che sono solo apparentemente neutrali[25], in quanto in grado

[23] *Ivi*, p. 104. Si veda, altresì, A. Caputo, *Irregolari, pericolosi, criminali. Il diritto delle migrazioni tra politiche sicuritarie e populismo penale*, in M. Giovannetti, N. Zorzella (a cura di), *Ius migrandi*, Franco Angeli, Milano, 2020, pp. 165 ss.

[24] Per un inquadramento del tema L. Portinale, *Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori*, in «MediaLaws, Rivista di diritto dei media», n. 3, 2021, pp. 13-28; T.E. Frosini, *L'orizzonte giuridico dell'Intelligenza Artificiale*, in «BioLaw Journal – Rivista di Biodiritto», n. 1, 2022, pp. 155-164; D. Vese, *Algorithms, competition law, public interest*, in «PA, Persona e Amministrazione», V. 13, n. 2, 2023, pp. 1239-1266.

[25] F. J. Garrido Carrillo, *Digitalizacion e inteligencia artificial en el control de los flujos migratorios. Oportunidades y riesgos desde el respeto a los derechos fundamentales*, in M.I. Romeo Pradas, Y. Lucchi Lopez-Tapia, *Ultimos avances en el camino hacia un derecho procesal civil de la Union Europea,* Tirant Lo Blanch, Valencia, 2024, pp. 231-283. L'autore afferma che proprio l'utilizzo rigido e non capace di considerare la condizione specifica del singolo migrante, potrebbe portare alla lesione dei diritti del soggetto. Si veda anche F.J. Garrido Carrillo, *La inteligencia artificial en el control de*

di delineare processi classificatori e identificativi degli individui, realizzati in via autonoma da algoritmi[26]. In particolare, gli algoritmi utilizzati nell'analisi predittiva valutano la probabilità o il rischio che un evento futuro possa realizzarsi, mediante un calcolo algoritmico che avviene su base statistica e che solo in astratto è possibile affermare sia neutrale o oggettivo, in quanto il meccanismo di funzionamento deriva da un insieme di istruzioni predefinite da un programmatore[27]. Si scorge immediatamente la prima criticità, legata alla difficoltà di predeterminare - da un punto di vista sia qualitativo che quantitativo - aspetti inerenti esseri umani e poiché anche gli algoritmi possono essere determinati da schemi che nascondono pregiudizi (per l'oggetto dell'analisi, possiamo citare «razza», «colore della pelle», «provenienza», ecc..), di conseguenza occorre vigilare criticamente sul loro utilizzo al fine di evitare «oppressioni»[28] soprattutto nei confronti di soggetti vulnerabili. Tali pregiudizi (*bias*) possono giungere, nell'ipotesi che oggi ci occupa, ad escludere totalmente i soggetti migranti dalla possibilità di accedere alla tutela del diritto all'istruzione. In altre parole, delegare alla macchina le valutazioni in ordine ai criteri di cui all'art. 6 e 7 della Direttiva UE/2016/801, già in grado di determinare per lo Stato membro una discrezionalità priva di reali limiti, continua a determinare delle perplessità, soprattutto in ragione di quello che è stato definito «razzismo algoritmico»[29] nei processi automatizzati classificatori, rinvenibile allorquando, a monte del processo algoritmico, le nuove tecnologie vengono caratterizzate da talune inclinazioni o, *rectius*, pre-concetti (*bias*) determinati dalla provenienza, dalla razza o dal colore della pelle del soggetto destinatario della decisione algoritmica[30]. Pertanto, nonostante l'utilizzo

---

los flujos migratorios en la Union Europea. La necesidad de un marco normativo garantista de los derechos fundamentales, in «Revista General de Derecho Europeo», n. 60, 2023.

[26] F. Ciracì, *Algo(r)etica e immigrazione*, in F. Ciracì, V. Alighieri, V. Alja De Franchis, F. Rinelli, S. Saraceno (a cura di), *Migrazioni. Giornate di studio sul razzismo. Atti della 5° edizione*, Unisalento, Lecce, 2024, pp. 35-41. Per una definizione giurisprudenziale di algoritmico si veda S. Cereda, *Il concetto di algoritmo in una recente sentenza del Consiglio di Stato*, in «MediaLaws, Rivista di diritto dei media», n. 3, 2022, pp. 296-300.

[27] In tema S. Garcia Garcia, *Una aproximacion a la futura reglulacion de la inteligencia artificial en la Union Europea,* in «Revista de estudios europeos», V. 79, 2022, pp. 304-323; M. Laukyte, *Reflexion sobre los derechos fundamentales en la nueva Ley de la Inteligencia Artificial*, in «Derechos y Libertades», n. 51, 2024, pp. 151-175.

[28] S.U. Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism*, NYU Press, New York, 2018.

[29] F. Ciracì, *Algo(r)etica e immigrazione*, cit., p. 37.

[30] F. Palmirotto, *When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis,* in «German Law Journal», 2024, pp. 1-27, in cui si sostiene che le attuali

di algoritmi e di strumenti di intelligenza artificiale voglia essere impiegato per replicare il concetto di «giudizio imparziale», caro al sistema processuale e, anzi, giungendo ad un nuovo standard di efficienza che solo la macchina può raggiungere, spesso sono proprio le peculiarità intrinseche dell'algoritmo che non consentono un giudizio qualificabile come imparziale, laddove il funzionamento dell'intelligenza artificiale si fonda su un'analisi di singole situazioni fattuali che, tuttavia, non vengono valutate come situazioni *sui generis* e, dunque, aventi caratteristiche specifiche e uniche, bensì come «dati» da incamerare, classificare e ricondurre a categorie ampie. Tale considerazione trova maggiore vigore nel caso di meccanismi di intelligenza artificiale con capacità adattive - fondate sull'apprendimento automatico attraverso il *machine learning*, tecnica che utilizza algoritmi che migliorano automaticamente con l'esperienza o imparano autonomamente, senza la necessità di una specifica programmazione - e predittive, in grado, sulla base di dati, di determinare la realizzabilità di eventi futuri. In conclusione, gli algoritmi utilizzati nelle nuove tecnologie di intelligenza artificiale possono potenzialmente risultare discriminatori o in ragione delle istruzioni di partenza (che potremmo definire *bias* indotti dalla programmazione) o in base al risultato della categorizzazione realizzata dagli stessi sistemi (definibili *bias* auto-prodotti dalla stessa IA)[31].

4. *Nuove tecnologie, nuove discriminazioni? L'intervento dell'AI ACT*

L'uso delle nuove tecnologie e, in particolare, dei sistemi decisionali automatizzati, può accelerare i processi decisionali a vantaggio delle agenzie governati-

---

definizioni e categorizzazioni utilizzate dai meccanismi di IA non riescono a cogliere la complessità e la diversità delle situazioni reali. Pertanto, si auspica un utilizzo che prenda atto di tale criticità e che sia fondato sulla tutela dei diritti fondamentali della persona umana, nonché su strumenti di protezione dall'automazione. In tema di comparazione con il sistema tedesco si segnala E. Buoso, *La Pubblica Amministrazione in Germania nell'era dell'Intelligenza Artificiale: procedimenti completamente automatizzati e decisioni amministrative robotiche*, in «PA Persona e Amministrazione», V. 8, n. 1, 2021, pp. 495-524. Nella medesima rivista anche C. Fraenkel-Haeberle, *Procedimenti amministrativi algoritmici: la risposta tedesca*, pp. 525-550.

[31] Sul punto E. Buoso, *La Pubblica Amministrazione in Germania*, cit., p. 519, che, in tema di eventuali discriminazioni, illustra uno specifico accadimento potenzialmente realizzabile, per cui i dati facciano emergere che in un determinato contesto etnico, sociale o religioso sono più frequenti delle irregolarità, per cui l'IA che realizza macro categorie per la «classificazione» delle istanze presentate, sarebbe potenzialmente indotta a ritenere tutti i componenti dello stesso contesto etnico, sociale o religioso come irregolari o, comunque, come soggetti «a rischio».

ve e di alcuni richiedenti[32]. Tuttavia, le stesse nuove tecnologie possono anche portare a nuove vulnerabilità[33] ovvero a potenziare vulnerabilità che già impattano su determinati soggetti, come i migranti. Se, da un lato, l'uso delle nuove tecnologie è in grado (potenzialmente) di facilitare taluni processi decisionali, dall'altro, i rischi intrinseci alle stesse di parzialità, discriminazione e potenziali errori della macchina rappresentano una minaccia significativa per i migranti e richiedenti asilo i cui diritti sono spesso compressi, risultando, così, complicato per i medesimi trovare forme di tutela.

In siffatto contesto, il già limitato accesso all'istruzione dei soggetti migranti sembrerebbe ulteriormente a rischio, a causa di meccanismi di Intelligenza artificiale non in grado di circoscrivere la risposta alla situazione specifica, concentrando, al contrario, l'attenzione alla categorizzazione delle istanze presentate: atteggiamento censurabile in ragione dei *bias* che caratterizzano inevitabilmente il meccanismo di funzionamento delle nuove tecnologie.

Con l'esponenziale aumento dell'uso delle tecnologie basate su meccanismi di intelligenza artificiale, e, di conseguenza, dei pericoli ad esse connesse, l'Unione Europea ha riconosciuto la necessità di garantire un quadro normativo adeguato che bilanci l'innovazione con la protezione della persona e dei diritti fondamentali della stessa, attraverso l'introduzione del Regolamento UE, 13 giugno 2024, n. 1689[34], primo atto normativo che offre, per l'appunto, un quadro normativo

---

[32] D. Ozkul, *Automating immigration and asylum: the uses of new technologies in migration and asylum governance in Europe*, Refugee Studies Centre, University of Oxford, Oxford 2023, p. 5.

[33] C. Nardocci, *Intelligenza Artificiale e discriminazioni*, in «Gruppo di Pisa», n. 3, 2021, pp. 9 - 60; della stessa autrice, *Artificial Intelligence-based Discrimination: Theoretical and Normative Responses. Perspectives from Europe,* in «DPCE Online», n. 3, 2023, pp. 2367-2393; C. Intachomphoo, O.D. Gundersen, *Artificial Intelligence and Race: a systematic review*, in «Legal Information Management», n. 20, 2020, pp. 74-84. In tema si veda A. Pajno, M. Bassini, G. De Gregorio, M. Macchia, F. P. Patti, O. Pollicino, S. Quattrocolo, D. Simeoli, P. Sirena, *AI: profili giuridici – Intelligenza artificiale: criticità emergenti e sfide per il giurista*, in «BioLaw Journal – Rivista di Biodiritto», n. 3, 2019, pp. 205-235; nella stessa rivista S. Quintarelli, F. Corea, F. Fossa, A. Loreggia, S. Sapienza, *AI: profili etici – Una prospettiva etica sull'intelligenza artificiale: principi, diritti e raccomandazioni*, pp. 183-204.

[34] Cronologicamente successivo all'introduzione di numerosi atti fondati sull'esigenza di dettare regole comuni in tema di dati e di diritto digitale, tra cui: Data Act (Regulation (EU) 2023/2854 of the European Parliament and of the Council on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), 13.12.2023), Data Governance Act (Regulation (EU) 2022/868 of the European Parliament and of the Council on European data governance and amending Regulation (EU) 2018/1724, 30.05.2022),

uniforme diretto a disciplinare la commercializzazione, lo sviluppo e l'utilizzo dei sistemi di intelligenza artificiale nel rispetto dei principi fondamentali dell'Unione Europea[35]. L'«European Artificial Intelligence Act»[36], con il suo approccio basato sul «rischio»[37] – definito ai sensi dell'art. 3, par. 1, n. 2 AI ACT, come «la

---

Digital Services Act (Regulation (EU) 2022/2065 of the European Parliament and of the Council, on a Single Market For Digital Services and amending Directive 2000/31/EC, 19.10.2022),

Digital Markets Act (Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, 14.09.2022).

[35] Considerando 1 dell'AI ACT, secondo cui «Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione. Il presente regolamento garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del presente regolamento».

[36] In tema K. Soderlund, S. Larsson, *Enforcement Design Patterns in EU Law: An Analysis of the AI Act*, in «Digital Society», 3:41, luglio 2024, pp. 1-21; C. Nardocci, *Artificial Intelligence at the crossroads between the European Union & the Council of Europe: who safeguards what & how?,* in «Italian Journal of Public Law», V. 16, n. 1, 2024, pp. 165–196; C. Trincado Castan, *The legal concept of artificial intelligence: the debate surrounding the definition of AI System in the AI Act,* in «BIoLaw Journal – Rivista di BioDiritto», n. 1, 2024, pp. 305-334; G. Barone, *Artificial Intelligence Act: un primo sguardo al regolamento che verrà*, in «Cassazione penale», n. 3, 2024, pp. 1047-1062; G. Olivato, *Paving the path towards general purpose AI systems regulation in the AI Act: an analysis of the Parliament's and Council'S proposals*, in «MediaLaws, Rivista di diritto dei media», n. 3, 2023, pp. 50-71; D. Messina, *La proposta di regolamento europeo in materia di Intelligenza Artificiale: verso una "discutibile" tutela individuale di tipo consumer-centric la società dominata dal "pensiero artificiale"*, «MediaLaws, Rivista di diritto dei media», n. 2, 2022, pp. 196-231; C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di Regolamento dell'Unione europea in materia di Intelligenza Artificiale*, in «BioLaw Journal – Rivista di Biodiritto», n. 3, 2021, pp. 415-437.

[37] F.M. Mancioppi, *La regolamentazione dell'intelligenza artificiale come opzione per la salvaguardia dei valori fondamentali dell'UE*, in «federalismi.it», n. 7, 2024, 112-134. A. Pirozzoli, *The human-centric perspective in the regulation of Artificial Intelligence*,

combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso» - riflette la consapevolezza che non tutte le applicazioni in tema di intelligenza artificiale generano gli stessi livelli di impatto e rischio per la società. In altre parole, l'idea principale alla base della normativa è quella di aumentare il livello di rigidità della disciplina al crescere del livello di rischio di violazione dei diritti fondamentali generato dall'IA. In particolare, il quadro legislativo europeo individua diversi livelli di rischio che fungono da guida fondamentale per l'applicazione delle misure introdotte[38].

In tale complesso meccanismo, basato sul sistema di gestione del «rischio» in ordine all'uso dei sistemi di intelligenza artificiale, la materia dell'immigrazione[39], ai sensi dell'art. 6, par. 2 AI ACT, viene qualificata come «ad alto rischio» alla luce della vulnerabilità dei soggetti su cui impatta[40]. La stessa materia

---

in «European Papers», V. 9, n. 1, 2024, pp. 105-116.

[38] Ivi, p. 124, in cui si delinea una «piramide del rischio».

[39] Così come la materia dell'istruzione di cui al par. 1, punto 3 dell'Allegato III, Reg. UE 1689/2024, qualificata, per l'appunto, «ad alto rischio». Sul punto, il Considerando 56 afferma che « i sistemi di IA utilizzati nell'istruzione o nella formazione professionale, in particolare per determinare l'accesso o l'ammissione, per assegnare persone agli istituti o ai programmi di istruzione e formazione professionale a tutti i livelli, per valutare i risultati dell'apprendimento delle persone, per valutare il livello di istruzione adeguato per una persona e influenzare materialmente il livello di istruzione e formazione che le persone riceveranno o a cui potranno avere accesso o per monitorare e rilevare comportamenti vietati degli studenti durante le prove, dovrebbero essere classificati come sistemi di IA ad alto rischio, in quanto possono determinare il percorso d'istruzione e professionale della vita di una persona e quindi può incidere sulla sua capacità di garantire il proprio sostentamento. Se progettati e utilizzati in modo inadeguato, tali sistemi possono essere particolarmente intrusivi e violare il diritto all'istruzione e alla formazione, nonché il diritto alla non discriminazione, e perpetuare modelli storici di discriminazione, ad esempio nei confronti delle donne, di talune fasce di età, delle persone con disabilità o delle persone aventi determinate origini razziali o etniche o un determinato orientamento sessuale».

[40] Si veda il Considerando 60, secondo cui «I sistemi di IA utilizzati nel settore della migrazione, dell'asilo e della gestione del controllo delle frontiere hanno effetti su persone che si trovano spesso in una posizione particolarmente vulnerabile e il cui futuro dipende dall'esito delle azioni delle autorità pubbliche competenti. L'accuratezza, la natura non discriminatoria e la trasparenza dei sistemi di IA utilizzati in tali contesti sono pertanto particolarmente importanti per garantire il rispetto dei diritti fondamentali delle persone interessate, in particolare i loro diritti alla libera circolazione, alla non discriminazione, alla protezione della vita privata e dei dati personali, alla protezione internazionale e alla buona amministrazione. È pertanto opportuno classificare come ad alto rischio, nella misura in cui il loro uso è consentito dal pertinente diritto dell'Unione e nazionale, i sistemi di IA destinati a essere utilizzati

dell'immigrazione si trova contenuta nell'Allegato III del Regolamento in oggetto che, al par. 1, punto 7, lett. b) e c) definisce, con riferimento alla materia della «migrazione, asilo e gestione del controllo delle frontiere», impiegabili dallo Stato membro - tenendo presente che trattasi di materia ad «ad alto rischio» - «i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti o per loro conto, oppure da istituzioni, organi e organismi dell'Unione, per valutare un rischio (compresi un rischio per la sicurezza, un rischio di migrazione irregolare o un rischio per la salute) posto da una persona fisica che intende entrare o è entrata nel territorio di uno Stato membro» (lett. b)), e «i sistemi di IA destinati a essere usati dalle autorità pubbliche competenti o per loro conto, oppure da istituzioni, organi e organismi dell'Unione, per assistere le autorità pubbliche competenti nell'esame delle domande di asilo, di visto o di permesso di soggiorno e per i relativi reclami per quanto riguarda l'ammissibilità delle persone fisiche che richiedono tale status, compresa le valutazioni correlate dell'affidabilità degli elementi probatori» (lett. c)). Alla luce della qualificazione dei sistemi IA come

---

dalle autorità pubbliche competenti, o per loro conto, o dalle istituzioni, dagli organi o dagli organismi dell'Unione, incaricati di compiti in materia di migrazione, asilo e gestione del controllo delle frontiere, come poligrafi e strumenti analoghi, per valutare taluni rischi presentati da persone fisiche che entrano nel territorio di uno Stato membro o presentano domanda di visto o di asilo, per assistere le autorità pubbliche competenti nell'esame delle domande di asilo, di visto e di permesso di soggiorno e dei relativi reclami in relazione all'obiettivo di determinare l'ammissibilità delle persone fisiche che richiedono tale status, compresa la connessa valutazione dell'affidabilità degli elementi probatori, al fine di individuare, riconoscere o identificare persone fisiche nel contesto della migrazione, dell'asilo e della gestione del controllo delle frontiere con l'eccezione della verifica dei documenti di viaggio. I sistemi di IA nel settore della migrazione, dell'asilo e della gestione del controllo delle frontiere disciplinati dal presente regolamento dovrebbero essere conformi ai pertinenti requisiti procedurali stabiliti dal regolamento (CE) n, 810/2009 del Parlamento europeo e del Consiglio, dalla direttiva 2013/32/UE del Parlamento europeo e del Consiglio, e da altre pertinenti disposizioni di diritto dell'Unione. I sistemi di IA nel settore della migrazione, dell'asilo e della gestione del controllo delle frontiere non dovrebbero in alcun caso essere utilizzati dagli Stati membri o dalle istituzioni, dagli organi o dagli organismi dell'Unione come mezzo per eludere gli obblighi internazionali a essi derivanti a titolo della convenzione delle Nazioni Unite relativa allo status dei rifugiati firmata a Ginevra il 28 luglio 1951, modificata dal protocollo del 31 gennaio 1967. Essi non dovrebbero essere utilizzati per violare in alcun modo il principio di non respingimento o per negare sicure ed efficaci vie legali di ingresso nel territorio dell'Unione, compreso il diritto alla protezione internazionale». In tema di preoccupazioni in ordine a nuove possibili forme di discriminazione fondate sul nuovo Regolamento si veda R. De Caria, *L'AI Act e il divieto di discriminazioni,* in «MediaLaws, Rivista di diritto dei media», 30 marzo 2022.

«ad alto rischio» il Regolamento UE stabilisce stringenti regole per i produttori, importatori e utenti professionali[41], tra cui la «Valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio» (art. 27) e la «Sorveglianza umana» (art. 14).

Con riferimento alla valutazione d'impatto, ai sensi dell'art. 27, l' AI ACT afferma che «prima di utilizzare un sistema di IA ad alto rischio […] i deployer[42] che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici […] effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre»[43]. Pertanto, in base ai risultati della «Valutazione di impatto», i deployers saranno tenuti a sviluppare piani per mitigare le eventuali conseguenze negative sui diritti fondamentali e, qualora non possano regolarizzarsi le medesime conseguenze negative, con conseguente impossibilità di formulare un piano adeguato, dovranno cessare la distribuzione del sistema IA. Tuttavia, esistono talune perplessità legate alla «Valutazione di impatto». Il primo elemento di criticità riguarda il soggetto che conduce la valutazione, il quale sarà chiamato a realizzare una operazione di bilanciamento tra l'uso dei sistemi di IA e l'impatto sui diritti fondamentali. In altre parole, dovrà comprendersi se l'impatto dell'IA può risultare tollerabile o, al contrario, comporterà una compressione eccessiva per i diritti dei migranti[44]. La seconda

---

[41] E. Longo, *Il possibile impatto dell'AI Act sull'immigrazione: iniziamo a discuterne*, in «ADiM BLOG, Editoriale», febbraio 2023.

[42] Definito dallo stesso AI ACT come «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale».

[43] In particolare, le attività che dovranno essere realizzate sono: a) una descrizione dei processi del deployer in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista; b) una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza; c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico; d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13; e) una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso; f) le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo.

[44] Valutazione che, allo stato, non sembra realizzabile sulla base di orientamenti o linee guida, il che comporta una forma di autoregolamentazione che potrebbe portare a ineguaglianza e incertezza a livello di trattamento amministrativo. Sul punto C. Novelli, *L'Artificial Intelligence Act Europeo: alcune questioni di implementazione*, in «federalismi.it», n. 2, 2024, pp. 95-113.

criticità, invece, appare legata all'omogeneità delle «Valutazioni» realizzate dai diversi operatori pubblici che non garantirebbe certezza nella gestione dell'impatto sui diritti fondamentali[45].

Inoltre, sebbene possa apparire esclusivamente una formula di principio, sembra decisiva la disposizione di cui all'art. 14 AI ACT, in tema di necessarietà di una «Sorveglianza umana», secondo cui «i sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso» al fine di «prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere» dall'utilizzo dei meccanismi di intelligenza artificiale.

Il meccanismo di «sorveglianza umana», così come l'approccio cd. human in the loop[46] - che colloca la conoscenza e l'esperienza delle persone al centro dei processi di apprendimento automatico - dovranno orientare l'intero sistema basato sui sistemi di intelligenza artificiale che, oltre a garantire spazi di intervento umano in senso correttivo, dovrà assicurare un intervento etico[47], non potendosi la macchina sostituire al decisore umano. Solo attraverso una «intelligenza artificiale antropocentrica», fondata solo su sistemi caratterizzati da un atteggiamento volto al servizio dell'uomo, senza pretese di sostituzione[48], si potrà giungere alla creazione di meccanismi non limitanti dei diritti, soprattutto, di soggetti vulnerabili come i migranti.

5. *Conclusioni*

Il contributo, prendendo in considerazione l'avvento delle nuove tecnologie fondate su algoritmi decisori, nonché predittivi, mostra «i rischi» di un utilizzo

---

[45] *Ivi*, p. 112.

[46] Per un'analisi dell'approccio si veda E. Mosqueira-Rey, E. Hernandez Pereira, D. Alonso Rios, J. Bobes Bascaran, A. Fernandez Leal, *Human in the loop machine learning: a state of the art*, in «Artificial Intelligence Review», n. 56, 2023, pp. 3005-3054; B. Marchetti, *La garanzia dello human in the loop alla prova della decisione amministrativa algoritmica*, in «BioLaw Journal – Rivista di Biodiritto», n. 2, 2021, pp. 367-385. Sulla centralità del soggetto umano si veda altresì F.M. MANCIOPPI, *The anthropocentric view in the bill on AI introduced by the Italian Government*, in «MediaLaws, Rivista di diritto dei media», 19 settembre 2024; A. Pirozzoli, *The human-centric perspective,* cit., p. 114.

[47] In tema L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Raffaello Cortina Editore, Milano, 2022, in cui si sottolinea, tra gli altri, il valore della dignità umana che deve porsi alla base della decisione (anche) algoritmica.

[48] F.M. Mancioppi, *The anthropocentric view*, cit.

privo di limiti per la tutela dei diritti di soggetti particolarmente vulnerabili, come i migranti (in particolare, il diritto all'istruzione, già alquanto limitato), evidenziando, altresì, il possibile insorgere di «discriminazioni 2.0» fondate proprio sull'utilizzo dell'intelligenza artificiale.

Per provare a rintracciare un limite che possa scongiurare i rischi appena evidenziati l'analisi ha concentrato l'attenzione su due nuovi istituti (la «Valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio» e la «Sorveglianza umana»), introdotti dal nuovo Regolamento UE 1689/2024, ma che sembrano trovare fondamento in concetti già noti e da cui l'impianto delle nuove tecnologie non sembra potersi sganciare.

Il rischio che le macchine, svolgendo la serie dei passaggi logici previsti per lo svolgimento delle operazioni, possano creare delle situazioni configurabili come discriminatorie ha portato il Consiglio di Stato a delineare il «principio di non discriminazione algoritmica», alla stregua del quale è necessario programmare i sistemi di intelligenza artificiale in modo che non vengano attuate ingiuste distinzioni che possano ledere i diritti umani[49]. Da questa angolazione, appare irrinunciabile il concetto di «sovranità umana»[50], espressione fondata sull'orientamento antropocentrico che deve orientare tutti i sistemi basati sull'utilizzo delle nuove tecnologie. Pertanto, la decisione amministrativa, proprio perché riferita a bisogni, interessi e aspettative umane, dovrà provenire da un decisore su cui la volontà della persona possa incidere e in cui la persona conserva il ruolo principale e l'intelligenza artificiale diviene esclusivamente un supporto per meglio declinare il principio di efficienza e buon andamento, in grado di avere ricadute positive sulla qualità della vita e in termini di tutela dei diritti umani[51].

In altre parole, dovrà assicurarsi centralità all'individuo sia in quanto destinatario della decisione sia in quanto influente sulla stessa decisione finale, dovendosi assicurare, con riguardo al momento finale dell'assunzione della scelta, meccanismi con cui il risultato elaborato dal software, prima di rifluire in una decisione, possa essere sottoposto a revisione da parte di una persona fisica che

---

[49] F. Laviola, *Algoritmico, troppo algoritmico: decisioni amministrative automatizzate, protezione dei dati personali e tutela delle libertà dei cittadini alla luce della più recente giurisprudenza amministrativa*, in «BioLaw Journal – Rivista di Biodiritto», n. 3, 2020, pp. 389-440.

[50] R. Rolli, *La necessaria lettura antropocentrica della lettura 4.0*, in «PA, Persona e Amministrazione», V. 8, n. 1, 2021, p. 595.

[51] *Ibidem*. Sul punto anche P. Piras, *L'amministrazione digitale tra divari e doveri. "Non camminare davanti a me, ma al mio fianco"*, in «PA, Persona e Amministrazione», V. 11, n. 2, 2022, pp. 417-432.

sia a ciò preposta[52]. Ciò che si auspica è la cd. «riserva di umanità»[53], che trova fondamento diretto nella Costituzione, imperniata su una lettura che pone l'uomo al centro del sistema sia in quanto destinatario di tutele agganciate ai bisogni e alla soddisfazione di diritti umani legati al concetto di «dignità», sia in quanto decisore.

[52] G. Gallone, *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione tra procedimento e processo*, Cedam, Milano, 2023. Dello stesso autore, *Digitalizzazione, Amministrazione e Persona: per una "riserva di umanità" tra spunti codicistici di teoria giuridica dell'automazione*, in «PA, Persona e Amministrazione», V. 12, n. 1, 2023, pp. 329-365; J. Ponce Sole', *Limites juridicos de la toma de decisions discrecionales automatizadas mediante inteligencia artificial: racionalidad, sabiduria y necesaria reserva juridica de humanidad en el ambito digital*, in «Revista General de Derecho Administrativo», n. 66, 2024; dello stesso autore, *Inteligencia artificial, derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debito tecnologico*, in «Revista General de Derecho Administrativo», n. 50, 2019.

[53] Da intendere come il divieto di esercizio delle potestà amministrative in forma totalmente meccanica e automatizzata senza alcun contributo della persona fisica. Per un'analisi più approfondita si vedano i riferimenti precedenti.

Sezione II
IA, PROCESSO E PROCEDIMENTO

Sui limiti, anche costituzionali, all'utilizzo dell'intelligenza artificiale nel processo civile e sui possibili risvolti in tema di validità degli atti

di **Francesca Casciaro**

1. *Premessa – Luci ed ombre sull'intelligenza artificiale: l'ultima frontiera della rivoluzione tecnologica*

Gli anni più recenti sono stati caratterizzati da un'evoluzione tecnologica profonda ed incessante, tale da assumere le fattezze di una vera e propria rivoluzione, per la sua attitudine a stravolgere i nostri costumi ed abitudini di vita.

L'approdo finale di questo processo – peraltro ancora in divenire – è rappresentato dallo sviluppo dell'intelligenza artificiale: un campo dell'informatica che sviluppa sistemi in grado di svolgere compiti ed operazioni complesse emulando (sembrerebbe) il funzionamento dell'intelligenza umana.

L'intelligenza artificiale, dunque, fa un passo avanti rispetto agli algoritmi tradizionali.

Questi ultimi hanno una struttura rigida e deterministica: si limitano ad eseguire le istruzioni predefinite da colui che li ha programmati, fornendo, sulla base delle stesse, una risposta univoca.

Invece, gli algoritmi di intelligenza artificiale non seguono regole fisse, ma sono progettati per imparare dai dati "di addestramento" che vengono inseriti nel sistema dal programmatore (c.d. *machine learning*, o autoapprendimento della macchina)[1]. Questo consente alla macchina di migliorare le proprie pre-

[1] Per un approfondimento in ordine alla nozione di intelligenza artificiale cfr. G. Sartor, *L'intelligenza artificiale e il diritto*, Torino, 2022, 3; C. Casonato, *Intelligenza*

stazioni sulla base delle esperienze maturate, nonché di adattarsi automaticamente alla gestione di nuove variabili. Tuttavia, la capacità inferenziale[2] che caratterizza tali sistemi, fa sì che essi tendano a risposte probabilistiche e non univoche.

L'ultima frontiera di questa nuova tecnologia è la c.d. intelligenza artificiale generativa, ossia una sottocategoria di intelligenza artificiale che si contraddistingue per la sua capacità di elaborare i dati in maniera creativa[3], generando contenuti originali (come immagini, video, testi, traduzioni o codici di programmazione). Inoltre, quei modelli di intelligenza artificiale generativa specializzati nell'elaborazione del linguaggio e nella creazione di testi prendono il nome di «LLM» (acronimo di Large Language Model).

Tale breve premessa, di ordine squisitamente tecnico, si è resa necessaria al fine di far luce sulle potenzialità ed i benefici che tali nuove tecnologie potrebbero apportare al settore della giustizia[4], essendo innegabile che l'utilizzo di tali

---

artificiale e giustizia: potenzialità e rischi, in *DPCE online,* 3, 2020, 3371; F. De Stefano, *Intelligenza artificiale e redazione degli atti giudiziari civili*, in *Giustizia Insieme*, 5 febbraio 2024, https://www.giustiziainsieme.it/it/diritto-e-innovazione/3034-intelligenza-artificiale-e-redazione-degli-atti-giudiziari-civili.

[2] Sul punto, si rinvia al considerando n. 12 dell'Reg. UE 1689/2024 (AI Act), ove si afferma che: «Una caratteristica fondamentale dei sistemi di IA è la loro capacità inferenziale. Tale capacità inferenziale si riferisce al processo di ottenimento degli output (…) e alla capacità dei sistemi di IA di ricavare modelli o algoritmi da input o dati. Le tecniche che consentono l'inferenza nella costruzione di un sistema di IA comprendono approcci di apprendimento automatico che imparano dai dati come conseguire determinati obiettivi e approcci basati sulla logica e sulla conoscenza che traggono inferenze dalla conoscenza codificata o dalla rappresentazione simbolica del compito da risolvere».

[3] Sul punto v. F. Barracca, *L'intelligenza artificiale generativa nel processo civile: prime normative e prospettive di applicazione,* in *Ius, Processo Civile*, 4 settembre 2024, https://ius.giuffrefl.it/dettaglio/10979114/lintelligenza-artificiale-generativa-nel-processo-civile-prime-normative-e-prospettive-di-applicazione, per cui «l'IA generativa funziona apprendendo modelli e caratteristiche da ampie raccolte di dati. Si basa su una comprensione statistica del linguaggio: il suo scopo è quello di definire, con la massima certezza possibile, la parola successiva, senza alcuna conoscenza propria».

[4] Sul punto v. M. Civinini, *Nuove tecnologie e giustizia*, in *Questione Giustizia,* 19 febbraio 2023, https://www.questionegiustizia.it/articolo/nuove-tecnologie-e-giustizia, 2. Con riferimento al rapporto tra innovazioni tecnologiche e amministrazione della giustizia, l'Autrice ritiene che «L'introduzione della tecnologia nell'amministrazione della giustizia, finalizzata al miglioramento della qualità e dell'efficienza, non può essere ragionevolmente contrastata. I giudici non possono tornare nella loro torre d'avorio e vivere a distanza da un mondo in cui professionisti e giovani useranno la tecnologia; la legittimità e la percezione della magistratura potrebbero essere gravemente compromesse,

modelli potrebbe fornire un contributo significativo[5] all'incremento della produttività e dell'efficienza degli uffici giudiziari e che tale apporto, in un sistema come il nostro – caratterizzato dall'endemica crisi della giustizia civile e dall'irragionevole durata dei processi – sarebbe viepiù prezioso.

In primo luogo, l'intelligenza artificiale potrebbe essere proficuamente adoperata nello svolgimento delle attività organizzative dei Tribunali, svolgendo con rapidità e precisione i compiti inerenti alla gestione del personale e all'assegnazione delle cause ai magistrati e, rapportando i molteplici elementi che possono venire in rilievo (quali le competenze dei singoli, il carico di lavoro e le tempistiche di risoluzione dei procedimenti) potrebbe ricercare le soluzioni più efficienti[6].-

Inoltre, l'IA potrebbe fornire un preziosissimo contributo anche nel facilitare e velocizzare la ricerca giurisprudenziale[7]. Sono molte le banche dati giuridiche che stanno implementando il loro funzionamento con l'utilizzo dell'intelligenza artificiale, che consente una migliore indicizzazione dei contenuti, l'esecuzione di ricerche c.d. semantiche (che non richiedono la necessaria corrispondenza tra la parola chiave inserita nel pannello di ricerca ed i termini utilizzati nei testi), nonché l'analisi e la sintesi automatica delle sentenze. Tutto ciò consentirebbe una maggiore conoscibilità (e, di conseguenza, anche la prevedibilità) delle decisioni, favorendo la certezza del diritto[8].

---

così come il ruolo della giustizia».

[5] Sui vantaggi e sulle sfide legate ad una digitalizzazione della giustizia cfr. M. Civinini, *Nuove tecnologie,* cit.,4. Cfr. anche G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Diritto penale contemporaneo*, 4, 2024, 75, per il quale un incontro tra il mondo del diritto e quello dell'intelligenza artificiale e dell'evoluzione tecnologica rappresenta un'esigenza «ineludibile».

Sulle ragioni che hanno portato allo sviluppo ed all'applicazione dell'intelligenza artificiale nel campo del diritto v. D. Bourcier, *La décision artificielle: le droit, la machine et l'humain*, Paris, 1995, 27; C. Aguzzi, *Le juge et l'intelligence artificielle: la perspective d'une justice rendue par la machine*, in *Annuaire international de justice constitutionnelle, 35-2019, 2020. Constitution et environnement- La justice predictive,* 622.

[6] Esemplificativamente, si considerino i compiti e le incombenze amministrative ed organizzative svolte dai Presidenti dei Tribunali e dai Presidenti di sezione, così come la gestione dei ruoli di udienza e le attività di monitoraggio delle scadenze e di segnalazione di eventuali inefficienze, che ben potrebbero essere delegate all'intelligenza artificiale.

[7] Sul punto v. S. Abiteboul, F. G'sell, *Les algorithmes pourraient-ils remplacer les juges?*, in F. G'sell (dir.), *Le Big Data et le droit*, Paris, Dalloz, 2019, https://inria.hal.science/hal-02304016v2/document, 4.

[8] Così M. Civinini, *Nuove tecnologie*, cit, 13, secondo cui «i sistemi che utilizzano l'IA potrebbero aiutare i giudici (ma anche gli avvocati) a: ottenere una migliore e più

Da ultimo, i modelli «LLM» (ossia quegli algoritmi di intelligenza artificiale specializzati nella creazione di contenuti testuali) potrebbero essere finanche utilizzati per la redazione dei provvedimenti finali: un'intelligenza artificiale collegata alla rete internet ed alle banche dati è capace di analizzare ed elaborare una mole impressionante di dati ed informazioni, assumere una decisione ed argomentarla per iscritto e, nel compiere tutte queste attività, disporrebbe di una precisione ed una rapidità alle quali un essere umano mai potrebbe aspirare[9].

Con riferimento all'attività defensionale svolta dall'avvocato, invece, l'intelligenza artificiale potrebbe essere utilizzata non solo per agevolare l'espletamento di attività organizzative e/o automatiche (come il controllo capillare dei termini e delle scadenze per il deposito degli atti e per la proposizione delle impugnazioni), ma anche per prevedere le decisioni del giudice e – di conseguenza – suggerire al legale le migliori strategie difensive da adoperare per cambiare l'esito della lite.

In altri termini, la macchina potrebbe esaminare, nell'arco di pochi istanti, tutte le pronunce di quel giudice su questioni simili o analoghe, rapportarle con la giurisprudenza di altre Corti e Tribunali ed individuare gli argomenti giuridici che – con maggiori probabilità – potrebbero far ottenere una sentenza favorevole.

Inoltre, l'avvocato potrebbe avvalersi dell'intelligenza artificiale generativa per la stessa redazione dell'atto processuale, riducendo drasticamente le tempistiche

---

rapida conoscenza dei casi; migliorare e velocizzare la stesura dei documenti; selezionare le parti più significative dei precedenti; fare un uso migliore e più consapevole dei precedenti; migliorare la leggibilità dei documenti legali e delle decisioni giudiziarie; prevedere una possibile decisione sulla base dei precedenti; capire come una possibile decisione si posizionerebbe nel quadro dei precedenti».

[9] Sul punto v. D. Dalfino, *Stupidità (non solo) artificiale, predittività e processo*, in *Questione giustizia*, 3 luglio 2019, https://www.questionegiustizia.it/articolo/stupidita-non-solo-artificiale-predittivita-e-processo_03-07-2019.php, il quale rileva che, con l'utilizzo dell'intelligenza artificiale, «si potrebbero automatizzare molte delle eccezioni processuali generalmente risolte nella prima udienza (mancanza di capacità di agire in caso di minore età, difetto di rappresentanza, sussistenza di precedente giudicato, litispendenza)».

Cfr. anche M. Ancona, *Giustizia predittiva*, in *Il processo telematico*, 7 ottobre 2019, ove l'Autore osserva che «nel nostro ordinamento alcune ipotesi di giustizia predittiva già esistono», come nel processo amministrativo telematico (DPCM 16 febbraio 2016, n. 40), che «ha introdotto le norme tecnico-operative che consentono al sistema informatico procedure automatiche di controllo della regolarità formale degli atti e documenti prodotti nell'ambito del processo amministrativo telematico, subordinando all'esito positivo di tale controllo le operazioni di acquisizione e registrazione di tali atti e documenti. Il tutto, senza l'intervento del giudice».

di studio e di scrittura ed assicurando il rispetto dei parametri di sinteticità e chiarezza richiesti dalla legge.

Icasticamente, si potrebbe finanche osservare che l'utilizzo dell'intelligenza artificiale potrebbe avere il pregio di rendere la tutela dei diritti altamente democratica, assicurando uno *standard* minimo di competenza e capacità espositiva ed evitando quegli errori umani che, talvolta, pregiudicano irrimediabilmente la difesa del cliente.

Tuttavia, tali prospettive avveniristiche, se da un lato ci consentono di cogliere a pieno le potenzialità e i benefici che queste nuove tecnologie potrebbero potenzialmente apportare nel migliorare l'efficienza del sistema giudiziario, d'altra parte destano scetticismo e preoccupazione (se non – addirittura – sgomento): immaginare un mondo in cui l'essere umano abdica al proprio ruolo di custode dei diritti dei singoli, per delegare tale compito ad una macchina, suscita una marcata inquietudine.

Tali remore, invero, risultano acuite dalla circostanza che l'intelligenza artificiale non è progettata per fornire risposte univoche, bensì probabilistiche e ciò non consentirebbe una piena controllabilità degli esiti decisionali.

Inoltre, molti sistemi di intelligenza artificiale non riescono a garantire, in termini assoluti, l'accuratezza e la veridicità delle informazioni e delle soluzioni che forniscono.

I modelli di intelligenza artificiale generativa sono programmati per generare risposte sulla base dei dati e degli schemi linguistici presenti nel loro addestramento ma, quando non dispongono di informazioni sufficienti per fornire una risposta esatta alla domanda specificamente posta, spesso non sono progettati per ammettere la loro mancanza di conoscenza, ma tendono comunque a fornire quella che appare la soluzione più plausibile (individuata sulla base delle relazioni statistiche tra le frasi e le parole che rientrano nel loro *background* conoscitivo)[10]. In questo modo, vengono assicurate fluidità e coerenza del linguaggio generato e viene ottimizzata l'esperienza dell'utente, ma ciò va irrimediabilmente a scapito dell'esattezza delle soluzioni fornite.

L'evenienza che la macchina fornisca risposte errate, senza esprimersi in termini dubitativi ed invitare ad un maggiore approfondimento, è suscettibile di generare molteplici inconvenienti in ambiti – come quello del diritto – che devono essere caratterizzati dalla maggiore certezza possibile[11].

---

[10] Sul punto v. G. Finocchiaro, in *Riv. trim. dir. proc*, 2, 2024, 425.

[11] F. Barracca, *L'intelligenza artificiale generativa nel processo civile: prime normative e prospettive di applicazione, cit.,* per cui «il maggior rischio derivante dall'IA generativa è quello della potenziale produzione di informazioni di fatto inesatte (risposte false, "allucinazioni" e "pregiudizi")».

Tali rilievi finiscono per mettere in dubbio la certezza dei benefici che l'utilizzo dell'IA potrebbe apportare nel settore giustizia.

2. *Un difficile bilanciamento tra rischi e benefici: i limiti costituzionali all'utilizzo dell'intelligenza artificiale e gli ulteriori limiti derivanti dai principi generali del processo civile*

Alle criticità legate all'inattendibilità delle risposte generate dai sistemi di IA si aggiungono ulteriori remore che portano ad opporsi ad un utilizzo indiscriminato della nuova tecnologia, specialmente in quei settori che, per le loro intrinseche caratteristiche, sono particolarmente sensibili e richiedono particolari controlli, fra i quali, indiscutibilmente, quello della giustizia.

Le ragioni che portano ad auspicare un uso controllato e circoscritto dell'intelligenza artificiale rinvengono la loro *ratio* nella stessa architettura costituzionale.

In primo luogo, si deve rilevare che l'importanza fondamentale attribuita dalla Carta fondamentale alla funzione giurisdizionale, unitamente al suo ruolo imprescindibile nella salvaguardia dei beni giuridici di rilievo costituzionale, costituisce un ostacolo al conferimento – in tale ambito – di un ruolo rilevante a sistemi algoritmici.

Inoltre, un ulteriore limite si impone alla luce del principio di centralità della persona umana, desumibile dall'art. 2 Cost., poiché affidare a un modello di intelligenza artificiale una funzione decisionale di rilievo nei processi che impattano sui diritti fondamentali della persona presenterebbe ineludibili rischi, minando la libertà e la dignità dell'individuo[12].

Tutto ciò evidenzia l'importanza di salvaguardare la supervisione umana sul processo decisionale.

Ulteriori argomenti in tal senso possono essere tratti dall'art. 25 Cost. che, nel prevedere che nessuno possa essere distolto dal giudice naturale precostituito per legge, si fa carico di tali esigenze. In tale disposizione, si rinviene uno dei principali pilastri che sorreggono i principi di autonomia, terzietà ed imparzialità che devono sempre contraddistinguere l'esercizio della funzione giurisdizionale a garanzia dei cittadini e della loro fiducia nel sistema giudiziario[13].

---

[12] Cfr. F. Donati, *Intelligenza artificiale e giustizia,* in *Rivista Aic*, 1, 2020, 423.

[13] A tal proposito v. M. Civinini, *Nuove tecnologie*, cit, 11. L'Autrice si interroga sulle possibili conseguenze dell'applicazione dell'intelligenza artificiale a supporto del processo decisionale del giudice sui principi di indipendenza ed imparzialità della magistratura. Nello stesso senso cfr. A. Di Domenico, *Intelligenza artificiale nella decisione giudiziaria: nuove prospettive per il processo penale*, in *Cammino diritto*, 10 giugno 2020, 5440_6-2020.pdf.

Tale visione trova conferma anche nelle disposizioni del Titolo IV della Costituzione, volte a disciplinare la magistratura e l'ordinamento giurisdizionale, come l'art. 102 Cost. che – nel prevedere che la funzione giurisdizionale debba essere esercitata dai magistrati – sembra vietare implicitamente che questi ultimi possano abdicare a tale compito in favore un sistema di intelligenza artificiale (e di chi lo ha programmato[14]).

D'altronde, vi sarebbero resistenze anche di ordine etico e morale ad abbracciare l'idea di una giustizia interamente algoritmica: la nostra stessa cultura è imperniata sull'idea che la giustizia sia un fatto intrinsecamente umano, espressione non solo di ferrei precetti e rigide regole, ma anche di equilibrio e buon senso[15].

---

[14] Sul punto cfr. D. Dalfino, *Stupidità (non solo) artificiale, predittività e processo, cit;* M. Borgobello*, AI e giusto processo, facciamo il punto: le norme, le applicazioni, le sentenze*, in *Agenda Digitale*, 17 gennaio 2024, https://www.agendadigitale.eu/documenti/giustizia-digitale/ai-e-giusto-processo-facciamo-il-punto-le-norme-le-applicazioni-le-sentenze/.

[15] Cfr. D. Dalfino, *Stupidità (non solo) artificiale*, cit; Id, *Decisione amministrativa robotica ed effetto performativo. Un beffardo algoritmo per una "buona scuola"*, in *Questione Giustizia*, https://www.questionegiustizia.it/articolo/decisione-amministrativa-robotica-ed-effetto-performativo-un-beffardo-algoritmo-per-una-buona-scuola_13-01-2020.php. Nello stesso senso v. A. Garapon, *Les enjeux de la justice prédictive*, in *La semaine juridique (édition générale),* 1-2, 2017, 31.

Si pone i medesimi interrogativi C. Aguzzi, *Le juge et l'intelligence artificielle*, cit, 621 e in part. p. 624 e 628. L'Autore si chiede se l'uso degli strumenti di AI possa mettere in discussione l'attuale modo di concepire il giudizio, in linea con la contrapposizione che si suole fare tra la creatività presunta del giudice e la logica puramente matematica dell'intelligenza artificiale. Inoltre, evidenzia come il processo cognitivo sotteso all'atto del giudicare non possa essere ricondotto al mero «ragionamento sillogistico», a meno di non voler ritenere – come faceva Montesquieu – che «il potere di giudicare è in qualche modo nullo», tornando all'antica (e superata) concezione del giudice come «bouche de la loi»; vi sono infatti decisioni «complesse» per le quali la libertà dell'interprete e la capacità creativa che essa implica renderebbero più difficile l'utilizzo dell'intelligenza artificiale.

Cfr. anche S. Abiteboul, F. G'sell, *Les algorithmes pourraient-ils remplacer les juges ?,* cit., 4 e 8. Gli Autori osservano che anche la giustizia umana è ben lontana dall'essere perfetta, poiché i giudici sono spesso influenzati da preferenze politiche, origini etniche, genere, caratteristiche demografiche, nonché da fattori ulteriori quali la tendenziale riluttanza a prendere più decisioni consecutive nella stessa direzione, il contesto di una campagna elettorale, il contesto mediatico, i risultati di una squadra di calcio locale e (finanche) la data di compleanno dell'imputato. Benché la motivazione della sentenza abbia la funzione di convincere i suoi destinatari della «giustizia» della decisione, questa non sempre è chiara e comprensibile. Dunque, «la parzialità degli esseri umani incaricati di giudicare i propri simili, così come l'eventuale opacità del processo decisionale, possono portare a concludere che un'intelligenza artificiale programmata per prendere decisioni

La garanzia di un controllo umano sull'operato della macchina si conferma, allora, un'esigenza imprescindibile.

Tutto ciò trova riflesso nei «sette principi etici per un'IA affidabile», elaborati dall'AI HLEG[16] (un gruppo di esperti nominati dalla Commissione europea) nel 2019, che (sebbene non vincolanti) dovrebbero essere impiegati nella progettazione ed utilizzo dei sistemi di intelligenza artificiale. Il primo fra questi principi è quello di «intervento e sorveglianza umani», alla luce del quale «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 esseri umani*»[17]. Gli altri sei principi comprendono: «robustezza tecnica e sicurezza, vita privata e governance dei dati, trasparenza, diversità*, non discriminazione ed* equità*, benessere sociale e ambientale e* responsabilità» e mirano a prevenire «l'uso illegale del sistema da parte di terzi, ad assicurare il rispetto delle norme in materia di vita privata e protezione dei dati, a consentire un'adeguata tracciabilità degli stessi, a promuovere la parità *di accesso* ai modelli di IA, l'uguaglianza di genere e la diversità *culturale,* ad evitare effetti discriminatori ed ingiusti pregiudizi, nonché ad assicurare che "vengano sviluppati e utilizzati in modo sostenibile e rispettoso dell'ambiente e in modo da apportare benefici a tutti gli esseri umani, monitorando e valutando gli impatti a lungo termine sull'individuo, sulla società *e sulla democrazia*»[18].

---

in base a criteri oggettivi, in modo quasi matematico, potrebbe, alla fine, rivelarsi più giusta e legittima». Tali conclusioni, tuttavia, sono poi parzialmente disattese, poiché gli Autori osservano, conclusivamente, che anche la decisione algoritmica non sempre è giusta per definizione, in quanto «un algoritmo può essere progettato male o basarsi su dati di scarsa qualità e distorti. Gli algoritmi non operano correttamente per loro natura». A tal proposito v. C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy,* New York, 2016*;* J. Angwin, J. Larson, S. Mattu, L. Kirchner, *Machine Bias*, in *Pro Publica*, 23 maggio 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; L. Armstrong, A. Liu, S. MacNeil, D. Metaxa, *The Silicon Ceiling: Auditing GPT's Race and Gender Biases in Hiring Proceedings of the 4th ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization*, 2024, https://dl.acm.org/doi/pdf/10.1145/3689904.3694699 ; G. Ubertis, *Intelligenza artificiale, giustizia penale,* cit, 78.

Sui possibili esiti discriminatori delle decisioni algoritmiche cfr. anche G. Sartor, *L'intelligenza artificiale e il diritto*, cit.,70.

[16] Per gli orientamenti redatti dall'AI HLEG per un'intelligenza artificiale etica ed affidabile v. ai_hleg_ethics_guidelines_for_trustworthy_ai-en_87F84A41-A6E8-F38C-BFF661481B40077B_60419.pdf

[17] Cfr. considerando n. 27, Reg. UE 1689/2024 (c.d. AI Act).

[18] Sul punto, cfr. anche M. Civinini, *Nuove tecnologie*, cit, 7. L'Autrice rileva che

3. *La legislazione positiva: il varo dell'AI Act del Parlamento europeo e il d.d.l. n. 1146 AS del Governo italiano*

Il 2 agosto 2024 è formalmente entrato in vigore l'AI Act, approvato dal Parlamento Europeo il 13 marzo dello stesso anno, sulla base della proposta presentata dalla Commissione.

Lo scopo del Regolamento (art. 1, co. 1) è quello di introdurre, all'interno dell'Unione, una disciplina armonizzata in materia di intelligenza artificiale, realizzando un contemperamento tra la promozione dell'innovazione tecnologica e le esigenze legate alla tutela dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione Europea (salute, sicurezza, ambiente, democrazia e Stato di diritto), nonché la garanzia delle libertà fondamentali sancite dai trattati.

L'obbiettivo è, dunque, quello di promuovere un'intelligenza artificiale «antropocentrica», rendendo l'Unione un «leader nell'adozione di un'AI affidabile» e sicura.

A tal fine, il regolamento opera una classificazione dei sistemi di intelligenza artificiale sulla base del rischio che il loro utilizzo potrebbe generare, distinguendo tra: a) pratiche con «rischio inaccettabile», totalmente vietate; b) attività a rischio «alto», il cui utilizzo – pur consentito – viene sottoposto a specifici requisiti, con la previsione di particolari obblighi per gli operatori di tali sistemi[19]; c)

«gli algoritmi e l'IA sono una possibilità rivoluzionaria di innovazione e miglioramento, ma ad alcune condizioni. I sistemi, gli strumenti e la loro applicazione pratica devono essere conformi ai valori giudiziari, come l'indipendenza e l'imparzialità, l'uguaglianza, la trasparenza e la responsabilità; devono garantire il rispetto dei diritti umani e la protezione di tutti i membri della società dal rischio di discriminazione e di uso improprio dei dati personali; deve rispondere agli imperativi etici e legali e ai principi guida fondamentali», precisando che «i cambiamenti nel campo della cyber-giustizia devono essere guidati dalle corti e non dalla tecnologia; ogni sistema informativo giudiziario deve essere implementato tenendo conto dei valori giudiziari fondamentali; noi, giudici e altri attori della giustizia, dobbiamo imparare a contribuire allo sviluppo di questi strumenti e sistemi e a monitorare e valutare la loro qualità e la conformità alle risorse umane».

[19] Cfr. considerando n. 96 all'AI Act, ove si afferma che i *deployer* di sistemi di IA ad alto rischio (che sono organismi di diritto pubblico o gli operatori privati che forniscono servizi pubblici e gli operatori che impiegano taluni sistemi di IA ad alto rischio elencati nell'allegato III del regolamento) dovrebbero svolgere una valutazione d'impatto sui diritti fondamentali prima di metterli in uso.

V. anche il considerando n. 159, ove si afferma che «ciascuna autorità di vigilanza del mercato per i sistemi di IA ad alto rischio nel settore della biometria elencati in un allegato del presente regolamento nella misura in cui tali sistemi siano utilizzati a fini di contrasto, migrazione, asilo e gestione del controllo delle frontiere, o per l'amministrazione della giustizia e dei processi democratici, dovrebbe disporre di poteri

pratiche a rischio basso o minimo[20].

Il settore della giustizia viene classificato come sistema ad alto rischio (essendo indicato nell'allegato III del regolamento, al punto 8, lett. a), in ragione del significativo impatto dallo stesso spiegato nella salvaguardia dei principi fondamentali della democrazia e dello Stato di diritto, nonché per la sua incidenza sulle libertà individuali e sul diritto al giusto processo e, correlativamente, al diritto a una tutela giurisdizionale effettiva dinanzi a un giudice imparziale.

Tale classificazione, si precisa, è limitata a quei sistemi di IA destinati ad essere utilizzati dal magistrato nello svolgimento dell'attività di sua competenza, come la ricerca giurisprudenziale e normativa, l'interpretazione dei fatti e delle disposizioni giuridiche e nell'operazione di sussunzione del caso concreto entro l'ambito applicativo della norma generale ed astratta. Inoltre, nella medesima classificazione dovrebbero rientrare altresì i sistemi di intelligenza artificiale utilizzati dalle c.d. ADR, quando tali procedimenti di risoluzione alternativa delle controversie sono destinati a produrre effetti giuridici vincolanti tra le parti che hanno adito l'organismo[21].

Tuttavia, il Regolamento si premura di precisare che «il processo decisionale finale deve rimanere un'attività a guida umana» e, di conseguenza, se da un lato è auspicabile che l'utilizzo delle nuove tecnologie fornisca sostegno al magistrato nell'espletamento dei suoi compiti, d'altra parte si nega la possibilità che il giudice venga sostituito dalla macchina.

---

di indagine e correttivi efficaci, tra cui almeno il potere di ottenere l'accesso a tutti i dati personali trattati e a tutte le informazioni necessarie per lo svolgimento dei suoi compiti». L'art. 74, co. 8 dell'AI Act prevede che tali autorità di vigilanza per i sistemi di IA ad alto rischio vadano individuate nelle «autorità di controllo competenti per la protezione dei dati a norma del regolamento (UE) 2016/679 o della direttiva (UE) 2016/680 o qualsiasi altra autorità designata a norma delle stesse condizioni di cui agli articoli da 41 a 44 della direttiva (UE) 2016/680».

Cfr. F. Barracca, *L'intelligenza artificiale generativa, cit,* che osserva che, alla luce del nuovo AI Act, «prima di immettere un sistema di IA ad alto rischio sul mercato dell'UE - o prima di farlo entrare in servizio - i fornitori dovranno sottoporlo a una valutazione della conformità. Dovranno, quindi, dimostrare che il loro sistema è conforme ai requisiti obbligatori per un'IA affidabile (ad esempio: qualità dei dati, documentazione e tracciabilità, trasparenza, sorveglianza umana, accuratezza, cybersicurezza e robustezza)».

[20] Sul punto v. F. Barracca, *L'intelligenza artificiale generativa, cit.*

[21] Il considerando n. 61 all'AI Act precisa che non vanno classificati come sistemi di IA ad «alto rischio» quelli destinati allo svolgimento di attività organizzative ed accessorie (quali l'anonimizzazione o la pseudonimizzazione di decisioni, documenti o dati giudiziari, la comunicazione tra il personale, i compiti amministrativi), che restano estranei all'effettiva amministrazione della giustizia.

In sintesi, dunque, si può rilevare che sull'utilizzo dell'intelligenza artificiale nel settore della giustizia gli organi dell'UE hanno adottato un atteggiamento piuttosto ambivalente, di fascinazione e diffidenza: da un lato ne hanno evidenziato le potenzialità, illustrandone ed incentivandone i possibili utilizzi, dall'altro l'hanno classificato come «ad alto rischio», mettendone in luce le possibili distorsioni e i conseguenti rischi per i principi fondamentali dell'ordinamento democratico, circondandolo di limiti e controlli.

Il Governo italiano, nel predisporre il disegno di legge[22] che, se approvato, regolerà l'uso dell'intelligenza artificiale a livello nazionale, segue le medesime linee guida, ma adotta un approccio ancor più cauto e prudente.

L'art. 14 del ddl, nel dettare le disposizioni relative al settore giustizia, mira a tracciare un confine netto tra l'utilizzo consentito, se non addirittura incoraggiato, dell'IA con funzione di supporto organizzativo e, quindi, con la finalità di ausilio per assecondare e semplificare il lavoro giudiziario, e quello viceversa vietato, nell'ambito, strettamente riservato al magistrato, dell'interpretazione della legge, della valutazione dei fatti e delle prove, ivi compresi i processi decisionali, tra cui l'adozione delle sentenze.

Siffatta soluzione, nella parte in cui pone un espresso divieto all'utilizzo della nuova tecnologia per le attività che costituiscono diretta espressione dell'attività di *jus dicere*, va indubbiamente oltre quanto richiesto dal Regolamento Europeo, che si limita ad imporre il rispetto del c.d. principio di salvaguardia umana e, dunque, che venga sempre assicurato un controllo finale del magistrato sulle valutazioni e sulle decisioni assunte dalla macchina.

Tali previsioni, se dovessero essere confermate (perlomeno nei loro tratti essenziali) all'esito del confronto parlamentare, escluderebbero l'utilizzo dell'intelligenza artificiale nell'attività interpretativa e valutativa – inderogabilmente affidata al magistrato – nonché nell'adozione del provvedimento finale.

Tutto ciò pone una serie di ulteriori interrogativi in ordine alla sorte degli atti processuali (ivi compresa la sentenza) adottati in violazione di tale divieto. In particolar modo, v'è da chiedersi se l'utilizzo dell'intelligenza artificiale per attività non consentite sia suscettibile o meno di tradursi in forme di invalidità degli atti processuali e del provvedimento decisorio, ovvero se sia destinata a rilevare solo sul piano (limitato) della responsabilità del singolo magistrato, resosi autore della violazione.

---

[22] Il disegno di legge n. 1146 AS, recante «Disposizioni e delega al Governo in materia di intelligenza artificiale», è stato varato dal Consiglio dei ministri il 23 aprile 2024. Il 17 settembre 2025, mentre il presente contributo era in corso di pubblicazione, il Senato ha approvato in via definitiva il citato ddl. La legge n. 132 del 23 settembre 2025 è stata poi pubblicata in GU serie generale n. 223 del 25 settembre 2025 ed è entrata in vigore il 10 ottobre 2025.

4. *Prospettive* de iure *condendo. La tesi contraria all'invalidità degli atti processuali redatti mediante un uso non consentito dell'intelligenza artificiale*

L'AI Act è entrato in vigore il 1° agosto 2024 ma il Regolamento UE, con riferimento al settore giustizia, non pone alcun esplicito divieto all'utilizzo dell'intelligenza artificiale per singole attività, limitandosi a richiedere – abbastanza genericamente – che il processo decisionale resti «a guida umana».

La disciplina nazionale sull'intelligenza artificiale è ancora ben lontana dall'entrare in vigore, dovendo ancora passare al vaglio delle Camere per l'adozione. Tuttavia, come si è dinanzi evidenziato, l'art. 14 del disegno di legge, nella sua attuale (e interinale) formulazione, vieta espressamente l'utilizzo di pratiche di IA per la valutazione dei fatti e delle prove, nonché per l'adozione della decisione finale, ma non prevede espressamente alcuna sanzione in caso di inosservanza.

Dunque, al momento, non risulta vigente alcuna disposizione volta a escludere l'utilizzo della nuova tecnologia per il compimento di specifiche attività processuali.

Pertanto, in attesa che il Parlamento si esprima definitivamente sull'impiego dei sistemi di intelligenza artificiale all'interno del processo, non resta che adottare una prospettiva *de iure condendo*, al fine di verificare quali sarebbero le soluzioni più auspicabili. Non sorgono particolari dubbi laddove la decisione adottata con un utilizzo non consentito dell'intelligenza artificiale si presenti errata e – dunque – censurabile dal punto di vista logico e giuridico.

In tale evenienza, già la normativa attuale consentirebbe (è evidente) di far valere i vizi della pronuncia con gli ordinari mezzi di impugnazione e, eventualmente, si potrà profilare anche la responsabilità civile e/o disciplinare del magistrato che – con dolo o colpa grave – ha adottato la sentenza illegittima. L'elemento soggettivo della responsabilità del giudice, in questo caso, andrebbe individuato nell'omessa verifica sull'operato dell'intelligenza artificiale: a tal proposito non assumerebbe rilevanza alcuna la circostanza che il vizio della decisione sia derivato da un uso consentito o non consentito dell'IA, poiché il giudice, quando sottoscrive la sentenza, ne acquisisce la paternità e la conseguente responsabilità.

Laddove, invece, la decisione assunta con un utilizzo non consentito dell'IA sia corretta sotto il profilo formale e sostanziale, v'è da chiedersi se la pronuncia possa essere censurata (e, dunque, ritenuta invalida) per il sol fatto che essa si presenta quale «prodotto» di un'attività creativa artificiale e non umana.

La questione, a prima vista, potrebbe apparire priva di rilevanza pratica: discutere sulla possibilità di impugnare una pronuncia che presenta, quale unico vizio, quello di essere il risultato di un uso non consentito dell'intelligenza artificiale sarebbe utile solo qualora fosse possibile accertare con certezza l'effettiva sussistenza di tale utilizzo illecito.

Questa prima criticità potrebbe portare a ritenere che l'uso non consentito dell'IA, laddove non si traduca in un vizio ulteriore della sentenza, sia destinato a rimanere un divieto privo di sanzione.

Tuttavia, bisogna dare atto che esistono taluni strumenti che, analizzando i testi e valutando elementi come la coerenza semantica e la logica troppo lineare, riescono ad individuare gli schemi tipici dell'intelligenza artificiale. Si tratta – comunque – di sistemi di rilevamento probabilistici e non infallibili, che difficilmente si presterebbero a costituire una solida premessa per dichiarare invalido l'atto processuale.

D'altronde, nel nostro ordinamento gli artt. 121 e 156 del codice di rito recepiscono i principi di libertà delle forme e del raggiungimento dello scopo.

Alla luce del primo, gli atti processuali non devono necessariamente rivestire una forma prestabilita, a meno che questa non sia espressamente richiesta dalla legge, essendo all'uopo richiesto soltanto che essi siano idonei a raggiungere il loro scopo. Tale principio potrebbe essere valorizzato per pervenire alla conclusione che la tecnologia ben potrebbe supportare il magistrato nella redazione delle decisioni finali, a condizione che l'atto che ne risulta sia conforme alla legge ed ottemperi ai requisiti minimi di validità.

Allo stesso modo, il principio del raggiungimento dello scopo di cui all'art. 156 c.p.c. consente di considerare valido l'utilizzo di forme o modalità diverse da quelle prescritte dal legislatore, purché queste ultime non finiscano per compromettere l'effettivo conseguimento delle finalità cui l'atto era proteso. Siffatta previsione potrebbe portare a ritenere che anche un atto generato – in tutto o in parte – con l'intelligenza artificiale potrebbe essere ritenuto valido, a condizione che risulti comunque garantito il raggiungimento dello scopo cui l'atto era diretto.

Si consideri, inoltre, che il nostro ordinamento già consente a soggetti estranei alla magistratura di assistere il magistrato nell'esercizio di funzioni puramente giurisdizionali. In particolare, si fa riferimento alla figura recentemente introdotta dei «funzionari addetti all'Ufficio per il Processo», i quali, tra le loro molteplici mansioni, si occupano anche della redazione di bozze di provvedimenti. Tali bozze, predisposte dagli addetti, devono essere successivamente verificate e, se necessario, modificate dai magistrati assegnatari, che potranno sottoscriverle facendole proprie.

In sostanza, i funzionari svolgono un lavoro preparatorio, che comprende la ricerca giurisprudenziale e lo studio del fascicolo, nonché la stesura preliminare della sentenza, che sarà poi oggetto di controllo da parte del giudice. Dunque, se i funzionari addetti all'Ufficio per il Processo possono svolgere tali attività, è difficile comprendere perché l›intelligenza artificiale non possa assumere un ruolo analogo: anche nel primo caso, infatti, la decisione – sebbene di competenza «umana» – non sarebbe frutto dell'elaborazione di «quella» specifica figura uma-

na individuata dall'ordinamento, ossia il giudice naturale precostituito per legge, di cui all'art. 25 della Costituzione.

Se il controllo successivo del giudice è in grado di convalidare la bozza di provvedimento redatta da un funzionario, non si vede perché non ci si possa avvalere del medesimo meccanismo per approvare una sentenza predisposta dall'intelligenza artificiale.

Adottare un approccio contrario comporterebbe un atteggiamento aprioristicamente diffidente nei confronti delle decisioni generate dalla macchina, un atteggiamento che, a ben vedere, non sembra possa trovare giustificazione nella realtà empirica.

In sostanza, ragionando in questi termini, le possibili limitazioni all'uso dell'IA sembrerebbero più di natura etica che pratica, poiché l'efficacia del controllo giudiziale rimarrebbe invariata indipendentemente dall'origine della bozza di sentenza.

Pertanto, una prima conclusione potrebbe essere quella di ritenere che l'uso dell'IA – se non compromette l'integrità e la finalità dell'atto processuale e non genera vizi ulteriori, tali da rendere la pronuncia altrimenti censurabile – non possa impingere nell'invalidità dell'atto processuale e del provvedimento finale[23].

5. *La tesi favorevole alla configurabilità di una nuova causa di invalidità dell'atto processuale. Prospettive di classificazione*

Come dianzi affermato, nell'attuale formulazione dell'art. 14 d.d.l. AS 1662, il divieto di utilizzo dell'intelligenza artificiale per l'attività di valutazione dei fatti e delle prove e per la redazione del provvedimento finale risulta privo di specifiche sanzioni. Pertanto, se il silenzio normativo dovesse permanere, sarebbe preferibile ritenere che un uso illegittimo della nuova tecnologia non possa automaticamente condurre alla nullità dell'atto.

Nondimeno, essendo il testo ancora in fase di approvazione e suscettibile di essere emendato nel corso dell'iter parlamentare, è utile interrogarsi sull'opportunità di introdurre, quale sanzione specifica per l'uso dell'IA in violazione del divieto normativo, un'autonoma ipotesi di invalidità dell'atto processuale.

Una prima soluzione – la più «estrema» – potrebbe essere quella di ritenere che il provvedimento redatto dall'intelligenza artificiale non sia in alcun modo

[23] Così F. De Stefano, *Intelligenza artificiale*, cit, per il quale «nulla pare disciplinare, a pena di invalidità di qualsiasi tipo, le modalità con cui si redigono gli atti giudiziari, né, tanto meno, i procedimenti in base ai quali si perviene alla loro definitiva stesura; sicché ad un sistema di intelligenza artificiale, allo stato, ben potrebbe devolversi la redazione di quelli, alla sola condizione che siano fatti propri dall'agente umano».

riferibile alla persona del giudice, con la conseguenza che andrebbe considerato radicalmente inesistente.

La categoria dell'inesistenza, in ambito giuridico, si riferisce ai vizi che, per la loro estrema gravità e abnormità, non consentono di ricondurre l'atto entro il paradigma normativo di riferimento, rendendolo completamente avulso dal contesto ordinamentale. Di conseguenza, un vizio che comporta l'inesistenza è sempre e radicalmente insanabile.

Nel processo civile, l'unico vizio della sentenza riconducibile alla categoria dell'inesistenza è il difetto della sottoscrizione del magistrato (requisito essenziale per attribuire l'atto alla paternità del giudicante), ai sensi dell'art. 161, co. 2, cod. proc. civ..

Nondimeno, si potrebbe ipotizzare che nei casi in cui il provvedimento finale si limita a recepire la decisione assunta da un sistema di intelligenza artificiale, il *vulnus* recato ai principi costituzionali di indipendenza e autonomia del giudice ed ai canoni del giusto processo sia tale da configurare un vizio della sentenza equiparabile (per gravità) alla mancata sottoscrizione del giudice.

Una soluzione meno drastica potrebbe essere quella di ritenere che l'uso dell'intelligenza artificiale nella valutazione dei fatti e delle prove e/o nella redazione del provvedimento finale sia una causa di nullità della sentenza, che tuttavia risulterebbe sanata in assenza di tempestiva impugnazione con mezzi ordinari in aderenza al generale principio di conversione dei motivi di nullità in motivi di impugnazione ex art. 161, co. 1, cod. proc. civ.

Tali proposte si rivelano indubbiamente suggestive, in quanto potrebbero porre efficacemente rimedio alle principali problematiche legate all'uso dell'intelligenza artificiale nel processo civile.

I rischi insiti in un diffuso riscorso agli algoritmi per l'espletamento di attività strettamente giurisdizionali sono facilmente intuibili, poiché potrebbero risultare compromesse la stessa trasparenza del sistema di tutela dei diritti e la fiducia che i cittadini ripongono nello stesso. Le parti, infatti, non sarebbero in condizione di individuare correttamente l'origine della decisione e il grado di intervento umano nella sua redazione. Inoltre, v'è chi ha evidenziato come l'utilizzo dell'intelligenza artificiale porterebbe, verosimilmente, ad una «una standardizzazione delle decisioni giudiziarie», che impedirebbe all'ordinamento di progredire adattandosi ai mutamenti del contesto sociale[24].

---

[24] Così G. Ariolli, *Nomofiliachia, giustizia predittiva e intelligenza artificiale*, in *Giustizia Insieme*, 3 novembre 2023, Nomofilachia, giustizia predittiva e intelligenza artificiale - www.giustiziainsieme.it. Sul punto v. anche M. Civinini, *Nuove tecnologie*, cit., 16. L'Autrice evidenzia che uno dei possibili rischi insiti nell'uso dei mezzi di IA nel supporto del lavoro giudiziario «può essere descritto come il "rischio del giudice pigro" cioè del giudice che tenderebbe ad accontentarsi della soluzione proposta dall'IA

Tuttavia, come dianzi evidenziato, uno dei principali ostacoli all'accoglimento di siffatta soluzione consiste nelle evidenti difficoltà che si riscontrerebbero ove si volesse stabilire con certezza se un determinato atto è stato redatto da un sistema di intelligenza artificiale generativa. D'altronde, va osservato che una sentenza redatta dall'IA (o fondata su valutazioni dei fatti e delle prove operate sulla base di un algoritmo) ben potrebbe essere sostanzialmente giusta. In tali casi, riscontrare nella pronuncia un vizio suscettibile di comportarne la caducazione rischierebbe di essere disfunzionale rispetto ai principi di economia processuale e di ragionevole durata dei giudizi. D'altronde, in un ordinamento giuridico che tende a far prevalere la sostanza sulla forma, difficilmente potrebbe trovare giustificazione la cancellazione di una decisione corretta per la sola circostanza (peraltro difficilmente dimostrabile in concreto) che il processo decisionale sia stato illegittimamente demandato a un sistema di intelligenza artificiale.

Inoltre, va ribadito che con la sottoscrizione della sentenza il giudice assume la paternità della decisione e le correlate responsabilità. In tal modo, dunque, si può comunque assicurare il controllo umano, imprescindibile per assicurare un utilizzo etico e consapevole dell'IA nel settore della giustizia. In altri termini, la sottoscrizione della sentenza potrebbe essere ritenuta un elemento di garanzia adeguato, assicurando – in una certa misura – una supervisione umana sull'operato della macchina.

6. *Sulla responsabilità civile e disciplinare del magistrato*

Considerato che introdurre una nuova ed autonoma causa di invalidità per le sentenze redatte con il supporto dell'intelligenza artificiale in violazione delle normative non sembra una soluzione opportuna, appare rilevante esaminare le ripercussioni che un utilizzo illecito dell'IA potrebbe avere sulla responsabilità del magistrato, sia sotto il profilo civile sia sotto quello disciplinare.

Con riferimento alla responsabilità disciplinare, il d.lgs. 23 febbraio 2006, n. 109 tipizza gli illeciti funzionali ed extrafunzionali dei magistrati.

---

senza approfondire, inaridendo così l'evoluzione della giurisprudenza e non prestando attenzione ai dettagli del caso concreto», concludendo – tuttavia – che la descritta problematica attiene più alla formazione ed alla valutazione della professionalità del singolo magistrato che allo sviluppo tecnologico.

Cfr. anche D. Dalfino, *Giurisprudenza "creativa" e prevedibilità del "diritto giurisprudenziale"*, in *Giusto proc. civ.,* 2017, 1030; F. De Stefano, *Intelligenza artificiale*, cit., secondo cui «l'attività decisionale in senso stretto, cioè l'opzione tra due o più soluzioni di questioni di ricostruzione in fatto e di questioni in diritto, nei singoli passaggi sopra ricordati, non può mai essere devoluta ad un'automazione, ma essere sempre riservata all'agente umano».

In relazione al tema in esame, l'art. 2 del summenzionato decreto contempla diverse categorie di illecito che potrebbero venire in considerazione ove il magistrato, nell'adoperare in maniera poco avveduta la nuova tecnologia, pronunci una sentenza errata sotto il profilo formale e sostanziale.

Nello specifico, potrebbe configurarsi la responsabilità disciplinare del giudice qualora quest'ultimo, nell'utilizzare l'intelligenza artificiale, adotti una decisione caratterizzata da grave violazione di legge o da un evidente travisamento dei fatti, dovuti a negligenza inescusabile. Ciò risulterebbe altresì applicabile nel caso in cui la sentenza generata dall'IA sia insufficiente nella motivazione e il giudice ometta di integrarne adeguatamente il contenuto. In tali casi – è evidente – l'omissione della dovuta attività di controllo e supervisione può senz'altro integrare la "negligenza inescusabile" richiesta dalla norma.

Anche in tal caso, tuttavia, i maggiori dubbi attengono alla possibilità di configurare una responsabilità disciplinare del magistrato qualora l'illecito consista esclusivamente nell'uso improprio dell'intelligenza artificiale, indipendentemente dall'eventuale ingiustizia della decisione che ne è derivata.

In questo caso, probabilmente, potrebbe comunque ritenersi il magistrato responsabile alla luce della previsione di cui alla lett. o) dell'art. 2, d.lgs. n. 109/2006, che vieta espressamente «l'indebito affidamento ad altri di attività rientranti nei propri compiti».

Inoltre, è innegabile che l'uso dell'intelligenza artificiale per lo svolgimento dell'attività istruttoria e decisoria potrebbe generare non pochi inconvenienti in relazione alla tutela della privacy delle parti processuali. In effetti, l'inserimento di informazioni relative alla controversia nei sistemi di intelligenza artificiale ben potrebbe integrare l'illecito di cui all'art. 2, lett. u), che sanziona «la divulgazione, anche dipendente da negligenza, di atti del procedimento coperti dal segreto o di cui sia previsto il divieto di pubblicazione, nonché la violazione del dovere di riservatezza sugli affari in corso di trattazione, o sugli affari definiti, quando è idonea a ledere indebitamente diritti altrui». D'altronde, le esigenze di riservatezza non sempre possono essere adeguatamente tutelate dalle procedure di anonimizzazione, specialmente considerando che l'utilizzo dell'IA nella valutazione dei fatti o delle prove rischierebbe di rendere pubblici dati personalissimi, o di violare segreti professionali o industriali.

Dunque, una responsabilità disciplinare del magistrato che ha utilizzato l'intelligenza artificiale in violazione del divieto normativo potrebbe ritenersi configurabile al di là della «giustizia» del provvedimento che ne costituisce il risultato finale.

Tuttavia, anche in questo caso, restano impregiudicati i dubbi attinenti alla difficoltà di provare che vi sia effettivamente stato tale uso illecito.

Quanto alla responsabilità civile, similmente, non vi sono ostacoli a ritenere che l'elemento soggettivo della colpa grave richiesto dalla legge n. 18/2015 ben

possa essere integrato quando l'utilizzo non accorto della nuova tecnologia si traduce in un errore di giudizio o in un travisamento dei fatti o delle prove.

Non sembra invece configurabile alcuna responsabilità civile in capo al magistrato che, facendo un uso non consentito dell'intelligenza artificiale, adotti una decisione corretta ed esente da vizi di altra natura. In tale evenienza, infatti, sarebbe finanche impossibile individuare un danno suscettibile di essere risarcito e la responsabilità civile – come noto – assolve ad una funzione ripristinatoria e non punitiva.

7. *Gli scritti difensivi degli avvocati*

Da ultimo, occorre domandarsi se quanto affermato in relazione alle conseguenze dell'uso dell'intelligenza artificiale nella redazione degli atti del processo civile da parte del giudice sia estensibile anche alla redazione degli atti di parte che promanano dal difensore.

Sul punto, giova precisare che l'art. 14 d.d.l. nulla dispone in relazione all'uso della nuova tecnologia negli scritti difensivi e, di conseguenza, allo stato non sembra che si voglia predisporre alcuna limitazione all'utilizzo della nuova tecnologia nella redazione degli scritti defensionali.

Anche per gli scritti degli avvocati, tuttavia, potrebbe essere opportuno valutare l'introduzione di una norma che limiti l'uso dell'intelligenza artificiale, in modo analogo a quanto proposto dal disegno di legge in relazione agli atti processuali redatti dal giudice.

Infatti, il problema di un uso improprio dell'intelligenza artificiale ad opera degli avvocati è già emerso negli Stati Uniti, aprendo questioni in ordine all'attendibilità delle informazioni fornite dai sistemi di intelligenza artificiale generativa.

Ha avuto grande risonanza l'ordinanza dalla Corte del distretto meridionale di New York del 22 giugno 2023, con la quale i giudici d'oltreoceano hanno comminato una sanzione pecuniaria a due avvocati (e alla loro Law firm) che, in una causa civile di risarcimento del danno, avevano fatto diffusamente riferimento a precedenti giurisprudenziali rivelatisi inesistenti, perché ideati (*rectius:* inventati) dal *chatbot* «Chat GPT», un sistema di intelligenza artificiale progettato per interagire direttamente con l'utente, simulando una conversazione[25].

Dalla motivazione della pronuncia, invero, emerge come la Corte di New York non abbia inteso sanzionare, in sé e per sé, l'utilizzo dell'intelligenza artificiale generativa per la predisposizione dell'atto processuale, quanto la mancanza

[25] Sul punto cfr. F. De Stefano, *Intelligenza artificiale,* cit.

di un'attenta attività di controllo e verifica sulla veridicità delle informazioni fornite dal *chatbot*, poi refluite nello scritto difensivo.

In altri termini, per i giudici statunitensi nel sistema non sarebbe rinvenibile alcun divieto di utilizzare l'intelligenza artificiale per la redazione degli atti del processo, fermo restando l'obbligo – gravante sui difensori che si avvalgono di strumenti tecnologici per la predisposizione degli scritti defensionali – di controllare con accuratezza la correttezza delle informazioni, configurandosi una loro responsabilità solo in caso di mancata supervisione dell'operato della macchina.

Con riferimento al medesimo tema, appare di sicuro rilievo – sotto il profilo strettamente processuale – la pronuncia emessa nel 2024 dalla Court of Appeal del Second Circuit nel caso Park v. Kim.[26]

La vicenda in esame ha ad oggetto l'appello avverso una pronuncia di inammissibilità della domanda *(dismissal)* ai sensi della Rule 37 del FRCP[27], per la reiterata violazione ad opera dell'attore degli *orders of discovery* impartiti dal giudice.

In particolare, il difensore dell'attore aveva sistematicamente omesso di ottemperare alla richiesta del giudice di produrre i precedenti giurisprudenziali invocati a sostegno della domanda, i quali si erano successivamente rivelati essere inesistenti. L'avvocato si era limitato a dichiarare che tali riferimenti giurisprudenziali erano stati forniti dal *chatbot* ChatGPT, del cui ausilio si era avvalso per la redazione dell'atto processuale.

La Corte, nel confermare la declaratoria di inammissibilità della domanda pronunciata dal giudice di primo grado, ha sanzionato l'avvocato per la mancata osservanza dei doveri professionali di controllo e certificazione sul contenuto degli scritti difensivi, deferendolo al competente ordine professionale ed imponendogli di comunicare al proprio assistito il testo integrale della decisione[28].

---

[26] V. Corte d'Appello federale U.S. per il secondo circuito, ord. 30 gennaio 2024, n. 22-2057, Park c. Kim, in Foro It, 10, 4, 2024, 496, con nota di A. Dondi, V. Ansanelli, P. Comoglio, *Responsabilità dell'avvocato nell'utilizzazione di Chat GPT. Aspetti di etica della difesa nel contesto statunitense.*

[27] Cfr, A. Dondi, V. Ansanelli, P. Comoglio, *Responsabilità dell'avvocato,* cit, 496, ove gli Autori, in una prospettiva comparatistica, osservano che è del tutto estranea alla nostra cultura giuridica la possibilità di sanzionare con l'inammissibilità della domanda i comportamenti non collaborativi dell'avvocato, mentre «negli Stati Uniti risulta del tutto acquisita la consapevolezza che tali comportamenti – e di qui la previsione delle relative sanzioni – hanno un'incidenza diretta sul livello complessivo di efficienza del modello processuale».

[28] Sul punto v. A. Dondi, V. Ansanelli, P. Comoglio, *Responsabilità dell'avvocato,* cit., 496. Gli Autori evidenziano che, nel caso di specie, la Corte statunitense aveva ritenuto applicabile la *Rule 11, section b)* delle *Federal Rules of Civil Procedure,* ai sensi della quale l'avvocato, sottoscrivendo l'atto processuale, garantisce

I casi sottoposti ai giudici statunitensi, indubbiamente, mettono in guardia dai rischi suscettibili di derivare da un utilizzo improprio e poco oculato delle nuove tecnologie per lo svolgimento delle attività demandate ai difensori, specie ove si consideri la fondamentale importanza della tutela giurisdizionale dei diritti che rischierebbe di risultare – irrimediabilmente – pregiudicata ove la difesa tecnica venisse affidata ad un sistema di intelligenza artificiale che si rivela poi essere del tutto inaffidabile.

Effettuata tale premessa di carattere comparatistico, appare opportuno interrogarsi sulle soluzioni che il nostro ordinamento potrebbe offrire per affrontare la delineata problematica, tenendo conto sia delle eventuali implicazioni sul piano della validità degli atti processuali, sia delle conseguenze sul piano deontologico-disciplinare e della responsabilità civile in capo all'avvocato.

Nell'attuale quadro normativo, le ipotesi in cui un utilizzo improprio dell'intelligenza artificiale potrebbe configurare una situazione di invalidità risultano, invero, residuali[29].

Tale eventualità – con riferimento all'atto introduttivo – sembrerebbe potersi concretizzare solo in casi limite, ovverosia quando l'atto redatto con il supporto della nuova tecnologia presenti un'imperizia tale da rendere assolutamente incerto il *petitum* o la *causa petendi,* come previsto dall'art. 164 cod. proc. civ.

---

che le difese in esso contenute siano fondate su solide basi giuridiche e non su «*frivolous argument*» e che la *subsection c)* della medesima norma consente al giudice di sanzionare la mancata osservanza di tali doveri di certificazione e controllo, affidandogli «il compito di scegliere, fra le sanzioni tipizzate, quella più appropriata ad evitare la riproposizione di comportamenti dello stesso genere e al limite, come esplicitamente prevede la norma, di adottare a tal fine *"any sanction may consider just"*».

Analoghe misure – osservano gli Autori – non potrebbero essere adottate nel nostro ordinamento, dove manca un «apparato sanzionatorio effettivo» nei confronti dell'avvocato che violi il suo dovere di correttezza processuale e «l'unico soggetto nei confronti del quale la conseguenza negativa opera è la parte-cliente» sulla quale incombe il risarcimento dei danni per lite temeraria ex art. 96 c.p.c. e sulla quale incide la condanna alle spese di lite.

[29] V. F. De Stefano, *Intelligenza artificiale,* cit., secondo cui «l'attività dell'avvocato civilista potrebbe ambire a raffinarsi fino al ruolo di colui che impartisce le coordinate generali per l'impostazione dell'atto difensivo in relazione ai tre elementi costitutivi della domanda (personae, causa petendi e petitum), ma senza mai rinunciare a quello di finale responsabile quale approfondito e consapevole ricognitore e supervisore del prodotto del sistema di intelligenza artificiale, prima di appropriarsene», purché tale sistema consenta di preservare l'indispensabile consequenzialità «tra ricostruzione del fatto, con indicazione dei relativi elementi istruttori (costituendi o precostituiti), ed elaborazione delle tesi in diritto da applicare», nonché tra «premesse, sviluppi argomentativi e conclusioni». Nello stesso senso, F. Barracca, *L'intelligenza artificiale generativa,* cit.

Inoltre, con riferimento all'opportunità di introdurre una fattispecie di invalidità *ad hoc* per sanzionare l'utilizzo improprio dell'IA ad opera del difensore, va evidenziato che l'attività difensiva da quest'ultimo esercitata non solleva le medesime criticità poste dall'uso di algoritmi nell'ambito della giurisdizione.

Per l'attività defensionale non verrebbero in rilievo i principi – di rilevanza costituzionale – dell'autonomia e indipendenza della magistratura e del giudice naturale precostituito per legge, ma andrebbe nondimeno salvaguardata l'esigenza di preservare adeguati standard di professionalità e perizia nella redazione degli scritti difensivi, onde tutelare effettività e qualità della difesa.

Conseguentemente, se l'atto del difensore risultasse redatto «a regola d'arte» sarebbe ultroneo prevedere una qualunque sanzione (processuale, civile o disciplinare) per l'utilizzo dell'intelligenza artificiale.

Tuttavia, anche in tali casi potrebbero emergere profili di responsabilità disciplinare dell'avvocato per violazione dell'obbligo di segretezza e riservatezza di cui all'art. 13 CDF, qualora i sistemi di IA utilizzati non consentano un'adeguata tutela della privacy del cliente.

Nel caso in cui l'utilizzo poco accorto dell'intelligenza artificiale dovesse pregiudicare la strategia difensiva e la tutela dei diritti del cliente, l'utilizzo poco accorto dei modelli di IA potrebbe altresì integrare una violazione del dovere di diligenza e competenza di cui all'art. 12 e 14 CDF e del dovere di lealtà e probità *ex* art. 88 c.p.c., nonché esporre il difensore a responsabilità civile *ex* art. 1218 cod. civ. per i danni causati[30].

8. *Conclusioni*

Da tutte le considerazioni suesposte emerge chiaramente come, in relazione all'utilizzo dell'IA nel settore giustizia, coesistono accese aspettative e grandi timori[31].

---

[30] Sul punto cfr. A. Dondi, V. Ansanelli, P. Comoglio, *Responsabilità dell'avvocato,* cit, 496. Gli Autori auspicano una maggiore «coinvolgimento dell'avvocato nell'arco di responsabilità concernenti le modalità della difesa» e «la necessità di non richiedere solamente una adeguata e chiara compilazione degli atti, ma di imporre una fattiva collaborazione nelle allegazioni e nelle argomentazioni poste a fondamento della posizione delle parti; e questo anche inevitabilmente attraverso un uso appropriato della tecnologia», rilevando che attualmente, nel nostro ordinamento, manca una disciplina sull'utilizzo delle nuove tecnologie nella redazione degli atti processuali dell'avvocato e che il rimedio esistente – l'art. 88 c.p.c. (che consente al giudice di riferire all'autorità disciplinare i comportamenti scorretti tenuti dall'avvocato nel corso del giudizio) – si presenta inadeguato.

Su doveri e responsabilità dell'avvocato, cfr. M. Bina, *La felicità dell'avvocato*, Torino, 2024

[31] La controversa tematica dell'utilizzazione dell'intelligenza artificiale nel settore

È dunque necessario continuare sull'intrapresa strada dello studio e della riflessione, tanto in ordine alle potenzialità, quanto dei pericoli e dei limiti – anche etici – insiti nell'utilizzo dello strumento dell'IA.

Solo così si riuscirà a governare il fenomeno dell'intelligenza artificiale rendendo tale tecnologia davvero al servizio della giustizia e, per essa, della società, scongiurando il rischio che gli algoritmi posti alla sua base possano prendere il sopravvento, attuando pericolosamente quella che è stata chiamata una «algocrazia» o, addirittura, che si realizzi «quella ribellione delle macchine all'uomo» (si perdoni il linguaggio iperbolico) che Stanley Kubrick aveva preconizzato nel suo visionario film «*2001 Odissea nello spazio*»[32].

della giustizia, a dimostrazione della sua centralità, è stata oggetto di approfondimento e confronto nell'ambito del 66° Congresso dell'Associazione internazionale dei giudici, che si è svolto nel mese di ottobre 2024 a Cape Town. Tra le relazioni tenute nel corso del *meeting,* si segnalano quelle di C. Bernardo, *Intelligenza artificiale, utilità e insidie nell'uso giurisdizionale,* https://lamagistratura.it/informatica-e-nuove-tecnologie/intelligenza-artificiale-utilita-e-insidie-nelluso-giurisdizionale/; M. M. McKeown, *Artificial Intelligence & Impact on Social/Labor Law* https://lamagistratura.it/wp-content/uploads/2024/10/McKeown_IAJ-Presentation_AI_2024.pdf; M. L. Huff, *The effects of artificial intelligence on the judiciary, https://lamagistratura.it/wp-content/uploads/2024/10/Huff-Speech-The-Effects-of-Artificial-Intelligence-on-the-Judiciary.pdf*.

[32] Così C. Bernardo, *Intelligenza artificiale, utilità e insidie nell'uso giurisdizionale,* cit.

I possibili impieghi dell'intelligenza artificiale nel processo penale e la regolamentazione delle statistiche processuali penali

di **Thomas Di Candia**[*]

In estrema sintesi, gli obiettivi del contributo sono di tracciare i possibili impieghi dell'intelligenza artificiale nel procedimento penale, di analizzare concisamente la disciplina che li regolamenta (o vieta), così definendone i limiti tecnici e giuridici, nonché di esaminare l'attuale sistema di raccolta dei dati processuali penali e di riflettere sul possibile aggiornamento della relativa normativa.

Sotto quest'ultimo profilo, alla crescente attenzione per lo sviluppo e l'elaborazione di sistemi di intelligenza artificiale connessi al processo penale non si accompagna un altrettanto cruciale interesse per i dati giudiziari penali, tanto che in futuro potremmo avere a disposizione sistemi tecnologicamente molto avanzati che "sottoperformano" a causa della mancanza di un adeguato sistema di raccolta delle statistiche processuali penali.

[*] Assegnista di ricerca in Diritto processuale penale Università degli Studi dell'Insubria.

1. *Gli impieghi dell'intelligenza artificiale nella giustizia penale*

Il ricorso all'intelligenza artificiale fa ormai parte, consapevolmente o meno, della nostra quotidianità. Con l'etichetta di sistemi di IA si individua una classe eterogenea di strumenti automatizzati con livelli di autonomia variabili in grado di fornire un *output* sotto forma di previsioni, contenuti, raccomandazioni o decisioni sulla scorta degli *input* ricevuti[1].

Tale ampiezza di risultati rende gli strumenti che sfruttano l'IA particolarmente flessibili, permettendo loro di incidere su tutti gli ambiti dello sviluppo umano, tra cui l'amministrazione della giustizia e i settori connessi.

Un primo obiettivo di questo contributo è fornire una ampia panoramica degli utilizzi tecnicamente possibili (a oggi già disponibili oppure immaginabili nel breve-medio periodo) dell'IA nel campo processuale penale e in quelli concatenati.

Più nel dettaglio, nei paragrafi successivi si approfondiranno, oltre alle applicazioni nel campo strettamente procedimentale penale, anche gli impieghi in funzione di sicurezza preventiva, nella fase dell'esecuzione e penitenziaria, nell'organizzazione degli uffici giudiziari, nella modellazione della legislazione processuale penale e nella raccolta delle statistiche giudiziarie.

2. *Prima del procedimento: attività preventiva e polizia predittiva*

I primi impieghi logicamente possibili dell'intelligenza artificiale si hanno già precedentemente all'inizio del procedimento penale, essendo utilizzati dalle autorità di pubblica sicurezza per prevenire la commissione del reato (c.d. *predictive policing*).

Tali strumenti sfruttano la capacità prognostica dell'intelligenza artificiale al fine di valutare il rischio del verificarsi di condotte penalmente rilevanti.

Le macro-tipologie di sistemi di polizia predittiva esistenti sono due, quella degli strumenti che valutano il rischio con riferimento al luogo dove potrebbero verificarsi dei reati (*place-based systems*) e quella dei *software* che individuano il profilo del soggetto a rischio di commissione del reato o della potenziale vittima

[1] La definizione di sistemi di IA si trova nell'art. 3 del Regolamento UE 2024/1689 (c.d. *AI Act*), in cui si legge che «Ai fini del presente regolamento si applicano le definizioni seguenti: 1) 'sistema di IA': un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».

(*person-based systems*)[2]. Tale distinzione non è rilevante solo sotto il profilo tecnico, ma, in ragione del diverso impatto sulle libertà della persona, si riverbera anche in una diversa regolamentazione giuridica da parte dell'*AI Act* (v. *infra* par. 8).

3. *Durante il procedimento*

Una volta emersa la commissione di un fatto di reato e incardinato il procedimento penale, sono molteplici gli strumenti che sfruttano l'intelligenza artificiale impiegabili dai diversi attori processuali.

I sistemi interamente incentrati sull'IA, o che la sfruttano per migliorare le proprie tradizionali prestazioni, operano in modo parzialmente diverso a seconda della funzione con cui tale tecnologia è sfruttata.

In questo senso, al fine di accomunare strumenti diversi che presentano dinamiche di funzionamento assimilabili, è possibile distinguere tra i sistemi che ampliano il contesto informativo di chi li utilizza (limitandosi a fornire degli ulteriori elementi che permettono una valutazione complessiva più completa), quelli in grado di generare dei contributi e i *tool* capaci di valutare dei parametri al fine di suggerire oppure prendere delle decisioni.

Tale polivalenza fa sì che alcuni strumenti di IA presentino un carattere trasversale, trovando applicazione, con alcuni minimi accorgimenti, in fasi diverse del procedimento rispetto a istituti aventi caratteristiche simili.

Gli strumenti che adottano tale tecnologia possono essere suddivisi, a seconda della combinazione tra la funzione con cui l'intelligenza artificiale è impiegata (di ampliamento del contesto informativo, di generazione di contributi o di decisione) e il soggetto che la sfrutta, nelle categorie che seguono.

---

[2] Propongono una tale distinzione A.G. Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, in *New York University Press*, 2017, pp. 34-83; P. Severino, *Intelligenza artificiale e diritto penale*, in *Intelligenza artificiale. Il diritto, i diritti, l'etica*, a cura di U. Ruffolo, Giuffrè, Milano, 2020, pp. 536-542; L. Camaldo, *Intelligenza artificiale e investigazione penale predittiva*, in *Rivista italiana di diritto e procedura penale*, n. 1, 2024, pp. 233-250. In merito si vedano anche L. Algeri, *Intelligenza artificiale e polizia predittiva*, in *Diritto penale e processo*, n. 6, 2021, pp. 729-733; F. Basile, *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova*, in *Diritto penale e intelligenza artificiale. "Nuovi scenari"*, a cura di G. Balbi, F. De Simone, A. Esposito e S. Manacorda, Giappichelli, Torino, 2022, pp. 7-9; E. Pietrocarlo, *La* predictive policing *nel regolamento europeo sull'intelligenza artificiale*, in *La legislazione penale*, 26.09.2024, pp. 5-10.

3.1 *Sistemi utilizzati da parte di magistrati con funzione di ampliamento del contesto informativo*

In primo luogo, sono i soggetti pubblici a poter beneficiare dell'apporto dell'intelligenza artificiale nel corso del procedimento penale. I magistrati, infatti, possono accedere a dei sistemi incentrati sullo sfruttamento dell'IA volti ad ampliare il campo delle informazioni che hanno a disposizione e funzionali alla raccolta di elementi utili a effettuare una valutazione completa.

Tali tecnologie, a cui possono ricorrere sia i giudici sia i pubblici ministeri, sono dirette ad ampliare il contesto conoscitivo mediante una prognosi sul verificarsi di un evento incerto futuro oppure, all'opposto, a completare il panorama informativo mediante la ricostruzione di eventi passati o presenti[3].

3.1.1 *…mediante un'attività prognostica*

Quanto agli strumenti di tipo prognostico nella disponibilità del giudice, lo stesso può avvalersi di sistemi di intelligenza artificiale in grado di fornire delle informazioni di tipo probabilistico sul concretizzarsi in futuro di un determinato rischio.

Si tratta dei *risk assessment tool*, ovvero di sistemi che permettono all'IA, mediante l'analisi dei dati, di indicare con un valore puntuale la probabilità che un dato accadimento si verifichi[4].

Con specifico riferimento all'ambito processuale penale, è tecnicamente possibile avvalersi di questi strumenti per valutare, tra gli altri, i parametri della pericolosità sociale di un soggetto e della probabilità di astensione dal commettere ulteriori reati.

Dette valutazioni prognostiche possono trovare largo impiego nelle fasi di cognizione ed esecuzione, nelle quali sono valorizzabili ai fini dell'applicazione della disciplina relativa: alle misure di sicurezza e di prevenzione; alla recidiva; alla concessione dei benefici penitenziari; alle misure alternative; all'istituto del proscioglimento per particolare tenuità del fatto di cui all'art. 131-*bis* c.p.; alla

---

[3] Sulla ragione delle somiglianze tra le macchine basate sull'IA volte a fornire risposte probabilistiche sull'accadimento di un evento futuro oppure sulla conoscenza di un evento presente o passato ignoto, individuata nella comune caratteristica dell'incertezza, si v. G. Ubertis, *Intelligenza artificiale e giustizia predittiva*, in *www.sistemapenale.it*, 16.10.2023, pp. 2-4.

[4] Per un'introduzione generale al tema dei *risk assessment tool* si rimanda alla lettura di S. Quattrocolo, *Artificial intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Springer, Svizzera, 2020, pp. 146-176, nonché P. Severino, *Intelligenza artificiale e diritto penale*, cit., pp. 542-545.

sospensione condizionale della pena. È ipotizzabile impiegare tali strumenti prognostici anche per verificare l'ammissione al rito alternativo della sospensione del procedimento con messa alla prova oppure il superamento dell'ostatività penitenziaria[5]. Questi sistemi sono particolarmente utili anche per fornire al giudice delle ulteriori informazioni di carattere probabilistico che consentono di operare una più corretta commisurazione della pena[6].

Un altro ambito in cui una tale tipologia di strumenti incentrati sull'impiego dell'intelligenza artificiale appare rilevante è quello delle misure cautelari, consentendo una migliore valutazione della probabilità di ledere uno dei beni tutelati dalle esigenze di cui all'art. 274 c.p.p. Con tale mezzo prognostico il magistrato sarebbe in grado di considerare ai fini della decisione anche la probabilità di concretizzazione del pericolo di inquinamento probatorio, di fuga o di reiterazione del reato[7].

---

[5] Con specifico riferimento all'utilizzo di detti sistemi in fase esecutiva e di predisposizione del trattamento penitenziario cfr. G. Zara, *Tra il probabile e il certo. La valutazione del rischio di violenza e di recidiva criminale*, in *Diritto penale contemporaneo*, 20.05.2016, pp. 1-28; G. Caneschi, *Intelligenza artificiale e sistema penitenziario*, in *Rivista italiana di diritto e procedura penale*, n. 1, 2024, pp. 251-269.

[6] In tema di utilizzo di strumenti di valutazione del rischio per la determinazione della pena si v. G. Contissa, G. Lasagni, G. Sartor, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Diritto di Internet*, 2019, n. 4, pp. 619-634; L. D'Agostino, *Gli algoritmi predittivi per la commisurazione della pena*, in *Diritto penale contemporaneo*, 2019, n. 2, pp. 355-371. È in questo ambito di applicazione, quello dell'utilizzo dei *risk assessment tool* ai fini della commisurazione della pena, che si è sviluppata la celebre vicenda giudiziaria *Loomis*. Oggetto della controversia era l'utilizzo di un sistema denominato *Correctional offender management profiling for alternative sanctions* (più noto con l'acronimo C.O.M.P.A.S.) da parte dei giudici statunitensi e, in modo particolare, del Wisconsin. Tali strumenti erano funzionali a supportare il giudice nel determinare l'entità della condotta, fornendo una valutazione sotto il profilo del rischio di recidiva. Con l'utilizzo è emerso che il *software* calcolava una probabilità raddoppiata di commissione di reati per i soggetti afroamericani, valorizzando in modo indebito alcuni parametri come quelli dell'estrazione sociale e dell'appartenenza razziale. Alla luce di tali emergenze, la Corte Suprema del Wisconsin, pur non vietando l'utilizzo del sistema C.O.M.P.A.S., ha indicato di sfruttare tale *tool* come un mero supporto e non come parametro unico per la decisione. In merito si veda la sentenza *Wisconsin Supreme Court, State v. Loomis,* caso n. *2015AP157-CR,* sentenza del 13.07.2016, liberamente accessibile al seguente indirizzo: www.law.justia.com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html.

[7] In particolare, si segnalano i contributi di J. Nieva-Fenoll, *Intelligenza artificiale e processo*, Giappichelli, Torino, 2019, pp. 52-67 e di E. Guido, *Intelligenza artificiale e procedimento penale: ragionando di valutazione del rischio* de libertate, in *Archivio Penale*, fasc. 1, 2023, pp. 1-16.

Infine, occorre evidenziare anche l'esistenza di un possibile ambito di sviluppo connesso all'impiego dei sistemi di IA da parte dei pubblici ministeri e dei giudici dell'udienza preliminare e predibattimentale per svolgere delle prognosi in termini di ragionevole previsione di condanna, valorizzando il materiale probatorio presente nel fascicolo del pubblico ministero ed, eventualmente, nel fascicolo delle indagini difensive. Mediante tale attività è possibile sfruttare l'intelligenza artificiale per far emergere ulteriori elementi conoscitivi al fine di una migliore determinazione in ordine all'esercizio dell'azione penale o all'emissione di una sentenza di non luogo a procedere[8].

3.1.2 …*mediante l'approfondimento di eventi passati o presenti*

I magistrati, ma per molti aspetti anche i difensori delle parti private[9], potrebbero poi ricorrere a sistemi di IA al fine di ampliare il proprio spettro informativo migliorando la conoscenza di eventi passati oppure presenti.

In primo luogo, vi sono degli strumenti utili per avere un approfondimento conoscitivo sul piano probatorio – permettendo in vario modo di raccogliere un numero superiore di informazioni o, comunque, di migliore qualità – sia nella fase delle indagini sia durante il dibattimento.

Quanto alla fase delle indagini preliminari, l'intelligenza artificiale è utilizzabile per potenziare la portata dei "tradizionali" mezzi di ricerca della prova. In tal senso basti pensare all'utilizzo di *software* a base IA per programmare *malware* di Stato oppure per trascrivere ore e ore di registrazioni di intercettazioni telefoniche o, ancora, per analizzare l'enorme volume di documenti sequestrati a seguito di una perquisizione informatica.

Uno dei sistemi implementati con le tecnologie di intelligenza artificiale che trova maggiore applicazione in questa fase è quello dell'identificazione biometrica, intesa come strumento in grado di «automatizzare le procedure di verifica dell'identità mediante la valutazione di caratteristiche fisiologiche della

---

[8] Di questa idea V. Gramuglia, *Obbligatorietà dell'azione penale e ruolo dell'IA nelle scelte del pubblico ministero*, in *Archivio Penale*, fasc. 3, 2024, pp. 14-23; E. Malino, *Esercizio dell'azione penale e prognosi di condanna mediante software predittivi. Verso la creazione di un pm-robot*, in *La Legislazione Penale*, 19.06.2024, pp. 5-9; S. Speranza, *Decisioni algoritmiche e diritto*, Giuffrè, Milano, 2024, pp. 73-75.

[9] Sulle applicazioni dell'intelligenza artificiale volte a potenziare il ruolo del difensore si leggano le interessanti considerazioni di G. Lasagni, *Difendersi dall'intelligenza artificiale o difendersi con l'intelligenza artificiale? Verso un cambio di paradigma*, in *Intelligenza artificiale e processo penale*, a cura di G. Di Paolo, L. Pressacco, Edizioni Scientifiche Italiane, Napoli, 2022, pp. 63-90.

persona, quali le impronte facciali o digitali e la forma della mano o dell'iride, oppure comportamentali come voce, firma, andatura»[10].

Tale tipologia di attività può essere eseguita con due modalità, confrontando *a posteriori* e in differita i dati biometrici con il materiale raccolto, c.d. statica, oppure in tempo reale effettuando un confronto del materiale di riferimento con quello raccolto in diretta, c.d. dinamica o *live*. Come avremo modo di evidenziare (v. *infra* par. 8), l'*AI Act* prevede un diverso trattamento normativo per le due differenti modalità di impiego, stante il differente impatto sulle libertà fondamentali.

Sempre in ambito investigativo, i sistemi di IA potrebbero essere utilizzati per valutare la metodologia d'indagine più adatta al caso di specie o per individuare eventuali ulteriori ipotesi investigative, in tal modo non precludendo a prescindere eventuali piste e, conseguentemente, la raccolta di informazioni che potrebbero rivelarsi *a posteriori* utili.

In questa direzione vanno i cc.dd. *multi-agent systems*, ovvero quegli strumenti che sfruttano l'intelligenza artificiale per ipotizzare l'operato di agenti virtuali addestrati a comportarsi come operanti reali, così da ridurre al minimo i possibili (irreparabili *a posteriori*) errori umani nella conduzione delle indagini[11].

Con riferimento agli strumenti connessi all'intelligenza artificiale utili per l'integrazione del patrimonio conoscitivo probatorio utilizzabili nel corso del dibattimento, se ne evidenziano molteplici applicazioni.

In prima battuta, si è ipotizzato di sfruttare tali tecnologie in funzione di filtro per l'ammissione delle richieste probatorie, velocizzando l'attività istruttoria riguardante l'individuazione delle prove vietate o di quelle sovrabbondanti[12].

Nella successiva fase di assunzione delle prove, il ruolo di supporto dell'IA potrebbe essere molto rilevante, immaginando di ricorrere a dei *software* per valutare la credibilità di un testimone sulla base di vari parametri (la luce al momento dell'osservazione, la distanza dall'avvenimento raccontato, l'età del dichiarante, ecc.)[13] oppure per vagliare la completezza del relativo esame ed, eventualmen-

---

[10] Così L. Camaldo, *Intelligenza artificiale e investigazione penale predittiva*, cit., p. 245.

[11] In proposito si vedano G. Lasagni, Policing via Multi-Agent Systems: *un nuovo volto per la* digital forensics *(e non solo)?*, in *Nuove questioni di informatica forense*, a cura di R. Brighi, Aracne, Roma, 2022, pp. 303-321; V. Gramuglia, *Obbligatorietà dell'azione penale e ruolo dell'IA nelle scelte del pubblico ministero*, cit., pp. 23-27.

[12] In questi termini J. Nieva-Fenoll, *Intelligenza artificiale e processo*, cit., pp. 91-95. In merito anche G. Ubertis, *Processo penale telematico, intelligenza artificiale e Costituzione*, in *Diritto penale contemporaneo*, n. 4, 2020, p. 448.

[13] In tema si rimanda a J. Nieva-Fenoll, *Intelligenza artificiale e processo*, cit., pp.70-80; L. Pressacco, *Intelligenza artificiale e ragionamento probatorio nel processo*

te, formulare quesiti per completare il "pacchetto" di informazioni necessarie per verificare l'attendibilità del teste o per decidere sulla responsabilità penale dell'imputato.

Un altro apporto dell'intelligenza artificiale in sede probatoria potrebbe essere quello di potenziare i tradizionali strumenti di indagine peritale con le nuove tecnologie computazionali, permettendo di migliorare e velocizzare le attività di analisi in ambiti molto complessi come la cinematica, la genomica, la balistica, ecc.[14].

In questo senso l'impiego dell'IA, in ragione dell'accesso a un numero amplissimo ed eterogeno di informazioni, consentirebbe di migliorare le attività di simulazione e ricostruzione della scena del crimine, analizzando e registrando elementi eventualmente non valorizzati dall'operatore umano[15].

Sempre tra gli strumenti utili ad ampliare il panorama conoscitivo del giudice o delle parti possono essere ricondotti i sistemi di IA dedicati all'analisi dei documenti, che scandagliando il contenuto dei fascicoli processuali, talvolta aventi volumi non facilmente governabili, possono aiutare nell'individuazione degli atti e dei documenti più rilevanti, nonché nella valorizzazione di informazioni che l'operatore giuridico potrebbe non cogliere.

3.2 *Sistemi utilizzati da parte dei magistrati o dei difensori con funzione generativa e dai giudici con funzione decisoria*

L'applicazione forse più nota al grande pubblico dei *software* di intelligenza artificiale è quella legata alla capacità generativa. Rientrano in questa categoria i prodotti IA attualmente più noti, ovvero *ChatGPT*, *Copilot*, *Gemini*, ecc., che sono in grado, sulla base dei comandi forniti (cc.dd. *prompt*), di "creare" o meglio generare, attraverso l'elaborazione delle informazioni a cui hanno accesso, prodotti, quali documenti, immagini, file audio, ecc.

Queste tecnologie, e quelle che verranno via via affinate per specializzarsi nel settore legale, possono essere sfruttate per la redazione di atti ricalcanti le indicazioni fornite dall'operatore giuridico. In particolare, il difensore può impiegarle per la formulazione di istanze e atti difensivi, mentre il giudice per redigere la

penale, in *Intelligenza artificiale e processo penale*, cit., pp. 116-117.

[14] Per un approfondimento J. Nieva-Fenoll, *Intelligenza artificiale e processo*, cit., pp. 83-88; L. Pressacco, *Intelligenza artificiale e ragionamento probatorio nel processo penale*, cit., pp. 117-118.

[15] Sul tema R.E. Kostoris, *Intelligenza artificiale, strumenti predittivi e processo penale*, in *Cassazione Penale*, n. 5, 2024, p. 1646.

motivazione e il corpo delle sentenze sulla scorta della decisione presa e condensata nel dispositivo del provvedimento[16].

Fino a qui si è trattato dei sistemi basati sull'IA come supporto informativo e creativo funzionale all'attività umana, ma è possibile spingersi ancora oltre, non apparendo poi così utopistico ipotizzare il ricorso all'intelligenza artificiale per suggerire delle decisioni incentrate su valutazioni proprie della macchina o, addirittura, consentendole di decidere autonomamente.

Fanno parte del primo gruppo di strumenti, funzionali a suggerire delle decisioni basate su valutazioni proprie dell'IA, i *software* diretti ad analizzare la giurisprudenza in uno spettro crescente di assistenza alla decisione. Partendo dai mezzi più semplici, si individuano i sistemi di ricerca di casi "precedenti" analoghi a quello oggetto di studio, passando ad altri più avanzati si hanno quelli in grado di avvisare il giudice che si sta discostando dalle decisioni precedenti, così creando un disallineamento, fino ad arrivare a strumenti in grado di suggerire al giudice una proposta di decisione nel merito a seguito di un'autonoma valutazione. Addirittura, è possibile immaginare degli applicativi in cui è direttamente la macchina a decidere, così riconoscendo un'importanza tale all'intelligenza artificiale da innalzarla al ruolo di protagonista decisionale[17].

---

[16] In generale sui limiti all'impiego attuale dell'IA generativa (in particolare di *ChatGPT*) per lo sviluppo di prodotti "legali", si rimanda all'interessante studio di D. Amidani, *ChatGPT bocciato all'esame di diritto processuale penale. Attendibilità e trasparenza dei sistemi di intelligenza artificiale alla luce di un esperimento*, in *Sistema penale*, 3.10.2024, pp. 1-32. Sul tema dell'utilizzo di strumenti generativi da parte dell'avvocato si rimanda a G.A. Parini, *Utilizzo dell'intelligenza artificiale in sostituzione o a supporto dell'avvocato: prospettive future e dovere di competenza tecnologica*, in *Teoria e prassi dell'informatica giuridica. Per una riflessione filosofica*, vol. 2, n. 23, 2021, pp. 161-174; G.A. Parini, *L'intelligenza artificiale, le professioni legali e il dovere di competenza tecnologica dell'avvocato*, in *Direito e Inteligência Artificial*, a cura di M.R. Guimarães, R.T. Pedro, pp. 251-273. Con riferimento all'utilizzo di strumenti di IA generativa a supporto del giudice si v. R.E. Kostoris*, Intelligenza artificiale, strumenti predittivi e processo penale*, cit., pp. 1650-1652.

[17] Con riferimento all'utilizzo dell'IA a supporto del giudice, o in sua sostituzione, nella decisione del giudizio e nella formulazione della motivazione della sentenza, si rimanda a J. Nieva-Fenoll, *Intelligenza artificiale e processo*, cit., pp. 90-115; R. Bichi, *Intelligenza artificiale, giurimetria, giustizia predittiva e algoritmo decisorio.* Machina sapiens *e il controllo sulla giurisdizione*, in *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., pp. 439-443; S. Quattrocolo, *Artificial intelligence, Computational Modelling and Criminal Proceedings*, cit., pp. 101-129; G. Barone, *Giustizia predittiva e certezza del diritto*, Pacini, Pisa, 2024, pp. 47-177. In tema di *algorithmic legitimacy*, errore giudiziario e possibile configurazione della responsabilità civile del magistrato si v. G. Pasceri, *La predittività delle decisioni. La funzione giurisprudenziale e la responsabilità delle parti nell'utilizzo dell'intelligenza artificiale*, Giuffré, Milano, 2022, pp. 143-149.

Due applicazioni pratiche di questi sistemi di decisione autonoma si potrebbero immaginare in relazione alla verifica della responsabilità penale dell'imputato oppure alla determinazione della pena da irrogare in concreto. In questo modo potrebbe essere ponderata la discrezionalità del giudice nella determinazione della pena con suggerimenti volti a garantire un'applicazione più omogenea di tale potere.

3.3 *La giurimetria*

Tra gli strumenti a cui potrebbero ricorrere il pubblico ministero, l'accusato, la persona offesa, le altre parti private o qualsiasi soggetto terzo durante il (o anche prima del) processo ci sono quelli riconducibili alla giurimetria, avente quale finalità di prevedere l'esito delle decisioni giudiziarie[18].

Si tratta di *software*, già in fase di sviluppo e che hanno visto una crescita esponenziale negli ultimi anni, volti a consentire agli utenti di "pronosticare", sulla scorta delle informazioni analizzate dall'algoritmo, gli esiti del processo.

Tali strumenti potrebbero esercitare una forte influenza sulle strategie e le decisioni difensive, soprattutto in termini di scelta del rito ordinario o alternativo da affrontare[19].

Sotto questo profilo è interessante monitorare anche lo sviluppo di specifici *tool* per valutare l'opportunità di ricorrere a un dato rito alternativo. Basti pensare, a mero titolo esemplificativo, all'applicazione della pena su richiesta delle parti, rispetto alla quale sarebbe cruciale poter prevedere in anticipo le potenziali condizioni alle quali il pubblico ministero sarebbe disposto a prestare il proprio consenso. Allo stesso tempo, avere informazioni prognostiche affidabili sull'esito statisticamente rilevante dei processi sarebbe importantissimo anche per decidere di presentare opposizione a un decreto penale di condanna oppure prestare acquiescenza.

Si tratta di sistemi che per elaborare previsioni affidabili richiedono una grande mole di dati e, soprattutto, una buona capacità di simulare le dinamiche correlate

---

[18] Sul tema della giurimetria nell'ambito del processo penale si rimanda alla lettura di R. Bichi, *Intelligenza artificiale, giurimetria, giustizia predittiva e algoritmo decisorio.* Machina sapiens *e il controllo sulla giurisdizione*, cit., pp. 428-438; R.E. Kostoris, *Intelligenza artificiale, strumenti predittivi e processo penale*, cit., pp. 1652-1654.

[19] Sul punto si vedano C. Parodi, V. Sellaroli, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto penale contemporaneo*, n. 6, 2019, pp. 65-66; G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Diritto penale contemporaneo*, n. 4, 2020, pp. 82-83.

all'esercizio della funzione giudiziale, al ragionamento giuridico, alla sensibilità valutativa della ragionevolezza del dubbio e all'esercizio dei poteri discrezionali[20].

4. *Gli impieghi dell'intelligenza artificiale nella fase dell'esecuzione e in quella penitenziaria*

Come anticipato, i sistemi di IA possono trovare applicazione anche successivamente alla conclusione della fase di cognizione e al passaggio in giudicato del provvedimento.

Si è già fatto riferimento ai possibili impieghi dell'intelligenza artificiale durante l'esecuzione con riferimento agli strumenti di tipo prognostico volti a fornire delle informazioni di natura probabilistica sul concretizzarsi in futuro di un determinato rischio (v. *supra* 3.1.1), quale quello di pericolosità sociale di un soggetto oppure di recidiva, utile per l'applicazione delle misure di sicurezza, della concessione dei benefici penitenziari, delle misure alternative o per valutare il superamento dell'ostatività penitenziaria.

Altri utilizzi si possono individuare in sede di esecuzione della pena detentiva in regime intramurario, apparendo utile l'impiego di sistemi IA anche nella gestione degli istituti penitenziari. In questo senso si potrebbe pensare di utilizzare le tecnologie di riconoscimento facciale per velocizzare le procedure di accesso dei visitatori per i colloqui.

Un'altra potenziale applicazione dell'intelligenza artificiale potrebbe essere legata agli spostamenti all'interno del penitenziario, configurando un sistema di domotica, incentrato sulle autorizzazioni preventive per l'accesso a determinate aree[21].

5. *IA e organizzazione giudiziaria*

Gli strumenti che utilizzano l'intelligenza artificiale possono giocare un ruolo molto rilevante anche nel miglioramento dell'organizzazione degli uffici giudiziari e dell'ordinamento giudiziario.

---

[20] In questi termini S. Quattrocolo, *Artificial intelligence, Computational Modelling and Criminal Proceedings*, cit., pp. 113 e 126, nonché R.E. Kostoris, *Predizione decisoria,* diversion *processuale e archiviazione*, in *www.sistemapenale.it*, 23.07.2021, p. 7.

[21] Tali spunti sull'impiego dell'intelligenza artificiale in carcere e, in particolare, su alcune forme avanzate di sorveglianza e controllo in Asia e in Europa sono offerti da G. Caneschi, *Intelligenza artificiale e sistema penitenziario*, cit., pp. 264-266.

Con riferimento a questo secondo profilo, è possibile immaginare l'utilizzo dell'IA per migliorare i meccanismi esistenti di distribuzione del lavoro tra i diversi magistrati in forza all'ufficio, così da affinare la distribuzione delle risorse e dei carichi di lavoro della magistratura. A titolo esemplificativo si pensi al *software* di Gestione Informatica Automatizzata Assegnazioni Dibattimento (noto con l'acronimo G.I.A.D.A.), utilizzato dai tribunali per l'assegnazione automatizzata e ponderata dei fascicoli ai giudici monocratici e al collegio. Tale applicativo si incentra su un sistema di classificazione che determina il "peso" di ogni nuovo processo, individuando così il carico di lavoro stimato per la definizione. I criteri sottesi a tale "pesatura" sono determinati in modo autonomo e discrezionale da ciascun tribunale. In tale contesto i sistemi di intelligenza artificiale potrebbero essere utilizzati per supportare i singoli uffici giudiziari nella definizione (ed, eventualmente, nell'aggiornamento) di tali parametri.

Un altro ambito in cui gli strumenti a base IA potrebbero essere impiegati al fine di supportare delle scelte di carattere organizzativo è quello dei criteri di priorità nella trattazione delle notizie di reato. In merito, è ipotizzabile il ricorso all'intelligenza artificiale per aiutare gli uffici del pubblico ministero a individuare dei criteri di priorità utili a garantire un elevato grado di efficacia e uniformità nell'esercizio dell'azione penale, attraverso l'analisi dei dati processuali al fine di intercettare e monitorare le aree di maggiore criticità[22].

Quanto al miglioramento dell'efficienza della "macchina" giustizia sotto il profilo della gestione amministrativa del processo penale, non è utopistico immaginare l'impiego di *software* potenziati dall'intelligenza artificiale in grado di analizzare i dati per identificare falle organizzative e aree di grave inefficienza. In tale settore, l'IA permetterebbe di automatizzare compiti ripetitivi e non discrezionali (come quelli relativi alle notifiche, ancor più se telematiche) o per tradurre atti e revisionare documenti o modelli standard.

6. *Modellazione predittiva giudiziaria per il legislatore penale*

Ampliando gli orizzonti dell'impiego degli strumenti di intelligenza artificiale anche ad ambiti non collegati al processo penale in senso stretto, ci si può ora

[22] Per un approfondimento sul tema si veda V. Gramuglia, *Obbligatorietà dell'azione penale e ruolo dell'IA nelle scelte del pubblico ministero*, cit., pp. 27-38. Sulla possibilità di configurare un modello di simulazione ad agenti per valutare l'impatto di alcuni criteri di priorità per lo smaltimento dei procedimenti penali adottabili dal giudice, che potrebbe fungere da base per un modello impiegabile dal pubblico ministero incentrato sullo sfruttamento dell'intelligenza artificiale, v. L. Bonaventura, A. Consoli, *La scelta dei criteri di priorità per il giudice penale: effetti sui carichi pendenti e sul costo sociale*, in *Munich Personal RePEc Archive*, 10.04.2009, pp. 5-14.

interrogare su come tale tecnologia possa supportare il legislatore nella redazione e nel miglioramento delle norme in materia processuale penale.

Al di là di eventuali *software* volti a semplificare la scrittura dei provvedimenti e a verificare la conformità con i principi sovranazionali e con le *best practices* internazionali, appare interessante soffermarsi sul tema che indicheremo come "modellazione predittiva".

Tale attività si concretizza, nel caso di specie, nell'utilizzo di strumenti di simulazione e previsionali potenziati dalla capacità computazionale dell'intelligenza artificiale per supportare il legislatore (o più in generale il *policy maker*) nell'elaborazione di norme processuali penali.

Grazie a questi *tool*, che permettono di valutare l'influsso di specifiche modifiche legislative sui dati giudiziari penali, è possibile immaginare una facilitazione nell'adozione delle scelte normative (o organizzative), avendo maggiore consapevolezza rispetto a quale possa essere il prevedibile impatto della propria decisione sulla giustizia penale.

Sul piano terminologico occorre precisare che il termine "modellazione predittiva" – da intendersi, come sopra indicato, quale impiego di strumenti di IA da parte del legislatore per prevedere l'impatto delle possibili modifiche legislative sul sistema – non deve essere confuso con quello più ampio di "giustizia predittiva", utilizzato per fare riferimento in via generale a tutti i sistemi che consentono, mediante l'adozione di calcoli matematici, di algoritmi e sistemi di intelligenza artificiale, di prevedere il verificarsi di un certo evento rilevante per il sistema penale.

Più nel dettaglio, il termine giustizia predittiva viene utilizzato per indicare diversi specifici impieghi dell'IA nel procedimento penale e, in particolare, per riferirsi alla giurimetria – quale strumento utile a prevedere l'esito decisorio di uno specifico processo sfruttando strutture matematiche –, alla possibilità di ricorrere all'IA a supporto o in sostituzione del giudice, nonché per indicare le attività di polizia predittiva[23].

La modellazione predittiva, invece, è costituita da tutti quegli strumenti che consentono – combinando i modelli di regressione lineare, regressione logistica, analisi delle serie storiche, ecc. con le tecniche algoritmiche, l'intelligenza artificiale e il *machine learning* – di operare predizioni sullo sviluppo dei dati, sul comportamento futuro di determinate variabili o sul verificarsi di eventi in ragione delle opzioni decisorie vagliate dal legislatore (distinguendosi pertanto dalla giurimetria per la differenza in punto di oggetto di previsione, l'impatto di una modifica legislativa sul sistema penale e non l'esito di uno specifico processo,

[23] In questi termini anche A. Maceratini, *La giustizia predittiva: potenzialità e incognite*, in *MediaLaws*, n. 2, 2024, pp. 231-241.

e per la specificità del soggetto destinatario, il *policy maker* e non le parti o coloro che sono interessati alla preventiva conoscenza di una determinata decisione processuale)[24].

Tali tecniche, in cui l'uso dell'IA è centrale, possono fornire un apporto utile al Parlamento e al Governo (trattandosi di ambiti tecnici dove spesso si ha il ricorso a decreti legislativi) nella definizione degli interventi normativi, permettendo di effettuare simulazioni realistiche e di avere uno spettro previsionale abbastanza preciso degli effetti sui numeri del processo penale derivanti dalle loro scelte.

Parallelamente, tali strumenti possono risultare particolarmente preziosi anche per l'apparato amministrativo (a livello sia centrale del Ministero della giustizia sia locale degli uffici giudiziari) nella programmazione dell'attività organizzativa e nella distribuzione delle risorse.

7. *Intelligenza artificiale e raccolta dei dati processuali penali*

Fondamentale per il corretto sviluppo e l'utilizzo dei sistemi di intelligenza artificiale collegati alla giustizia penale è la disponibilità di dati processuali penali appartenenti a classi eterogenee, nonché affidabili e completi, circostanza questa allo stato, almeno in Italia, non ricorrente (v. *infra* par. 9).

Partendo da questa premessa è possibile evidenziare che gli strumenti che sfruttano l'intelligenza artificiale possono essere utilizzati anche per migliorare il sistema di raccolta e conservazione dei dati processuali penali.

La rivoluzione informatica di inizio secolo ha già portato a un'automatizzazione della raccolta e conservazione dei dati, non più eseguita manualmente mediante registri cartacei, offrendo nuove opportunità di sfruttamento mediante le tecnologie dei *data warehouse* e dei più moderni *data lake* (sulla cui distinzione si rimanda al par. 9).

---

[24] Per una prima introduzione al tema si consenta di rimandare a T. Di Candia, *La tartaruga giudiziaria penale e la vela dei riti alternativi. Principio della ragionevole durata e statistica applicata*, Giappichelli, Torino, 2024, pp. 23-28. Quanto al rapporto di tali sistemi con le scienze sociali computazionali e il possibile impatto sui modelli legislativi ai fini della *compliance* con il principio europeo di *scientific evidence-based policy making*, si veda un contributo di prossima pubblicazione dal titolo *L'intelligenza artificiale al servizio del legislatore processuale penale:* data lake *e modellazione predittiva*, contenuto negli atti del convegno relativi alla Giornata della ricerca del Dipartimento di Diritto Economie e Culture dell'Università degli Studi dell'Insubria, denominata *Diritto, economia, culture e intelligenza artificiale. Presupposti, applicazioni e limiti*, tenutasi a Como il 26.09.2024.

Le potenzialità di questi strumenti possono essere ulteriormente ampliate ricorrendo all'IA, che consente di migliorare la raccolta automatizzata dei dati e di valorizzarli mediante tecniche di *machine learning* e *data mining*, favorendo l'estrazione di ulteriori informazioni dal *set* di dati già a disposizione[25].

8. *La disciplina in materia di utilizzo dell'IA nella giustizia penale*

Nei paragrafi precedenti sono stati individuati gli impieghi, allo stato tecnicamente possibili o immaginabili in futuro, dei sistemi di intelligenza artificiale nel procedimento penale e in alcuni campi affini.

L'impatto dell'IA sul processo penale potrebbe portare immensi vantaggi in termini di efficienza del sistema giustizia e di miglioramento della qualità delle decisioni giudiziarie. A fronte di tale luminosa prospettiva è presente un lato oscuro della medaglia, che cela insidiosi pericoli per le garanzie tutelate a livello costituzionale e sovranazionale.

In particolare, senza entrare qui nel dettaglio, i rischi più evidenti connaturati all'utilizzo dei diversi strumenti incentrati sull'IA possono essere quelli di un'eccessiva standardizzazione delle decisioni, con perdita della capacità di "personalizzazione" delle stesse, il passaggio da un diritto penale del fatto a un diritto penale dell'autore appartenente a una categoria più a rischio di commissione di reati e, ancora, l'appiattimento giudiziario e della macchina sulle decisioni precedenti, con effetto di stagnazione della giurisprudenza e di una carenza di sensibilità ai mutamenti sociali[26].

La necessità di contemperare tali, ed altri, rilevanti rischi con le opportunità derivanti dallo sfruttamento di tecnologie astrattamente capaci di avere un impatto molto positivo sul sistema giustizia (e non solo) ha spinto all'adozione di una regolamentazione in tema di intelligenza artificiale.

Trattandosi di un fenomeno di portata globale, i primi macro interventi si sono avuti nelle sedi sovranazionali, dapprima a livello di *soft law* nel contesto della grande Europa e, recentemente, a livello di *hard law* all'interno della piccola Europa.

In seno al Consiglio d'Europa, la Commissione europea per l'efficienza della giustizia (CEPEJ) ha adottato, il 3.12.2018, la Carta etica europea sull'utilizzo

---

[25] Con riferimento allo stato attuale del sistema di raccolta delle statistiche processuali penale si v. *infra* par. 9.

[26] Di questa idea V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., p. 559; G. Riccio, *Ragionando su intelligenza artificiale e processo penale*, in *Archivio Penale*, n. 3, 2019, p. 10; A. Santosuosso, G. Sartor, *La giustizia predittiva: una visione realistica*, in *Giurisprudenza Italiana*, n. 7, 2022, p. 1761.

dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, che indica cinque principi generali in tema per ridurre i possibili rischi derivanti dall'applicazione di queste tecnologie sui diritti della persona. Si tratta dei principi del rispetto dei diritti fondamentali, di non discriminazione della decisione algoritmica, di qualità e sicurezza dei dati giudiziari, di trasparenza, imparzialità ed equità dei processi decisionali, nonché del controllo da parte dell'utilizzatore, il quale dovrebbe agire informato e nel pieno controllo delle proprie scelte rispetto all'*output* dell'IA.

Facendo proprio questo approccio di tutela dei diritti umani, l'Unione europea ha regolamentato a livello generale l'impiego dell'IA con il Regolamento (Ue) 2024/1689 del Parlamento Europeo e del Consiglio, del 13.06.2024, che stabilisce regole armonizzate sull'intelligenza artificiale (c.d. *AI Act*).

Tale atto normativo consente a produttori, *providers*, *deployers*, importatori e distributori di sviluppare e commercializzare nel mercato unico europeo sistemi che incorporano l'IA in misura inversamente proporzionata al rischio che dall'impiego di questi strumenti possa derivare una lesione di diritti della persona, c.d. *risk-based approach*[27]. A un livello di rischio più alto corrisponde un divieto o una limitazione nell'utilizzo mediante la necessità di adottare una serie di garanzie, mentre al calare del rischio si ha una maggiore libertà di sviluppare e di utilizzare sistemi di intelligenza artificiale.

Più dettagliatamente, il regolamento individua quattro livelli di rischio connessi all'impiego di sistemi di IA: inaccettabile, elevato, limitato e minimo.

Con specifico riferimento all'utilizzo di strumenti di IA nell'amministrazione della giustizia, dalla lettura dei considerando e del testo normativo, appare evidente che le diverse possibili applicazioni al procedimento penale e agli ambiti connessi sono state valutate con livelli di rischio differenti.

In primo luogo, non sono considerati ad altro rischio i sistemi che sfruttano l'intelligenza artificiale destinati ad attività amministrative puramente accessorie, che non incidono sull'effettiva amministrazione della giustizia rispetto al singolo caso. In questo senso vengono considerate espressamente le attività di anonimizzazione o pseudonimizzazione di decisioni, documenti o dati giudiziari, la comunicazione tra il personale e i compiti amministrativi[28].

In tale categoria potrebbero essere fatte rientrare, in quanto di carattere organizzativo e non incidenti su singoli procedimenti, anche alcune delle attività individuate nel paragrafo 5, quale l'impiego dell'intelligenza artificiale per identificare aree di inefficienza organizzativa e automatizzare compiti ripetitivi e non

---

[27] In merito alla genesi e alla struttura dell'*AI Act* si consiglia la lettura di S. Quattrocolo, *Intelligenza artificiale e processo penale: le novità dell'AI Act*, in *Diritto di Difesa*, 16.01.2025, pp. 1-4.

[28] Cfr. considerando n. 61, ultimo periodo del Regolamento 2024/1689.

discrezionali, nonché per migliorare l'analisi e la distribuzione dei carichi di lavoro mediante l'integrazione nel sistema G.I.A.D.A.

Sono invece considerati come ad alto rischio, in ragione del potenziale impatto negativo rispetto alle libertà individuali, al diritto a un ricorso effettivo e a un giudice imparziale, i *tool* di IA destinati a essere utilizzati per assistere le autorità giudiziarie nelle attività di ricerca e interpretazione dei fatti e del diritto, nonché nell'applicazione della legge a una serie concreta di fatti[29].

Pertanto, è subordinato all'impiego di speciali precauzioni l'utilizzo dell'intelligenza artificiale in alcune applicazioni con funzione di ampliamento del contesto informativo mediante l'approfondimento di eventi passati o presenti (v. *supra* par. 3.1.2), quali la trascrizione automatizzata delle intercettazioni, l'analisi di ingenti volumi di documenti, l'impiego di *multi-agent systems*, l'individuazione di prove vietate o sovrabbondanti, la valutazione della credibilità del testimone oppure il potenziamento degli strumenti di simulazione a disposizione del perito. Parimenti ad alto rischio, in quanto potenzialmente in grado di incidere sull'attività di interpretazione dei fatti e di applicazione del diritto, può essere considerato l'impiego da parte dell'autorità giudiziaria di sistemi generativi, nonché di *software* che supportino il giudice suggerendo delle possibili decisioni a seguito di autonome valutazioni (v. *supra* par. 3.2). In questo senso va letto anche l'utilizzo dell'intelligenza artificiale per migliorare l'individuazione dei criteri di priorità (v. *supra* par. 5), non potendosi considerare un'applicazione con ricadute meramente organizzative ai sensi dell'art. 6, c. 2 del Regolamento e del punto 6, lett. c) dell'allegato III, incidendo invece sull'effettiva amministrazione della giustizia rispetto al caso concreto.

Inoltre, l'*AI Act* espressamente considera a rischio elevato i sistemi che sfruttano l'intelligenza artificiale per verificare l'affidabilità degli elementi probatori nel corso delle indagini o del processo, non incentrati sulla mera profilazione delle persone fisiche.

Analogamente, ad alto rischio sono considerati anche i *risk assessment tool* impiegati nel contrasto alle attività criminali per valutare il rischio per una persona fisica di diventare vittima di reati oppure per determinare il rischio di commissione del reato o di recidiva, non incentrati sulla mera profilazione delle persone fisiche[30]. Sono vietati, in quanto costituenti impieghi a rischio inaccettabile, gli strumenti che sfruttano l'IA per effettuare valutazioni del rischio relative a persone fisiche per prevedere il pericolo che le stesse commettano dei reati che si

[29] V. considerando n. 61, secondo periodo, art. 6, c. 2 del Regolamento e allegato III, punto 8.

[30] Si v. considerando n. 59, art. 6, c. 2 e allegato III, punto 6, lett. c) del Regolamento.

basino unicamente sulla profilazione della persona o sulla valutazione dei tratti e delle caratteristiche della personalità[31].

Riprendendo rapidamente la distinzione in punto di strumenti di polizia predittiva tra *place-based systems* e *person-based systems* (v. *supra* par. 2), i primi sono finalizzati a individuare delle zone a particolare rischio statistico per la commissione di reati (cc.dd. *hotspot*) mediante lo studio di dati di carattere geografico, ambientale e sociale[32]. In questo modo è possibile per le forze dell'ordine concentrare le proprie risorse in modo tale da farsi trovare "nel posto giusto".

I *person-based systems* analizzano una moltitudine di dati, tra i quali quelli relativi agli individui e alla reiterazione dei crimini, al fine di identificare chi statisticamente potrebbe commettere un reato. In particolare, i sistemi basati sulla persona ricercano dei profili di serialità criminale (cc.dd. *crime linking*) per anticipare la commissione della successiva condotta penalmente rilevante oppure per individuare i soggetti potenzialmente più a rischio di diventare vittime di reato[33].

Sulla scorta di quanto previsto dal Regolamento 2024/1689, appare evidente che non siano vietati i *place-based systems*, da considerarsi come sistemi ad alto rischio, in quanto sfruttano l'analisi di dati principalmente ambientali. Discorso diverso vale per i *person-based systems*, che sono considerati strumenti ad alto rischio quando impiegano informazioni provenienti da fonti eterogenee, mentre sono vietati quando volti a valutare o prevedere la probabilità che una persona fisica commetta un reato basandosi unicamente sulla profilazione di una persona fisica o sulla valutazione dei tratti e delle caratteristiche della personalità[34].

---

[31] Cfr. art. 5, c. 1, lett. d) Regolamento.

[32] Due tra i principali *software* di questo tipo sono *XLAW* e *PELTA Sicurezza Urbana*. *XLAW* è un sistema basato su un modello previsionale di *deep learning* volto a prevenire la commissione di reati mediante un sistema di allarmi georeferenziati ed è stato sperimentato dalle questure di Napoli, Prato, Salerno, Venezia, Modena e Parma. In merito si rimanda alla consultazione del relativo sito internet: www.xlaw.it. *PELTA Sicurezza Urbana* è un sistema di supporto decisionale per prevenire la commissione di reati attraverso l'analisi dinamica del rischio. È utilizzato dalle forze di polizia locale di alcuni comuni, tra cui Ancona, Como, Campobasso e Pescara. In merito si rimanda al sito: www.pelta.it/pelta-suite-sicurezza-urbana.

[33] Strumenti di questo tipo sono *KeyCrime* e il suo derivato *Giove*. Si tratta di due sistemi in grado di individuare delle correlazioni tra reati – analizzando i dati relativi al luogo, all'ora, alle modalità di commissione del delitto, al comportamento tenuti dagli autori – al fine di prevenire il compimento di nuovi e interrompere l'eventuale serialità. Per un approfondimento si rimanda a L. Camaldo, *Intelligenza artificiale e investigazione penale predittiva*, cit., pp. 238-240.

[34] Di questa idea E. Pietrocarlo, *La* predictive policing *nel regolamento europeo sull'intelligenza artificiale*, in *La legislazione penale*, 26.09.2024.

Del pari, simili considerazioni possono farsi rispetto ai *risk assessment tool* impiegabili dal giudice nel corso del giudizio per valutare la pericolosità sociale di un soggetto o la probabilità di astensione dal commettere ulteriori reati (v. *supra* par. 3.1.1), che, tuttavia, appaiono spesso basarsi unicamente sulla considerazione delle soggettività individuali, così rendendo necessaria un'attenta configurazione del sistema per non ricadere negli impieghi dell'intelligenza artificiale non consentiti[35].

Sono espressamente vietati anche i sistemi IA di identificazione biometrica remota in tempo reale[36], salvo che siano impiegati nel contrasto a reati connotati da particolare gravità[37].

Ne consegue che non è consentito il ricorso ai *software* di identificazione biometrica *live*, stante il pericolo di creare indebiti sistemi di sorveglianza di massa, poiché tali strumenti permettono di analizzare un flusso continuo di immagini e di automatizzare il riconoscimento in diretta dei soggetti che vengono video ripresi, così rintracciando i profili ricercati.

Sono invece classificati ad alto rischio gli strumenti IA di identificazione *a posteriori*, diretti ad automatizzare l'individuazione dei soggetti ritratti in un fotogram-

---

[35] Per un'analisi critica del tema si consiglia la lettura di S. Quattrocolo, *Intelligenza artificiale e processo penale: le novità dell'AI Act*, in *Diritto di Difesa*, cit., pp. 4-8. Con riferimento alla natura incerta dei *risk assessment tool*, v. L. Macrì, *I primi passi dell'Italia verso l'impiego dell'IA nel processo penale e il calcolo del rischio di recidiva*, in *Giustizia Penale Web*, 6.02.2025, pp. 11-19.

[36] Gli strumenti per il riconoscimento biometrico più diffusi sono quelli diretti al riconoscimento facciale mediante la raccolta di immagini con i sistemi di videosorveglianza, cc.dd. *facial recognition tool*. Tali tecnologie ricorrono alla c.d. *faceprint*, ovvero valorizzano l'insieme delle caratteristiche del viso che lo rendono unico. Si tratta di sistemi che presentano o che sono collegati a banche dati contenenti un numero elevatissimo di immagini a cui sono associati i dati di altrettanti soggetti. Per un approfondimento sui sistemi di riconoscimento facciale si rimanda alla lettura di M. Colacurci, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema penale*, n. 9, 2022, pp. 23-44; J. Della Torre, *Quale spazio per i* tools *di riconoscimento facciale nella giustizia penale?*, in *Intelligenza artificiale e processo penale*, cit., pp. 17-53. Il *software* di questo tipo più diffuso in Italia è il *Sistema automatico di riconoscimento immagini*, noto con l'acronimo S.A.R.I., in merito si vedano R.V.O. Valli, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, in *Il penalista*, 16.01.2019; E. Sacchetto, Face to face: *il complesso rapporto tra* automated facial recognition technology *e processo penale*, in *La Legislazione Penale*, 16.10.2020, p. 7-9; G. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato*, in *La Legislazione Penale*, 11.12.2021, pp. 4-22; L. Camaldo, *Intelligenza artificiale e investigazione penale predittiva*, cit., pp. 246-250

[37] Il divieto è posto dall'art. 5, c. 1, lett. h) del Regolamento 2024/1689.

ma. Si tratta di un'attività statica, in cui viene inserita l'immagine del soggetto alla cui identità si vuole risalire e il *software* la confronta con tutte quelle presenti in banca dati al fine di fornire uno o più nominativi a cui è potenzialmente riconducibile l'effigie, conseguendone un minore impatto sulle libertà individuali e un rischio di controllo generalizzato ben più contenuto rispetto agli strumenti *live*.

È ora possibile ampliare lo spettro della compatibilità con l'*AI Act* soffermandosi sugli impieghi dell'intelligenza artificiale negli ambiti connessi al procedimento penale.

Con riferimento all'utilizzo dell'IA nella giurimetria (v. *supra* par. 3.3), quale strumento per la previsione dell'esito di uno specifico processo, questo non sembrerebbe ricadere né nelle attività vietate di cui all'art. 3 del Regolamento né tra quelle ad alto rischio previste dal combinato disposto dell'art. 6 e dell'allegato III, punti 6 e 8. Un limite a tale tipo di impiego è quello di non ricadere nel generalizzato divieto di profilazione dell'attività del giudice persona fisica.

Del pari, l'intelligenza artificiale sembrerebbe legittimamente impiegabile anche nella modellazione predittiva (v. *supra* par. 6), non evidenziandosi particolari rischi per le libertà individuali e, in specie, per la determinazione dei processi democratici[38].

Anche l'impiego dell'IA per migliorare il sistema di raccolta delle statistiche giudiziarie (v. *supra* par. 7) non sembrerebbe porre particolari elementi di rischio rilevanti per il Regolamento 2024/1689.

Il dinamico quadro qui tratteggiato dei limiti normativi all'interno dei quali potranno svilupparsi le applicazioni dell'IA nel processo penale, potrebbe essere presto arricchito anche da una disciplina nazionale diretta, tra le diverse finalità perseguite, ad adeguare la normativa italiana al Regolamento europeo[39].

9. *L'attuale sistema di raccolta delle statistiche processuali penali e le prospettive di miglioramento*

Dalla disamina fin qui condotta dei sistemi di IA per l'amministrazione della giustizia penale emerge il ruolo fondamentale che ricoprono i dati per il corretto funzionamento dei *tool* che sfruttano l'intelligenza artificiale. Questi strumenti

[38] Il punto 8, lettera b) dell'allegato III del Regolamento ritiene ad alto rischio i sistemi IA impiegabili per influenzare l'esito di un'elezione o di un referendum o il comportamento di voto delle persone fisiche nell'esercizio del loro voto alle elezioni o ai referendum.

[39] Il riferimento è alla delega conferita dal Parlamento al Governo in materia di intelligenza artificiale con la L. 23 settembre 2025, n. 132, il cui art. 15 fornisce alcune indicazioni in tema di impiego dei sistemi di intelligenza artificiale nell'attività giudiziaria.

analizzano una immensa mole di dati di natura eterogenea, tra i quali, in misura preponderante, i dati processuali penali. Pertanto, presupposto per il corretto funzionamento di tali sistemi (e in particolar modo di quelli predittivi) è la disponibilità di un grande volume di informazioni di natura giudiziaria penale, che debbono essere complete, corrette e specifiche.

Il problema della selezione dei dati è fondamentale per evitare che la macchina faccia propri dei *bias* cognitivi, dei pregiudizi oppure che abbia delle "allucinazioni" derivanti dal mancato accesso al completo corredo informativo[40].

Fondamentale per evitare di "contaminare" le analisi computazionali con elementi di discrezionalità individuale è la corretta scelta degli elementi da raccogliere e dei requisiti che devono essere da questi posseduti.

Un'ulteriore difficoltà connaturata alle modalità di lavoro dei sistemi IA che sfruttano le tecniche di autoapprendimento è quella della c.d. *black box*, poiché l'autonoma capacità di automigliorarsi del sistema può non rendere possibile la ricostruzione del percorso computazionale seguito dalla macchina e l'identificazione dei dati utilizzati. Tale criticità crea delle difficoltà soprattutto sotto il profilo dell'eventuale garanzia del contraddittorio per l'imputato.

Appare evidente come l'esito dell'attività svolta dalla macchina dipenda dalla quantità e dalla qualità dei dati forniti alla stessa.

A fronte di tale necessità, il sistema attuale di raccolta dei dati processuali penali risulta arcaico e inefficace; infatti, le statistiche giudiziarie penali vengono attualmente acquisite dal Ministero della giustizia con modelli trimestrali informatizzati che devono essere estrapolati e inviati da parte dei singoli uffici giudiziari. Occorre evidenziare che il sistema informatico utilizzato per la gestione operativa e amministrativa dei fascicoli non è diretto alla, e ottimizzato per la, raccolta di dati, ma serve principalmente per registrare e conservare le più importanti informazioni relative ai singoli procedimenti penali. La raccolta dei dati giudiziari penali a livello centrale avviene ancora con il tradizionale metodo basato sull'invio con cadenza trimestrale alla Direzione Generale di Statistica del Ministero della giustizia dei dati in formato aggregato estratti dai registri informatizzati da parte di ogni singolo ufficio giudiziario (tali informazioni devono essere comunicate entro 45 giorni dalla scadenza del trimestre).

Tuttavia, come accennato (v. *supra* par. 7), esistono delle modalità di raccolta e organizzazione dei dati più moderne e idonee ad essere potenziate mediante l'impiego di tecnologie connesse all'intelligenza artificiale.

I *data warehouse* sono sistemi strutturati come "magazzini" di dati preorganizzati, integrati e dinamici che, filtrati e analizzati da appositi sistemi informatici,

[40] Per un caso di parziale concretizzazione di tale rischio si rimanda al caso *Loomis*, v. *supra* nota n. 6.

permettono di produrre dei rapporti conoscitivi utili per supportare i processi decisionali. I sistemi tradizionali di raccolta e conservazione dei dati hanno il solo scopo di automatizzare la memorizzazione e la ricerca degli stessi, mentre mediante i *data warehouse* è possibile trasformare i dati in informazioni strategiche.

Un ulteriore sviluppo nella tecnica informatica ha permesso di elaborare dei sistemi ancora più avanzati, quali i *data lake*. Si tratta di strutture informatiche caratterizzate da una maggiore flessibilità, poiché permettono di immagazzinare dati direttamente nel loro formato nativo senza necessità di una preventiva strutturazione nelle rigide classi in cui sono organizzati i *data warehouse*. Il vantaggio dei *data lake* è quello di poter organizzare i dati direttamente durante la fase dell'analisi specifica che si sta conducendo, così adottando la forma di aggregazione più adatta a seconda delle specifiche esigenze di analisi.

L'importanza di tale avanzamento tecnologico è stata percepita anche a livello nazionale, tanto che sono state previste nell'ambito del *recovery fund* e del P.N.R.R. la realizzazione di un «Sistema di Controllo di Gestione del processo civile e del processo penale» e di un «Sistema avanzato di statistica giudiziaria civile e penale», la cui originaria attuazione era prevista entro l'aprile 2025. Dalle ultime notizie a disposizione, derivante dalla «Relazione del Ministero sull'amministrazione della giustizia anno 2024», presentato in occasione dell'inaugurazione dell'anno giudiziario 2025, si evince l'intenzione di creare un *data lake*, composto da sei sistemi, tra cui uno di statistiche avanzate su processi civili e penali, con termine massimo di realizzazione indicato nel 30.06.2026 (M1C1–154). Nel medesimo contesto si è data un'apertura anche alla possibilità di sfruttare l'IA per «automatizzare l'analisi dei dati non strutturati per identificare *trend* e anomalie e allo sviluppo di sistemi predittivi per ottimizzare le risorse e migliorare la pianificazione strategica»[41], prospettandosi, in attesa di verificare le effettive modalità di realizzazioni di tali progetti, buoni margini di impiego dell'intelligenza artificiale nel sistema di gestione delle statistiche giudiziarie penali.

10. *La regolamentazione delle statistiche processuali penali*

L'attenzione per il tema della raccolta e della gestione dei dati e delle informazioni, nonché dei *big data* – fondamentale per garantire il funzionamento dei sistemi di IA – è in forte crescita; ne è prova la recente adozione del *Data Act* in sede unionale (Reg. UE/2023/2854), incentrato sul tema dell'accesso equo ai dati e al loro utilizzo.

[41] Risultano di particolare interesse le pp. 167-168, 524-527 e 556-557 della Relazione.

Si tratta di un atto volto a regolamentare il mercato europeo dei dati, chiarendo chi può creare valore dai dati e a quali condizioni, nonché stabilendo norme chiare ed eque per l'accesso e l'utilizzo delle informazioni quantitative all'interno dell'economia europea dei dati. Appare evidente che allo stato l'interesse è focalizzato più sull'aspetto economico connesso allo sfruttamento dei dati e meno alla regolamentazione specifica e unica a livello europei delle modalità di raccolta dei dati processuali penali.

Con specifico riferimento alla situazione italiana, il sistema attuale di raccolta dei dati processuali penali è affidato al Ministero della giustizia dagli articoli 2, 3, 4 e 6 del D.Lgs. 322/1989 e, in particolare, dal Decreto del Presidente del Consiglio dei ministri del 15.06.2015, n. 84, modificato e integrato dal Decreto del Presidente del Consiglio dei ministri del 22.04.2022, n. 54. La raccolta e conservazione dei dati processuali penali è ulteriormente demandata alla Direzione Generale di Statistica del Ministero della giustizia.

Quanto alle modalità di raccolta e accesso ai dati, la norma di riferimento è il «Regolamento concernente la tipologia e le modalità di estrazione, raccolta e trasmissione dei dati statistici dell'Amministrazione di cui al D.M. 102/2012», che individua i soggetti e le modalità di accesso alle statistiche processuali penali. Pur trattandosi di dati tendenzialmente pubblici, salva l'esigenza di tutelare i dati sensibili previa anonimizzazione, risulta molto difficile riuscire ad accedervi.

Alla luce delle considerazioni svolte nel paragrafo precedente in punto di incompletezza dei dati raccolti, a cui si aggiunga la circostanza che le informazioni contenute nelle banche date giuridiche sono per lo più ad accesso limitato, appare evidente che il nostro è un sistema alquanto complesso che non tiene attualmente in considerazione le esigenze di un mondo che sta vivendo una rivoluzione, in cui il ruolo dei dati e la loro accessibilità è sempre più centrale. Ne consegue la necessità di adeguare il sistema e la sua regolamentazione alle nuove sfide poste dall'intelligenza artificiale.

11. *Conclusioni*

All'esito di questo contributo ritengo utile riprendere alcuni concetti emersi nei paragrafi precedenti.

In primo luogo, nonostante ci troviamo agli albori dell'applicazione dei sistemi IA alla giustizia penale (e agli ambiti connessi) sono già molteplici gli impieghi possibili o immaginabili per migliorare in termini di efficienza e qualità il processo penale. Purtuttavia, a grandi possibili vantaggi si accompagnano importanti potenziali rischi di lesioni dei diritti fondamentali. Per tale ragione l'Unione europea con l'*AI Act* ha posto dei paletti generali allo sviluppo e all'utilizzo di sistemi di IA nell'amministrazione della giustizia e nei settori connessi. In meri-

to, occorrerà capire se l'ancora per molti aspetti criptico testo del Regolamento UE 2024/1689 sia sufficiente a ordinare lo straripante sviluppo degli impieghi dell'IA nel processo penale.

A una tale dinamicità normativa in sede di utilizzabilità dell'IA in ambito processuale penale non è ancora seguita altrettanta attenzione per la regolamentazione delle statistiche giudiziarie penali, che vengono ancora raccolte in modo poco efficiente e risultano di difficile accesso.

Appare evidente quindi lo scostamento tra i due settori, che si auspica venga colmato nel medio-breve periodo, anche al fine di garantire il miglior utilizzo possibile dei sistemi IA in ambito processuale penale, possibile solo attraverso l'analisi di *set* di dati completi e precisi.

In caso contrario, ritengo fondato il timore che anche la più avanzata e perfetta macchina incentrata sullo sfruttamento dell'intelligenza artificiale applicata al processo penale (definita all'interno dei limiti tecnici e giuridici sopra tracciati che ne delimitano la carreggiata) lanciata con grande entusiasmo verso l'auspicato radioso futuro del miglioramento del sistema penale, possa rivelarsi non in grado di mantenere le grandi attese create a causa della carenza di un idoneo propellente, consistente in un apparato ampio, completo, dettagliato e adeguato di dati e informazioni.

La trasparenza alla prova dell'azione amministrativa algoritmica

di **Andrea Tronci**

1. *Introduzione: attività amministrativa e IA*

Ormai da tempo la pubblica amministrazione ricorre all'utilizzo della tecnologia digitale. L'inesorabile ed inevitabile trasformazione tecnologica che caratterizza la contemporaneità ha reso necessario che l'amministrazione mettesse in atto un processo di digitalizzazione dotandosi di strumenti informatici e nuove tecnologie, non solo per realizzare un mero passaggio dal cartaceo al digitale, ma anche e soprattutto per orientare l'organizzazione e l'azione dell'amministrazione verso una maggiore efficienza, efficacia ed economicità.

Le potenzialità dell'avvio di un processo di digitalizzazione da parte della pubblica amministrazione erano state già colte negli anni '70, in cui si esortava l'utilizzo di elaboratori elettronici nel riordino dell'amministrazione dello Stato[1]. Nondimeno, fin da quegli stessi anni si sottolineava il ritardo nella traduzione dell'innovazione tecnologica in innovazione amministrativa[2]. Si fa riferimento, in particolare, al noto *Rapporto sui principali problemi dell'amministrazione dello Stato* redatto da Giannini nel 1979, all'interno del quale l'autore già evidenzia-

---

[1] Cfr. A. Predieri, *Gli elaboratori elettronici nell'amministrazione dello Stato*, Bologna, 1971; G. Duni, *L'utilizzabilità delle tecniche elettroniche nell'emanazione degli atti e nei procedimenti amministrativi. Spunto per una teoria dell'atto amministrativo emanato nella forma elettronica*, in *Riv. amm. repubbl. it.,* 1978, 407 ss.

[2] Così, E. Carloni, *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni*, in *Dir. Pub.*, 2, 2019, p. 366.

va come rispetto all'informatizzazione dell'amministrazione si fosse perduto un decennio.

A distanza di quasi mezzo secolo dalle suddette considerazioni, si riscontra un quadro normativo articolato, che ha iniziato a prender forma con l'introduzione di discipline settoriali relative all'ammissione dei supporti informatici accanto a quelli cartacei[3], per poi proseguire con rilevanti interventi di impatto sistematico.

Tra questi si annovera l'inserimento nella legge 241/90 sul procedimento amministrativo dell'art. 3 bis, il quale stabilisce una diretta connessione tra l'efficienza dell'amministrazione e l'utilizzo della tecnologia[4], nonché l'emanazione del d.lgs. 82/2005, intitolato «*Codice della Amministrazione Digitale*»[5], più volte riformato negli anni successivi alla sua emanazione[6]. Con l'introduzione di questo Codice il legislatore ha delineato una disciplina unitaria del processo di digitalizzazione della pubblica amministrazione, secondo la quale quest'ultima agisce, e si organizza per agire, al fine di esercitare funzioni amministrative e prestare servizi pubblici tramite delle ICT (*Information and Communication Technology*), ovvero con le modalità rese possibili dalle tecnologie dell'informazione e della comunicazione[7].

Se, dunque, sul piano astratto dell'attività normativa emerge una significativa evoluzione della disciplina in materia di digitalizzazione, non può dirsi lo stesso sul piano della sua concreta applicazione, caratterizzata tradizionalmente da uno

---

[3] L. Torchia, *Lo stato digitale. Una introduzione*, Bologna, 2023, p. 97.

[4] Attualmente, a seguito del d.l. 76/2020, non si prevede più semplicemente che le amministrazioni pubbliche «*incentivano l'uso della telematica*», ma si dispone che: «*Per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche agiscono mediante strumenti informatici e telematici, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati*».

[5] Sulla disciplina del Codice, *ex multis*, G. Duni, *L'amministrazione digitale. Il diritto amministrativo nell'evoluzione telematica*, Milano, 2008; I. Macrì, U. Macrì, G. Pontevolpe, *Il nuovo Codice dell'amministrazione digitale*, Milano, 2011; R. Arcella e G. Vitrani, *Il Codice dell'Amministrazione Digitale. Disciplina e applicazioni*, Milano, 2024.

[6] La necessità del legislatore di intervenire ripetutamente sulla disciplina contenuta nel C.A.D. deriva tanto dalla celere e continua evoluzione degli strumenti tecnologici, quanto dalla volontà di incentivare in maniera crescente il percorso di digitalizzazione della pubblica amministrazione al fine di renderne più semplice ed efficiente l'attività. Cfr. B. Carotti, *Il correttivo del codice dell'amministrazione digitale: una meta-riforma*, in *Giorn. Dir. Amm.*, 2, 2018, p. 131 ss.

[7] Così, S. Rossa, *Contributo allo studio delle funzioni amministrative digitali. Il processo di digitalizzazione della Pubblica Amministrazione e il ruolo dei dati aperti*, Milano, 2021, p. 59 ss.

sviluppo lento e non omogeneo del sistema amministrativo[8], dovuto, generalmente, ad una strutturale carenza di capitale economico ed umano necessario per il compimento di una transizione digitale[9].

Proprio al fine di far fronte a tali deficit, il PNRR (Piano nazionale di ripresa e resilienza) destina ingenti risorse economiche[10] alla transizione digitale, con l'obiettivo di «trasformare in profondità la pubblica amministrazione attraverso una strategia centrata sulla digitalizzazione»[11]. A tal fine, la digitalizzazione non deve più caratterizzarsi come una mera operazione di facciata con cui si trasferiscono i fogli di carta dentro i computer[12], ma piuttosto essa deve consistere nella dotazione alle pubbliche amministrazioni degli strumenti materiali ed immateriali essenziali per governare la nuova dimensione tecnologica fondata sull'utilizzo di algoritmi di intelligenza artificiale.

La quarta rivoluzione industriale[13] ha infatti aperto le porte ad una nuova fase di digitalizzazione caratterizzata dallo sviluppo di modelli algoritmici «intelligenti», non solo capaci di elaborare conoscenze preesistenti ma anche di apprendere, contribuendo a creare o modificare il modello su cui si basa il loro funzionamento[14], utilizzabili dalla pubblica amministrazione non unicamente per lo svolgimento di attività di archiviazione o comunicazione, bensì anche per attività decisorie.

---

[8] Appaiono emblematiche sul punto le parole pronunciate nel 2018 dall'ex Ministra per la pubblica amministrazione, Giulia Bongiorno, in occasione dell'EY Digital Summit: «*Negli anni passati si è sempre detto che la trasformazione digitale era già avvenuta e che praticamente dovevamo soltanto esultare. Invece io mi sono insediata da 10 mesi e posso dire che siamo all'anno zero*», riportate da E. Carloni, *Algoritmi su carta,* cit., p. 365.

[9] Sul punto, diffusamente, E. Carloni, *Algoritmi su carta,* cit., p. 368 ss.; B. Marchetti, *L'amministrazione digitale*, in *Enc. Dir.*, *I tematici*, *Funzioni amministrative*, diretto da B.G. Mattarella e M. Ramajoli, Milano, 2022.

[10] Il 27% delle risorse del PNRR sono dedicate alla transizione digitale, com'è espressamente indicato a p. 16 del PNRR, consultabile in *www.governo.it*.

[11] Così, Missione 1, Componente 1del PNRR, cit., p. 83. Per un'analisi degli obiettivi e delle prospettive poste dal PNRR in relazione alla transizione digitale della pubblica amministrazione cfr. D.U. Galetta, *Transizione digitale e diritto ad una buona amministrazione: fra prospettive aperte per le Pubbliche Amministrazioni dal Piano Nazionale di Ripresa e Resilienza e problemi ancora da affrontare,* in *www.federalismi.it.*

[12] Così, F. Caio, *Lo Stato del digitale*, Padova, 2014, p. 7.

[13] Sul punto si rinvia a K. Schwab, *La quarta rivoluzione industriale*, Milano, 2016; P. Bianchi, *4.0 La nuova rivoluzione industriale,* Bologna, 2018.

[14] G. Sartor, *L'intelligenza artificiale e il diritto*, Torino, 2022, p. 10.

Si delinea così una *species* del più ampio *genus* dell'amministrazione digitale, definibile come *amministrazione algoritmica*[15], la quale non deve però considerarsi dotata di un nuovo tipo di potere amministrativo privo di principi e regole. Al contrario, partendo dal presupposto che l'attività amministrativa algoritmica è retta dai medesimi principi che regolano l'esercizio del tradizionale potere amministrativo, pena un'antistorica ed incostituzionale immunità che caratterizzava il diritto amministrativo del passato[16], questo contributo si pone l'obiettivo di indagare come tali principi si adattino concretamente allo svolgimento dell'attività amministrativa compiuta mediante il ricorso ad algoritmi di intelligenza artificiale.

In particolare, prendendo le mosse da una breve disamina dei diversi modelli algoritmici di intelligenza artificiale, si analizzerà come il principio di trasparenza, inteso quale conoscibilità e comprensibilità dell'azione amministrativa, si declini in riferimento all'azione amministrativa algoritmica attraverso gli istituti dell'accesso agli atti del procedimento e della motivazione del provvedimento amministrativo.

2. *Algoritmi ed intelligenza artificiale*

Come anticipato, al fine di comprendere le problematiche e le sfide che derivano dall'utilizzo di algoritmi di intelligenza artificiale nel compimento dell'attività amministrativa, appare utile soffermarsi, seppur sinteticamente e senza pretesa di esaustività sul piano tecnico-informatico, sulla nozione di algoritmo e di intelligenza artificiale.

È bene infatti chiarire, fin da subito, che la nozione di algoritmo rappresenta un'ampia categoria in cui sono ricompresi anche i sistemi di intelligenza artificiale.

Nello specifico, si può definire l'algoritmo come una procedura di calcolo, che opera sulla base di un insieme di dati precisamente forniti, che consiste nell'esecuzione di una serie ordinata e finita di istruzioni volte a trovare una soluzione al problema posto[17].

---

[15] A. Simoncini, *Amministrazione digitale algoritmica. Il quadro costituzionale*, in *Il Diritto dell'Amministrazione Pubblica digitale*, a cura di R.C. Perin e D.U. Galetta, Torino, 2020, p. 5.

[16] Così, condivisibilmente, L. Torchia, *Lo stato digitale*, cit., p. 110.

[17] L. Edwards e M. Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably not the Remedy you are Looking for*, in *Duke Law & Technology Review*, 16, p. 18 ss; K. Yeung, *Algorithmic regulation: a critical interrogation*, in *Regulation & Governance*, 12, p. 505 ss. Sono individuabili nella letteratura scientifica internazionale anche ulteriori definizioni, come in R. Benítez, G. Escudero, S. Kanaan e D.M. Rodó, *Inteligencia*

Tali procedure di calcolo possono esser caratterizzate da un diverso grado di complessità. Invero, alcuni algoritmi sono definiti «semplici», come il cd. algoritmo di Euclide, che ha la funzione di trovare il massimo comune divisore tra due numeri[18], altri sono definiti «complessi», poiché capaci di svolgere un ragionamento inferenziale (cd. algoritmi deterministici o condizionali[19]) o di apprendere (cd. algoritmi di *machine learning*[20]) mediante l'elaborazione di un'ingente mole di dati.

Più nel dettaglio, gli algoritmi deterministici elaborano i dati che gli sono forniti, i quali formano il suo *data set*, in base a delle regole (informatiche) predeterminate che rappresentano il codice sorgente, così che al ricorrere di una determinata condizione esegua un certo comando. Da ciò deriva che a parità di dati d'ingresso, un algoritmo deterministico seguirà un solo possibile percorso e produrrà sempre un determinato risultato (*if this, than that*)[21].

Gli algoritmi di *machine learning* (*ML*), invece, sono caratterizzati da un modello matematico maggiormente articolato in grado di creare o modificare la regola informatica in base alla quale vengono elaborati i dati. In altre parole,

---

artificial avanzada. Barcellona, 2013, secondo cui l'algoritmo sarebbe la procedura per trovare una soluzione ad un problema riducendolo ad un insieme di regole, o, come in R. Hill, *What an algorithm is*, in *Philosophy & Technology*, 29 (1), p.35 ss., secondo cui l'algoritmo sarebbe un sistema finito, astratto, efficace, dotato di una struttura di controllo composta, imperativamente dato, che realizza un determinato scopo in base a determinate disposizioni. Anche la dottrina giuridica italiana si è cimentata nel delineare i tratti caratteristici ed essenziali degli algoritmi. Sul punto, cfr. R. Borruso, *Computer e diritto*, 1, Milano, 1988, p. 183 ss., dove si afferma che «*l'algoritmo è una successione finita di passi (intesi come "istruzioni") ognuno dei quali definito ed eseguibile, che opera sui dati producendo risultati*», oppure A. Masucci, *L'Atto amministrativo informatico. Primi lineamenti di una ricostruzione*, Napoli, 1993, che definisce l'algoritmo «*un certo processo di ragionamento usato per la risoluzione di un problema*».

[18] G. Sartor, *L'intelligenza artificiale*, cit., p. 9.

[19] Tali algoritmi sono definiti da alcuni autori «condizionali» al fine di indicare come essi siano basati su dei «*conditional statements…which…allow a program to execute diffent code depending on what happens as the program runs*», Cfr. M.J. Johnson, *A Concise Introduction to Programming in Python*, CRC Press, 2018, p. 23. L'espressione, invece, «deterministico» viene utilizzata per indicare il fatto che all'introduzione di determinati *input*, si avrà sempre un determinato *output*, che sarà dunque prevedibile. Cfr. E. Peres, *Che cosa sono gli algoritmi*, Firenze, 2020.

[20] Per un'analisi approfondita degli algoritmi *ML*, cfr. C. Coglianese e D. Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, in *www.scholarship.law.upenn.edu*, p. 1156 ss.

[21] F. Chollet, *Deep learning with Python*, 2, New York, 2021, p. 2; M. Peruzzi, *Intelligenza artificiale e tecniche di tutela*, in *Lav. dir.*, 3, 2022, p. 543 ss.

seguendo un processo induttivo che parte dall'osservazione delle informazioni immesse o raccolte durante l'addestramento, il sistema impara od ottimizza la regola informatica che garantisce, in termini probabilistici, la migliore utilità attesa per lo svolgimento di un determinato compito[22].

Siffatta capacità di apprendimento dell'algoritmo di *ML* rende complesso comprendere l'iter logico seguito da esso per giungere ad un determinato risultato, non essendo immediatamente ricavabile come l'algoritmo abbia messo in relazione i vari dati e quali siano stati i fattori determinanti per produrre una certa decisione[23]. Per tale ragione, gli algoritmi di *ML* si ritengono caratterizzati da un'intrinseca opacità e vengono descritti come capaci trasformare degli *inputs* in *outputs* attraverso una scatola nera (cd. *black box*) che può non rendere possibile comprendere come questa trasformazione sia avvenuta[24].

Come si vedrà più avanti, il grado di opacità dell'algoritmo e, di conseguenza, di *explainability* dello stesso, varia a seconda del tipo di addestramento utilizzato[25]

---

[22] N. Abriani e G. Schneider, *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corptech*, Bologna, 2021, p. 23 ss.; F. Chollet, *Deep learning*, cit. p. 3 ss.

[23] C. Coglianese e D. Lehr, *Regulating by Robot*, cit., p. 1159, evidenzia: «*The user of an algorithm cannot really discern which particular relationships between variables factor into the algorithm's classification, or at which point in the algorithm they do, nor can the user determine how exactly the algorithm puts together various relationships to yield its classifications. For this reason, machine-learning algorithms are often described as transforming inputs to outputs through a black box*».

[24] Sul concetto di *black box* la letteratura scientifica è ampia. Si segnalano in particolare, F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Londra, 2015; A. Cerrillo, *How can we open the black box of public administration?*, in *Revista catalana de dret public*, 58, 2019, p. 13 ss.; Y. Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, in *Harvard Journal of Law & Technology*, 2, 2018, p. 901 ss.; D. Castelvecchi, *Can We Open the Black Box of AI?*, in *Nature*, 538, 2016, p. 21 ss.

[25] Le modalità di addestramento dell'algoritmo di *ML* possono esser varie. In particolare, l'addestramento può essere: supervisionato (viene fornito all'algoritmo un ampio insieme di esempi, ciascuno dei quali combina la descrizione di un caso alla risposta corretta dello stesso, in modo tale che si possa costruire un modello generale, applicabile anche a casi nuovi parzialmente diversi da quelli presenti nell' insieme di addestramento); per rinforzo (in cui la fase di addestramento avviene senza alcun istruttore poiché l'algoritmo apprende dai risultati delle proprie azioni, da cui possono derivare delle ricompense o delle penalità); non supervisionato (l'algoritmo apprende senza ricevere istruzioni da fonti esterne, come avviene in caso di apprendimento con supervisione, o dai risultati della propria attività, come avviene nel caso di apprendimento per rinforzo). Cfr. G. Sartor, *L'intelligenza artificiale*, cit., p. 46 ss.

e, soprattutto, dell'eventuale ricorso a reti neurali artificiali[26] (cd. sistemi di *deep learning*).

Per rete neurale si intende un programma di *machine learning* che prende decisioni in modo simile al cervello umano, utilizzando processi che imitano il modo in cui i neuroni biologici lavorano insieme per identificare fenomeni, pesare le opzioni e arrivare alle conclusioni.

Più nello specifico, si tratta di modelli di calcolo organizzati in diversi livelli di unità di elaborazione (c.d. «neuroni artificiali/nodi») che partecipano al processo computazionale e che sono tra loro interconnessi: l'*output* di ogni nodo, al ricorrere di determinate condizioni, viene trasmesso al nodo successivo, determinando una stratificazione dell'elaborazione. Questa stratificazione indica la profondità delle reti e dell'apprendimento[27].

Se da un lato sono conoscibili con certezza i dati di ingresso su cui opera l'algoritmo di *deep learning*, e certamente l'*output* che esso fornisce, dall'altro lato non può esser ricostruito con esattezza il percorso decisionale seguito da questa tipologia di IA per giungere al risultato prodotto, così manifestandosi nella sua pienezza il *black box problem*.

Riportate le sfaccettature essenziali della nozione di algoritmo, non resta che chiarire cosa debba intendersi per sistema di intelligenza artificiale (IA). Secondo la letteratura scientifica, la locuzione «intelligenza artificiale» indica una classe di programmi informatici progettati per risolvere problemi che richiedono ragionamenti inferenziali, processi decisionali basati su informazioni incomplete o incerte, nonché attività di classificazione, ottimizzazione, percezione o apprendimento[28].

Da questa definizione appare chiaro come i sistemi di intelligenza artificiale, al pari di ogni sistema informatico, siano basati su un algoritmo, il quale tuttavia deve possedere precise caratteristiche, consistenti nella capacità di compiere ragionamenti inferenziali o di apprendere in autonomia. Emerge dunque, come evidenziato in apertura di questo paragrafo, la maggior ampiezza della categoria di algoritmo, in quanto possono costituire sistemi di intelligenza artificiale esclusivamente algoritmi complessi, ossia tanto deterministici quanto di *machine learning*.

---

[26] *Ex multis*, I. Goodfellow, Y. Bengio e A.Courville, *Deep learning*, Massachusetts, 2016; E. Charniak, *Introduction to Deep Learning*, Massachusetts, 2019.

[27] Cfr. M. Peruzzi, *Intelligenza artificiale*, cit., p. 545.

[28] Cfr. Y. Bathaee, *The artificial intelligence black box and the failure of intent and causation*, in *Harvard Journal of Law & Technology*, 31, 2, 2018, p. 898.

3. *La necessaria legalità dell'attività amministrativa algoritmica*

Dopo aver delineato la nozione e le tipologie più rilevanti di algoritmo, nonché dopo aver chiarito quando possa parlarsi di algoritmi di intelligenza artificiale, non resta che soffermarsi sull'individuazione dei principi giuridici che orientano l'attività amministrativa algoritmica.

Ciò si rende necessario, in particolar modo, laddove siffatti algoritmi siano utilizzati dalla pubblica amministrazione per adottare una decisione. Invero l'adozione di una decisione amministrativa, in quanto manifestazione dell'esercizio di pubblico potere, avviene a seguito del compimento di un procedimento amministrativo, il cui inizio, svolgimento e conclusione sono fondati sui principi indicati dall'art. 1 della legge 241/90[29].

Ne consegue allora l'esigenza di verificare come le tradizionali categorie concettuali rappresentate da questi principi siano in grado di adattarsi alle nuove problematiche poste dall'attività decisoria algoritmica della pubblica amministrazione[30], riservando particolare attenzione al principio di trasparenza e agli istituti con i quali esso si declina.

Tale questione può essere esplorata partendo da una disamina della giurisprudenza amministrativa recente, che ha già avuto modo di confrontarsi con le sfide conseguenti all'automatizzazione delle procedure decisionali.

Inizialmente la giurisprudenza assumeva una posizione fortemente restrittiva rispetto all'ammissibilità di una decisione algoritmica.

Precisamente, la giurisprudenza amministrativa, chiamata a pronunciarsi su una controversia sorta su dei provvedimenti di trasferimento o assegnazione di sede adottati nei confronti di alcuni docenti delle scuole pubbliche in base alle risultanze di un algoritmo deterministico[31], affermava drasticamente la natura

---

[29] Sui principi dell'attività amministrativa, cfr. Aa. V.v., *Principi e regole dell'azione amministrativa*, a cura di A. Sandulli, Milano, 2023.

[30] In quest'ottica, I.M. Delgado, *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi?*, in *Ist. Feder.*, 3, 2019, p. 659. Già relativamente all'atto amministrativo informatico ci si era interrogati sulla capacità dei tradizionali strumenti del diritto amministrativo di offrire adeguata tutela ai cittadini incisi dall'esercizio del potere. Sul punto, S. Puddu, *Contributo ad uno studio sull'anormalità dell'atto amministrativo informatico*, Napoli, 2006; F. Saitta, *Le patologie dell'atto amministrativo elettronico e il sindacato del giudice amministrativo*, in *Dir. econ.*, 2003, p. 615 ss.; A.G. Orofino, *La patologia dell'atto amministrativo elettronico: sindacato giurisdizionale e strumenti di tutela*, in *Foro Amm.*, 2002, p. 2256 ss.

[31] Invero esso operava in base a formule di calcolo lineari volte ad elaborare una significativa quantità dati di *input* forniti dagli interessati, secondo i criteri definiti dal Ministero, al fine di produrre, quale *output*, la graduatoria finale della procedura.

meramente strumentale dei dispositivi digitali all'interno del procedimento amministrativo[32].

Dopo che per diverso tempo si dava per scontato che il contenuto della decisione fosse frutto di un essere umano[33], nel momento in cui ci si è trovati dinanzi ad una decisione automatizzata, è emersa una reazione conservatrice e protezionista, non nuova nei confronti delle repentine innovazioni tecnologiche[34]. In particolare, si è statuita la centralità dell'uomo, in qualità di funzionario persona fisica, nella gestione del procedimento amministrativo, non demandabile ad un «impersonale algoritmo» al fine di assicurare il rispetto delle guarentigie procedimentali della partecipazione e della motivazione della decisione amministrativa.

Pertanto, in questo scenario, le nuove tecnologie potevano esser utilizzate nell'ambito dell'attività procedimentale in un'ottica esclusivamente ausiliaria e giammai sostitutiva.

Timide aperture si sono potute scorgere, invece, all'interno dei primi interventi del Consiglio di Stato, in cui si ammetteva il ricorso ad algoritmi per lo svolgimento di: «procedure seriali o standardizzate, implicanti l'elaborazione di ingenti quantità di istanze e caratterizzate dall'acquisizione di dati certi ed oggettivamente comprovabili e dall'assenza di ogni apprezzamento discrezionale»[35]. In

---

[32] Cfr. T.A.R. Lazio, 27 maggio 2019, n. 6606, con nota di S.S. Di Veroli, *Il TAR e il Consiglio di Stato in disaccordo sulla querelle dell'utilizzo dell'algoritmo nel meccanismo decisionale*, in *www.dirittodiinternet.it*. Per alcune riflessioni sulla decisione, S. Civitarese Matteucci, *«Umano troppo umano». Decisioni amministrative automatizzate e principio di legalità*, in *Dir. pub.*, 1, 2019.

[33] G. Carullo, *Decisione amministrativa e intelligenza artificiale*, in *Dir. informaz. informat.,* 3, 2021, p. 431.

[34] R. Cavallo Perin, *Ragionando come se la digitalizzazione fosse data*, in *Dir. amm.*, 2, 2020, pp. 313-314.

[35] Cons. Stato, 8 aprile 2019, n. 2270, con nota di V. Canalini, *L'algoritmo come «atto amministrativo informatico» e il sindacato del giudice*, in *Giorn. Dir. amm.*, 2019, 6, p. 781 ss. Già, in un'ottica più generale, Cons. Stato, 7 febbraio 1995, n. 152, segnalava l'opportunità di ricorrere a «*procedure informatizzate*» nello svolgimento dell'attività amministrativa: «[…] *per la maggiore oggettività ed imparzialità che la macchina può assicurare, specialmente nello svolgimento di operazioni ripetitive, non essendo soggetta alla caduta della curva di attenzione riscontrabile nell'uomo dopo un certo tempo di applicazione allo stesso compito*», cfr. E. Carloni, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm*., 2, 2020, p. 285 ss. Emerge invece da Cons. Stato, Sez. V, 20 ottobre 2008, n. 5114, che il ricorso a procedure automatizzate ai fini del reclutamento dei pubblici impiegati è ritenuto dalla giurisprudenza amministrativa una pratica ampiamente diffusa. In argomento cfr. G. Piperata, *Semplificazione e digitalizzazione nelle recenti politiche di riforma della Pubblica Amministrazione italiana*, in F. Mastragostino, C. Tubertini, G. Piperata (a

questi casi, secondo tale orientamento, l'utilizzo di strumenti digitali che consentono di automatizzare il procedimento decisionale non deve esser stigmatizzato, bensì incoraggiato, poiché rispondente ai principi di efficienza ed efficacia ex art.1 l. 241/90, i quali rappresentano i corollari del principio di buon andamento di cui all'art. 97 della Costituzione.

Queste ultime considerazioni sono state riprese e valorizzate nel tempo dal Consiglio di Stato, la quale, già nell'arco dello stesso anno rispetto alla sentenza di cui sopra[36], ha ammesso il ricorso alla decisione algoritmica a prescindere dal carattere vincolato o meno della decisione amministrativa. Nel compiere questo decisivo passo in avanti, la giurisprudenza si è mostrata consapevole della necessità di dover alzare l'asticella della legalità: deve infatti scongiurarsi il rischio che l'ingresso degli algoritmi nel cuore della decisione pubblica[37] comporti un'elusione dei principi che conformano l'attività amministrativa[38]. All'opposto, munita di tale consapevolezza, la giurisprudenza ha saputo cogliere, da una parte, l'attualità di vecchie categorie per affrontare nuove problematiche[39], seppur con dei necessari adattamenti, e dall'altra parte, l'esigenza di coniare nuove guarentigie essenziali al cospetto delle nuove tecnologie.

In questa direzione, il Consiglio di Stato ha scolpito tre principi che raffigurano le colonne portanti della legalità dell'attività amministrativa algoritmica[40], rappresentate dalla trasparenza dell'algoritmo e della decisione che ne deriva[41],

---

cura di), *L'amministrazione che cambia. Fonti, regole e percorsi di una nuova stagione di riforme*, Bologna, 2016, p. 255.

[36] Cfr. Cons. St., 13 dicembre 2019, n. 8472, con nota di M. Iaselli, *Consiglio di Stato: non è da escludere l'adozione di un algoritmo in un procedimento amministrativo*, in *www.dirittodiinternet.it.*

[37] Così, E. Carloni, *I principi della legalità algoritmica*, cit. p. 287.

[38] D.U. Galetta, *Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia*, in *Riv. it. dir. pub. com.*, 3-4, 2020, p. 511.

[39] Cfr. I.M. Delgado, *Automazione, intelligenza artificiale*, cit., p. 643 ss.

[40] L'ammissibilità di una decisione amministrativa esclusivamente algoritmica, seppur condizionata all'individuazione e definizione dei principi chiave che devono guidare i procedimenti amministrativi automatizzati, è stata manifestata anche dal *Conseil constitutionnel* in occasione di una pronuncia (Décision nº 2018-765 DC du 12 juin 2018) sulla costituzionalità delle eccezioni legislative al generale divieto di utilizzare procedure automatizzate nei confronti dei singoli individui. Cfr. G. Marchianò, *La legalità algoritmica nella giurisprudenza amministrativa*, in *www.dirittodelleconomia.it*, p. 15.

[41] N. Diakopoulos, *Accountability, Transparency, and Alghorithms*, in M.D. Dubber, F. Pasquale, S. Das (a cura di), *The Oxford Handbook of Ethics of AI*, Oxford,

dalla riserva di umanità all'interno del procedimento algoritmico[42] e dalla non discriminazione algoritmica[43].

3.1 *L'importanza della trasparenza*

Come può notarsi, il primo dei principi sopra richiamati è quello della trasparenza.

Esso rappresenta un principio generale dell'azione amministrativa, come può ricavarsi dall'art. 1 l. 241/90, nonché dal Trattato di Lisbona secondo cui la trasparenza regola l'azione della Commissione europea (art. 11, c. 3) e di ciascuna istituzione, organo od organismo europeo (art. 15 ex articolo 255 del TCE).

Autorevole dottrina[44], cogliendo una marcata inafferrabilità di siffatto principio, che spesso appare «fatalmente poco tecnico»[45], si è dedicata all'individuazione del suo contenuto, tracciandone chiaramente i confini con l'attiguo principio di pubblicità.

Il richiamo effettuato dall'art.1 della legge sul procedimento amministrativo ai principi di pubblicità e trasparenza non può esser infatti considerato una semplice endiadi con scopo rafforzativo, poiché se da un lato la pubblicità è una mera

---

2020, p. 197 ss.; E. Carloni, *Le intelligenze artificiali nella pubblica amministrazione e la sfida della trasparenza*, in A. Lalli (a cura di), *L'amministrazione pubblica nell'era digitale*, Torino, 2022, p. 45 ss.; Id., *La trasparenza amministrativa e gli algoritmi*, in E. Belisario e G. Cassano (a cura di), *Intelligenza artificiale per la pubblica amministrazione. Principi e regole del procedimento amministrativo algoritmico*, Pisa, 2023, p. 219 ss.

[42] E. Mosqueira Rey, E.H. Pereira, D.A. Rìos, J.B. Bascaràn e A.F. Leal, *Human-in-the-loop machine learning: a state of the art*, in *Artficial Intelligence Review*, 2022, 56, p. 3005 ss.; G. Gallone, *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, Padova, 2023.

[43] C. Coglianese e D. Lehr, *Regulating by Robot*, cit., p. 1191 ss.; V. Molaschi, *Algoritmi e discriminazione*, in *Studi in onore di Carlo Emanuele Gallo*, Torino, I, 2023, p. 355 ss.

[44] R. Marrama, *La pubblica amministrazione tra trasparenza e riservatezza nell'organizzazione e nel procedimento amministrativo*, in *Dir. proc. amm.*, 1989, p. 416 ss.; F. Manganaro , *Evoluzione del principio di trasparenza amministrativa*, in Aa.Vv., *Scritti in memoria di Roberto Marrama*, Napoli, 2010, p. 3 ss. Più in generale sul principio di trasparenza, la letteratura è ampia. Si rinvia principalmente a R. Villata, *La trasparenza dell'azione amministrativa,* in *La disciplina generale del procedimento amministrativo (Atti del XXXII Convegno di studi di scienza dell'amministrazione, Varenna – Villa Monastero, 18-20 settembre 1986)*, Milano, 1989, p. 15 ss.; E. Carloni, *La "casa di vetro" e le riforme. Modelli e paradossi della trasparenza amministrativa*, in *Dir. pub.*, 2009, III, p. 779 ss.

[45] Così, R. Marrama, *La pubblica amministrazione*, cit., p. 418.

caratteristica dell'atto, dell'organizzazione o del procedimento che consiste nella sua conoscibilità, dall'altro lato la trasparenza è chiarezza e comprensibilità dell'azione amministrativa. In questo senso può considerarsi pubblico ma non trasparente l'atto regolarmente pubblicato sul sito internet istituzionale della pubblica amministrazione ma connotato da un contenuto oscuro e non comprensibile dai cittadini[46].

Il principio di trasparenza si presenta quindi come maggiormente complesso e articolato rispetto al principio di pubblicità, portando con sé l'aspirazione, tramite gli imperativi della chiarezza e della comprensibilità, di render l'amministrazione una casa di vetro[47], con l'obiettivo di realizzare un effettivo e diretto rapporto tra governanti e governati, così da consentire a questi ultimi una consapevole partecipazione all'operato dei pubblici poteri[48]. Tale obiettivo è perseguito e realizzato mediante una pluralità di istituti che sono espressione puntuale e concreta del principio di trasparenza, quali l'obbligo di motivazione del provvedimento amministrativo di cui all'art. 3 l. 241/90[49], nonché l'accesso civico disci-

---

[46] In questo senso cfr. anche S. Vaccari, *L'evoluzione del rapporto tra la Pubblica Amministrazione e le persone nel prisma dello sviluppo della «trasparenza amministrativa»*, in *Jus-online*, 2015, 3, pp. 7-8, dove si è sottolineato come: «*L'attività di pubblicizzare rimanda ad un'operazione di tipo statico consistente nella mera estrinsecazione di un complesso di conoscenze e di informazioni sulla base di obblighi di fonte legale. A contrario, il concetto di trasparenza, non equipollente all'accennata pubblicità, non può trovare un rapporto di identità nella mera ostensione al pubblico dei dati informativi, bensì partecipa di un elemento aggiuntivo, definibile come momento dinamico, legato a precise caratteristiche qualitative quali chiarezza, comprensibilità ed intelligibilità delle informazioni precedentemente pubblicate*».

[47] Questa celebre metafora si attribuisce a Filippo Turati che nel 1908, durante un discorso tenuto alla Camera di Deputati, affermava: «*Dove un superiore pubblico interesse non imponga un momentaneo segreto, la casa dell'amministrazione dovrebbe essere di vetro*».

[48] Cfr. R. Villata, *La trasparenza dell'azione amministrativa*, o. c. Sulla trasparenza ed il suo indissolubile legame con il principio democratico, cfr. N. Bobbio, *Il futuro della democrazia*, Torino, 1984, in cui si afferma che la trasparenza distingue gli ordinamenti democratici da quelli autoritari, nei quali il segreto è la regola e la conoscibilità l'eccezione. Un potere invisibile, infatti, è contrario della democrazia, in quanto solo un potere trasparente può esser democratico.

[49] T. Autieri, *La motivazione del provvedimento amministrativo: raccolta di dottrina, giurisprudenza e legislazione*, Padova, 2002; P. Minetti, *La motivazione dell'atto amministrativo*, Macerata, 2003; R. Villata e M. Ramajoli, *Il provvedimento amministrativo*, Torino, 2017, p. 182 ss.; E. Casetta, *Manuale di diritto amministrativo*, a cura di F. Fracchia, XXVI, p. 515 ss.

plinato dagli artt. 5 e ss. d.lgs. 33/2013[50] e l'accesso ai documenti amministrativi regolamentato dagli artt. 22 e ss. l. 241/90[51].

Se dunque, come appena visto, la trasparenza è sinonimo di conoscibilità e comprensibilità, si comprende il motivo per il quale questo principio, non casualmente a parere di chi scrive, è stato indicato per primo all'interno di quel 'trittico' di principi che orienta l'azione amministrativa algoritmica. Invero, l'amministrazione come casa di vetro si pone come naturale antagonista non solo dell'opacità che deriva dall'indubbia complessità degli algoritmi, che operano in base a modelli matematici non comprensibili agli occhi del comune cittadino, ma soprattutto di quella scatola nera (cd. *black box*) che intrinsecamente connota soprattutto gli algoritmi di *deep learning*, in cui l'opacità può trasformarsi in vera e propria oscurità nella misura in cui non sia ricostruibile la logica su cui si fonda la decisione algoritmica.

Il ruolo cruciale affidato alla trasparenza nell'amministrazione 4.0[52] induce questo principio e gli istituti mediante cui si manifesta a mostrare la sua pervasività e la sua adattabilità, rivelandosi capace di tutelare gli interessi cui è preposto anche al mutare dell'amministrazione e del contesto in cui opera[53].

In quest'ottica, la giurisprudenza amministrativa si è preoccupata, innanzitutto, di garantire la conoscibilità dell'algoritmo utilizzato nel procedimento amministrativo, valorizzando il contenuto dell'art. 41 della Carta europea dei diritti fondamentali[54], che impone alla Pubblica Amministrazione che intende

---

[50] D. U. Galetta, *Accesso civico e trasparenza della pubblica amministrazione alla luce delle (previste) modifiche alle disposizioni del d.lgs. n. 33/2013*, in *www.federalismi.it*; Id., *Accesso (civico) generalizzato ed esigenze di tutela dei dati personali ad un anno dall'entrata in vigore del Decreto FOIA: la trasparenza de"le vite degli altri"?*, in *www.federalismi.it*; A. Del Prete, *Criticità e prospettive per la disciplina del diritto di accesso generalizzato*, in *Nuove autonomie*, 3, 2017, p. 507 ss.

[51] F. Cuocolo, *Il diritto di accesso ai documenti amministrativi. presupposti costituzionali*, in *Quad. reg.*, 2004, p. 1041 ss.; E. Carloni, *Nuove prospettive della trasparenza amministrativa: dall'accesso ai documenti alla disponibilità delle informazioni*, in *Dir. pubbl.*, 2005, p. 573 ss.; A. Sandulli, *La casa dai vetri oscurati: i nuovi ostacoli all'accesso ai documenti*, in *Giorn. dir. amm.*, 2007, p. 669 ss.; N. Paolantonio, *L'accesso alla documentazione amministrativa*, in F. G. Scoca (a cura di), *Diritto Amministrativo*, Torino, 2014, p. 270 ss.

[52] Espressione utilizzata per indicare una pubblica amministrazione che si trova in una quarta fase di evoluzione determinata dalle innovazioni tecnologiche sviluppatesi con la Quarta rivoluzione industriale. Cfr. D.U. Galetta e J.G. Corvalàn, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *www.federalismi.it*.

[53] Cfr. E. Carloni, *Il paradigma trasparenza*, Bologna, 2022.

[54] Per una disamina della disposizione, cfr. D.U. Galetta, *Il diritto ad una buona*

adottare una decisione da cui può derivare un pregiudizio alla sfera giuridica di una persona, di adempiere l'obbligo di sentirla prima di agire, di consentirle l'accesso ai suoi archivi e documenti, ed, infine, di fornire le ragioni della propria decisione[55].

In particolare, qualificando l'algoritmo come un «atto amministrativo ad elaborazione elettronica»[56], si è riconosciuta al privato destinatario dell'esercizio del potere la possibilità di aver accesso, ex art. 22 l. 241/90, al linguaggio informatico sorgente (c.d. codice sorgente) del sistema algoritmico[57] e alle istruzioni tecniche relative al funzionamento dell'algoritmo.

Nondimeno, l'assimilazione dell'algoritmo ad un atto amministrativo non pare indispensabile al fine di consentire al privato destinatario della decisione automatizzata di accedere all'algoritmo.

Oltre ai dubbi sotto il profilo dogmatico di tale qualificazione giuridica[58], si vuole sottolineare come la sussunzione del software nella categoria dell'atto amministrativo si rivela, a ben guardare, un'operazione ermeneutica eccessiva e non necessaria rispetto al fine perseguito. Invero, l'art. 22, che apre la disciplina dell'accesso agli atti, non fornisce la nozione di atto o provvedimento amministrativo, ma solo quella di documento amministrativo. All'interno di questa nozione, stante la sua ampiezza, non è dubitabile che rientrino anche il codice sorgente e le istruzioni tecniche per l'utilizzo del software.

---

amministrazione europea come fonte di essenziali garanzie procedimentali nei confronti della Pubblica Amministrazione, in *Riv. it. dir. pub. com.*, 3, 2005, p. 819 ss.

[55] Cfr. Cons. St., 13 dicembre 2019, n. 8472, cit.

[56] Così, Cons. St., 8 aprile 2019, n. 2270, cit. Tale qualificazione dell'algoritmo è stata sostenuta anche in dottrina, seppur con diverse sfumature: U. Fantigrossi, *Automazione e pubblica amministrazione*, Bologna, 1993, ha definito il *software* come atto di natura provvedimentale; A. Usai, *Le prospettive di automazione delle decisioni amministrative in un sistema di teleamministrazione*, in *Dir. Inf.*, 1, 1993, p. 174, come atto interno; A. Boix Palop, *Los algoritmos son reglamentos: la necesidad de extender las garanti´as propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones*, in *Revista de Derecho Público: Teoría y Método*, 1, 2020, p. 223, come regolamento.

[57] La cui ostensibilità determina inevitabilmente delle frizioni con il diritto d'autore, salvo che l'algoritmo utilizzato non sia *open source*. Sulla questione cfr. F. Bravo, *Trasparenza del codice sorgente e decisioni automatizzate*, in *Dir. informaz. informat.*, 4, 2020, p. 693 ss.; M. Farina, *Intellectual property rights in the era of Italian "artificial" public decisions: time to collapse?*, in *Riv. it. informat. dir.*, 1, 2023, p. 127 ss.

[58] Sul punto, A.G. Orofino e G. Gallone, *L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione*, nota a Cons. St., 4 febbraio 2020, n. 881, in *Giur. it.*, 7, 2020, p. 1742 ss.

Pertanto, nel perseguire l'obiettivo di garantire la trasparenza sotto il profilo della conoscibilità, si ritiene maggiormente corretto, come già sostenuto da rilevante dottrina[59], riferirsi all'algoritmo come documento, e non come atto, amministrativo accessibile.

Come precedentemente evidenziato, la trasparenza non è solo conoscibilità, ma anche comprensibilità della decisione, soprattutto nei procedimenti amministrativi automatizzati. In tal senso, la disciplina di matrice europea contenuta nel GDPR[60], alla quale i giudici amministrativi riconoscono la valenza di normativa di carattere generale in materia di procedimenti 'robotizzati'[61], sancisce che, in caso di processo decisionale automatizzato, l'interessato dal trattamento dei dati deve avere conoscenza dell'esistenza di un processo decisionale automatizzato e deve anche poter aver accesso alle informazioni significative sulla logica utilizzata, nonché sull'importanza e le conseguenze previste dal trattamento[62].

Perciò per soddisfare le esigenze di trasparenza, non è sufficiente consentire solo l'accesso alle regole informatiche su cui si fonda l'operatività dell'algoritmo, per la cui comprensione sono necessarie delle conoscenze tecniche che vanno ben al di là del bagaglio di conoscenze del comune cittadino, ma è anche indispensabile che: «[…] la 'formula tecnica', che di fatto rappresenta l'algoritmo, sia corredata da spiegazioni che la traducano nella «regola giuridica» ad essa sottesa e che la rendano leggibile e comprensibile[63]».

Infine, trattandosi dell'utilizzo di tecnologie di intelligenza artificiale all'interno del procedimento decisionale, risulta indispensabile che la decisione algoritmica sia corredata da una motivazione[64] in grado di spiegare compiutamente

---

[59] A.G. Orofino e G. Gallone, *L'intelligenza artificiale*, cit., p. 1744.

[60] In generale, sul Reg. 679/2016, cfr. M. Goddard, *The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact*, in *International Journal of Market Research*, 59, 6, 2017, p. 703-705 ss.; C. J. Hoofnagle, B. van der Sloot e F. Z. Borgesius, *The European Union general data protection regulation: what it is and what it means*, in *Information & Communications Technology Law*, 28, 1, 2019, p. 65 ss.; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016; M.G. Stanzione, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Eur. dir. priv.*, 4, 2016, p. 1249 ss.

[61] Così, E. Carloni, *La trasparenza amministrativa*, cit., p. 222.

[62] Cfr. Regolamento 679/2016 (GDPR), art. 15, comma 1.

[63] Così, Cons. St., 4 febbraio 2020, n. 881, cit.

[64] Il cui contenuto varia, in termini di ampiezza e profondità argomentativa, a seconda del potere vincolato o discrezionale esercitato dall'amministrazione. Sul punto, G. Carullo, *Decisione amministrativa*, cit. p. 439 ss.

l'*output* prodotto dall'algoritmo e su cui si è fondata la decisione, in ossequio agli artt. 3 l. 241/90, nonché 41 CDFUE.

L'indicazione dei presupposti di fatto e delle ragioni di diritto su cui si fonda la decisione algoritmica, quale ulteriore declinazione del principio di trasparenza, non può considerarsi, secondo la giurisprudenza amministrativa, un mero adempimento formale discendente da una rigida e meccanica applicazione delle regole procedimentali della l. n. 241 del 1990[65]. Il dovere di motivazione assume in quest'ambito certamente rilievo sostanziale, la cui violazione costituisce di per sé un vizio tale da inficiare la decisione emanata poiché la giustificazione della decisione è essenziale a garantire la comprensibilità dell'azione amministrativa algoritmica[66].

4. *Primi fondamenti positivi dell'utilizzo pubblico dell'IA e la persistente attualità di un quesito: quale trasparenza per il* deep learning*?*

L'enucleazione dei principi compiuta dai giudici amministrativi, su cui si basa la legalità dell'azione amministrativa algoritmica, è stata fortemente valorizzata dal legislatore[67] nel nuovo codice dei contratti pubblici.

All'interno del d.lgs. 36/2023, nella parte dedicata alla digitalizzazione del ciclo di vita dei contratti pubblici – la quale contiene delle disposizioni che nel loro insieme mirano a modificare radicalmente la gestione delle procedure contrattuali pubbliche mediante la digitalizzazione di ogni fase della procedura di gara[68] – è inserita la prima norma di diritto positivo (art. 30) che disciplina l'utilizzo pubblico di soluzioni tecnologiche avanzate, tra cui i sistemi di intelligenza artificiale[69].

---

[65] Cfr. Cons. St., 13 dicembre 2019, n. 8472, cit.

[66] Cfr. Così, E. Carloni, *I principi della legalità algoritmica*, cit., p. 293; D.U. Galetta, *Algoritmi, procedimento amministrativo*, cit., p. 516.

[67] Sebbene sia doveroso sottolineare come la redazione del d.lgs. 36/2023 sia stata affidata ad una commissione operante presso il Consiglio di Stato, composta in misura prevalente da giudici amministrativi. Cfr. E. Carloni, *La trasparenza amministrativa*, cit., p. 225.

[68] Per un'analisi organica delle disposizioni relative alla digitalizzazione del ciclo di vita dei contratti pubblici, cfr. Aa. V.v., *La digitalizzazione dei contratti pubblici nel nuovo codice*, a cura di B. Marchetti e B.G. Mattarella, Torino, 2024.

[69] Per un'approfondita disamina dell'intero art. 30, cfr. G.F. Licata, *Intelligenza artificiale e contratti pubblici: problemi e prospettive*, in *www.ceridap.eu*; B. Marchetti, *L'impiego dell'intelligenza artificiale nell'attività contrattuale dell'amministrazione pubblica*, in B. Marchetti e B.G. Mattarella (a cura di), *La digitalizzazione dei contratti pubblici nel nuovo codice*, cit., p. 45.

Con particolare riferimento all'utilizzo di tale tecnologia nello svolgimento dell'attività decisoria, può notarsi come il legislatore, al comma 3 dell'art. 30, disponga chiaramente che le decisioni assunte mediante automazione devono rispettare i principi di conoscibilità e comprensibilità, nonché di non esclusività della decisione algoritmica e di non discriminazione algoritmica sanciti dalla giurisprudenza.

Come, tuttavia, ha sottolineato la più recente dottrina[70], i principi positivizzati dal legislatore nel nuovo codice, il cui valore sistematico o settoriale è discusso[71], sono stati enucleati dal giudice amministrativo nell'ambito di controversie che riguardavano l'utilizzo da parte della p.a. di algoritmi complessi esclusivamente deterministici.

Per questa ragione, è necessario interrogarsi sulla capacità di siffatti principi di porsi come colonne portanti dell'azione amministrativa algoritmica anche in caso di ricorso ad algoritmi fondati su sistemi di apprendimento automatico, soprattutto qualora essi siano implementati da reti neurali artificiali.

Dalla relazione illustrativa al Codice si ricava una risposta di segno pienamente positivo sul punto: l'art. 30 vien descritto come una norma che guarda ad un futuro prossimo in cui l'amministrazione, in base alla: «[…] disponibilità di grandi quantità di dati possa consentire l'addestramento di algoritmi di apprendimento da applicare alle procedure di gara più complesse»[72]. Non emergono quindi dubbi sulla volontà del legislatore di ammettere l'impiego di algoritmi di *ML* anche per finalità decisorie alle stesse condizioni previste per gli algoritmi deterministici.

Nondimeno, per rispondere compiutamente ad un tale interrogativo, pare doveroso compiere un'analisi maggiormente articolata[73] che miri ad esaminare come i principi della legalità algoritmica possano concretamente atteggiarsi, mediante gli istituti che di essi sono espressione ed attuazione, dinanzi agli algoritmi di *machine learning* e di *deep learning*, tenendo conto delle peculiarità e delle differenze, che già in questa sede si sono evidenziate, tra questi sistemi di intelligenza artificiale.

---

[70] B. Marchetti, *L'impiego dell'intelligenza artificiale*, cit., p. 55; E. Carloni, *Dalla legalità algoritmica alla legalità (dell'amministrazione) artificiale. Premesse ad uno studio*, in *Riv. it. informat. dir.*, 2, 2024, pp. 457-458.

[71] Cfr. E. Carloni, *La trasparenza amministrativa*, cit., p. 225.

[72] Così si ricava dalla Relazione illustrativa al d.lgs. 36/2023, consultabile su *www.giustiziaamministrativa.it.*, p. 48.

[73] Diversamente dall'approccio «*forse troppo semplicistico*» adottato dal legislatore. Così, E. Carloni, *Dalla legalità algoritmica*, cit., p. 458.

Volendosi soffermare sulla trasparenza algoritmica, intesa quale conoscibilità e comprensione della decisione, può tentarsi di affrontare la suddetta analisi verificando se gli istituti dell'accesso e della motivazione del provvedimento si atteggino diversamente a seconda del tipo di algoritmo utilizzato.

Relativamente al primo dei due istituti menzionati, rimane ferma la possibilità, oltre che la necessità, di consentire al privato destinatario dell'esercizio del potere amministrativo l'accesso all'algoritmo al di là della tipologia di algoritmo impiegata nell'emanazione della decisione, dovendosi render conoscibili: gli autori dell'algoritmo, il codice sorgente, le istruzioni tecniche relative al funzionamento dell'algoritmo, nonché, come evidenziato da autorevole dottrina[74], il *data set* utilizzato dal sistema di IA[75].

Diversamente, per ciò che concerne la motivazione del provvedimento, si ritiene che il contenuto di quest'ultima vari a seconda che si utilizzi un algoritmo di *ML* implementato o meno da reti neurali artificiali (cd. *deep learning).*

Invero, nel caso in cui si faccia ricorso a degli algoritmi di *machine learning* privi di reti neurali, che hanno compiuto un processo di apprendimento, per esempio, supervisionato[76], volto ad allenare l'algoritmo a generare un *output* in forma assimilabile al contenuto di un provvedimento amministrativo di umana fattura[77], è possibile realizzare una *transparency by design*[78]. Con questa espres-

---

[74] Così, R. Cavallo Perin, *Ragionando come se*, cit., p. 315. L'A. afferma che l'ostensione del *data set*, prevista dall'art. 15 GDPR, è posta: «*[…] a garanzia dei destinatari e dei controinteressati della decisione in sé considerata, ma anche al fine di un esercizio del diritto di cancellazione dei dati considerati non più attuali (art. 17, Reg. UE 679/2016) o del diritto di rettifica (art. 16, Reg. UE 679/2016), in entrambi i casi ad integrazione della casistica con dati ulteriori e 'significativi'*».

[75] Rimane ferma, peraltro, la conseguente problematica di compiere un equilibrato bilanciamento tra le esigenze poste a fondamento delle diverse tipologie di accesso e i diritti potenzialmente lesi dall'ostensione del documento (cfr. nt. 58), tenendo conto anche delle importanti indicazioni che possono ricavarsi dal comma 2 dell'art. 30 d.lgs. 36/2023, secondo cui le stazioni appaltanti o gli enti concedenti, nell'acquisto o sviluppo di sistemi di IA o blockchain, assicurano: «*[…] la disponibilità del codice sorgente, della relativa documentazione, nonché di ogni altro elemento utile a comprenderne le logiche di funzionamento*».

[76] Cfr. nt. 25.

[77] Come evidenziato da G. Carullo, *Decisione amministrativa*, cit., p. 444: «*Si pensi, ad esempio, ad un algoritmo basato sul machine learning allenato su milioni di valutazioni paesaggistiche al fine di produrre quale output una valutazione della compatibilità di determinati interventi sul territorio. Laddove un tale algoritmo venisse eseguito su di una nuova pratica, l'output dovrebbe essere un testo assimilabile alle precedenti valutazioni paesaggistiche, con i diversi contenuti specifici della fattispecie esaminata*».

[78] M. Peruzzi, *Intelligenza artificiale*, o. c.

sione si intende indicare la possibilità che l'algoritmo *ML* sia programmato in modo da poter formulare una motivazione della decisione automatizzata che, oltre a indicare le disposizioni giuridiche applicate, evidenzi quali siano stati i dati ritenuti rilevanti ai fini della decisione adottata[79]. In tal modo è possibile soddisfare i requisiti di legittimità del provvedimento sanciti dall'art. 3 l. 241/90 anche nei casi in cui la quantità di dati su cui opera l'IA di *machine learning* si rivela estremamente elevata[80].

Una siffatta *transparency by design* non può invece esser realizzata con riferimento agli algoritmi di *deep learning*, in cui la comprensibilità e l'esplicabilità degli *output*, a causa della presenza di reti neurali artificiali, non può esser garantita mediante una programmazione che assicuri *ex ante* la comprensibilità della decisione, potendo quest'ultima esser garantita solo in termini probabilistici attraverso tecniche di *explainability* applicabili *ex post* (*XAI*)[81].

Volendo fornire un esempio per maggiore chiarezza, tra i metodi *XAI* più diffusi può individuarsi il *perturbation-based method*, che si basa su una ripetuta mescolazione dei dati di entrata che compongono il *data set* su cui opera l'algoritmo volta a verificare se ed in che modo vari l'*output* prodotto, così da individuare, seppur in termini di probabilità statistica, quali siano i dati che sono stati ritenuti determinati per la risposta fornita dal sistema di IA[82].

Dunque, dinanzi a decisioni automatizzate adottate con algoritmi di *deep learning*, è indispensabile che l'unità organizzativa responsabile del procedimento utilizzi tali metodi di *explainability ex post* al fine di poter interpretare l'*output* prodotto dall'algoritmo e conseguentemente di indicare quali siano i presupposti di fatto e le ragioni di diritto probabilmente determinanti per l'adozione della decisione.

È bene evidenziare però che una probabile comprensibilità della decisione algoritmica adottata con algoritmi di *deep learning* possa esser raggiunta solamente qualora siano fornite ai funzionari amministrativi adeguate, compiute e puntuali informazioni da parte dei fornitori dei sistemi di IA, riguardo non solo i meccanismi di funzionamento di tali tecnologie, la cui conoscenza è essenziale per tutti i tipi di algoritmi, ma anche sui metodi di *XAI* che dovranno esser impiegati

---

[79] G. Carullo, *Decisione amministrativa*, cit., p. 446.

[80] G. Carullo, *Decisione amministrativa*, cit., p. 442.

[81] Si fa riferimento ai metodi di *Explainable AI – XAI*. Cfr. *ex multis*, W. Ding, M. Abdel, Basset, H. Hawash e A.M. Ali, *Explainability of artificial intelligence methods, applications and challenges: A comprehensive survey*, in *Information Sciences*, Amsterdam, 2022, p. 238 ss.

[82] Cfr. W. Ding, M. Abdel, Basset, H. Hawash e A.M. Ali, *Explainability of artificial intelligence*, cit., p. 249.

dall'unità organizzativa responsabile del procedimento per soddisfare i requisiti di legittimità del provvedimento richiesti dall'art. 3 l. 241/90.

In questa direzione, il recentissimo Reg. 1689/2024 (cd. *AI Act*), pone in capo ai fornitori dei sistemi di IA degli obblighi informativi, la cui intensità varia a seconda della finalità per cui l'algoritmo è utilizzato, che ne determina, secondo la normativa europea, la latitudine del rischio[83]. Appare particolarmente significativa, con riferimento alla necessità di fornire delle adeguate informazioni sui metodi di *XAI*, la disposizione prevista dall'art. 13, comma 3, lett. b), n. vii, in tema trasparenza e fornitura di informazioni ai *deployer*[84] per i sistemi di IA ad altro rischio, in cui si dispone che devono esser messe a disposizione: «se del caso, informazioni che consentano ai *deployer* di interpretare l'output del sistema di IA ad alto rischio e di usarlo in modo opportuno».

Tali obblighi informativi, nondimeno, risulterebbero delle armi spuntate laddove le unità organizzative responsabili dei procedimenti automatizzati, soprattutto in caso di ricorso ad algoritmi di *ML* implementati da reti neurali artificiali, non siano composte anche da specialisti informatici-digitali[85] e qualora i funzionari amministrativi non siano adeguatamente formati per comprendere le istruzioni d'uso fornite[86].

Infatti, al fine di realizzare compiutamente il processo di digitalizzazione in atto, è necessario che la pubblica amministrazione disponga, non soltanto delle avanzate risorse materiali tecnologiche, rappresentate dai contemporanei sistemi di intelligenza artificiale, ma bensì anche delle risorse umane, adeguatamente formate e professionalmente qualificate, indispensabili per poter utilizzare queste tecnologie in maniera conforme ai principi della legalità algoritmica.

Come già messo in luce, tuttavia, l'adempimento degli obblighi informativi e l'adeguamento del personale amministrativo rispetto ai livelli di competenze richiesti dall'attuale contesto tecnologico, rappresentano unicamente dei pre-

---

[83] Per una disamina generale del Regolamento europeo, cfr. G. Lo Sapio, *L'Artificial Intelligence Act e la prova di resistenza per la legalità algoritmica*, in *www.federalismi.it.*

[84] Ai sensi dell'*AI Act*, il *deployer* è: «[…] *qualsiasi persona fisica o giuridica, compresi un'autorità pubblica, un'agenzia o altro organismo, che utilizza un sistema di IA sotto la sua autorità, salvo nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale*».

[85] E. Carloni, *Dalla legalità algoritmica*, cit., pp. 461-462, sottolinea come: «*L'amministrazione artificiale richiede capacità di alto livello, non riducibili a "semplici" questioni di riqualificazione del personale: deve disporre di AI Talent*».

[86] Si riscontra già da diverso tempo la sensibilità dell'ordinamento verso l'esigenza di attuare delle politiche di formazione e riqualificazione del personale, come emerge dall'art. 13 C.A.D. e, più di recente, dall'art. 2, comma 4, del d.lgs. 36/2023.

supposti essenziali per garantire una trasparenza che, sotto il profilo della comprensibilità della decisione, può realizzarsi solo entro i margini della probabilità statistica per gli algoritmi di *deep learning*.

Pertanto, con l'obiettivo di rispondere, in conclusione, al quesito posto nel titolo di questo paragrafo, si evidenzia che il principio di trasparenza dinanzi ai sistemi di *deep learning* si rivela estremamente fragile. Ciò conduce a ritenere che la pubblica amministrazione non possa ricorrere all'utilizzo di tale tecnologia in ogni ambito dell'attività amministrativa, in quanto il grado di incertezza ineliminabile che la contraddistingue è incompatibile e perfino intollerabile rispetto ai diritti fondamentali con i quali il potere amministrativo può confrontarsi.

Emerge allora, al fine di individuare gli ambiti di applicazione dei sistemi di intelligenza artificiale, soprattutto se di *deep learning*, l'essenziale bisogno dell'adozione di un approccio *risk-based*, come mostrato dall'*AI Act*, che si orienti sulle coordinate tracciate dal principio di proporzionalità, avendo di mira l'intento di operare un ragionevole bilanciamento tra lo sviluppo tecnologico (e l'efficienza che da esso consegue) ed i principi su cui si fonda lo Stato di diritto, tra cui spicca la trasparenza del pubblico potere.

L'utilizzo dell'intelligenza artificiale nella fase dei controlli tributari: interesse statuale e diritti dei contribuenti

di **Francesca De Vincentiis**

1. *L'impatto dello sviluppo tecnologico nel settore del diritto tributario*

Il settore del diritto tributario, più di altri, da sempre subisce un potente impatto derivante dai cambiamenti del contesto economico e sociale, e ciò ragionevolmente perché si tratta di un settore caratterizzato dalla compresenza di interessi tanto rilevanti quanto antagonisti, stridenti tra loro e posti in un rapporto dialogico di costante tensione.

Il crescente spazio riservato al mondo digitale e la diffusione di strumenti inediti - come le valute virtuali, rappresentative di una ricchezza dematerializzata ed atipica - mettono a dura prova la resistenza dei principi sottesi al diritto tributario moderno, imponendo al legislatore una razionalizzazione del sistema normativo[1] che tenga in considerazione il significato più intimo dei principi regolatori della materia, primo fra tutti quello della capacità contributiva, così come cristallizzato, all'esito di un lungo *excursus* storico, nell'art. 53 della Costituzione.

Oltre a questo aspetto, però, meritevoli di autonoma considerazione sono le potenzialità in termini di efficientamento amministrativo che sono fornite all'amministrazione finanziaria dallo sviluppo tecnologico, potenzialmente in grado di dimezzare l'evasione fiscale italiana[2] attraverso strumenti innovativi, oltretutto poco dispendiosi sotto un profilo prettamente economico.

---

[1] Sul rapporto tra principi costituzionali e categorie tradizionali del diritto tributario con le nuove forme di ricchezza e le innovazioni tecnologiche si veda V. Mastroiacovo (a cura di), *Il diritto costituzionale tributario nella prospettiva del terzo millennio*, Torino, 2022.

[2] In questi termini si è espresso V. Visco (*Cosa insegna la e-fattura: la tecnologia*

Da tempo che l'amministrazione finanziaria si serve di strumenti informatici a supporto delle proprie attività di controllo, ma è solo in tempi recenti che si sta assistendo ad una significativa incidenza sui tradizionali schemi di attuazione dei tributi, grazie agli elevatissimi standards raggiunti dalla tecnica informatica, con conseguente sviluppo di uno specifico interesse dottrinario, giurisprudenziale e legislativo.

L'utilizzo di sistemi automatizzati è attualmente favorito anche dal progetto di riforme concordato con il Consiglio dell'Unione Europea per l'attuazione del Piano Nazionale di Ripresa e Resilienza (PNRR), comprendente l'estensione della dichiarazione precompilata ai soggetti passivi IVA, l'introduzione di strumenti di disincentivazione all'utilizzo di contanti, il potenziamento delle *cc.dd.* lettere di *compliance* e il completamento dell'infrastruttura di analisi del rischio di evasione.

In merito alla legittimità dell'impiego degli strumenti di intelligenza artificiale da parte della pubblica amministrazione imprescindibile rilevanza assumono i principi enucleati dal Consiglio di Stato nelle sentenze 2270 e 8472 del 2019, nelle quali viene ammesso l'utilizzo di procedure interamente automatizzate nell'ambito dello svolgimento sia di attività vincolate che discrezionali, a condizione però che l'impiego di dette procedure, ammesse perché funzionali all'implementazione dell'economicità e dell'efficienza amministrativa, non sia motivo di elusione dei principi ordinamentali e amministrativi fondamentali, ponendo quindi quale condizione necessaria ed imprescindibile la conoscibilità e la trasparenza del procedimento robotizzato[3].

---

dimezza l'evasione, in *Diritto e pratica tributaria*, n. 4/2019, p. 1671), secondo il quale *"le nuove tecnologie se utilizzate consapevolmente e coerentemente, potrebbero in pochi anni più che dimezzare l'evasione fiscale italiana"*. Per una panoramica dei possibili impieghi di strumenti di intelligenza artificiale nell'ambito della prevenzione e del contrasto all'evasione fiscale si rinvia a A. Contrino, *Digitalizzazione dell'amministrazione finanziaria e attuazione del rapporto tributario: questioni aperte e ipotesi di lavoro nella prospettiva dei principi generali*, in *Rivista di Diritto Tributario*, n. 2/2023, pp. 105 ss.; F. Paparella, *L'ausilio delle tecnologie digitali nella fase di attuazione dei tributi*, in *Rivista di Diritto Tributario*, n. 6/2022 pp. 617 ss.

[3] Il contributo fornito dalla giurisprudenza amministrativa all'impiego di sistemi di intelligenza artificiale nel peculiare settore del diritto tributario è efficacemente analizzato da F. Paparella, *Procedimento tributario, algoritmi e intelligenza artificiale*, in E. Marello e A. Contrino (a cura di), *La digitalizzazione dell'amministrazione finanziaria tra contrasto all'evasione e tutela dei diritti del contribuente*, vol. II, Milano, 2023, pp. 13 ss. Per l'Autore la differenza sostanziale tra l'impiego algoritmico nel diritto amministrativo e in quello tributario risiede nei limiti, giacché solo in quest'ultimo vi è la necessità di adottare regole che, conformi a norme primarie di tipo sostanziale e procedimentale, siano dirette ad impedire che la ponderazione degli interessi sia sottratta

Detti criteri - anche al fine di evitare un inutile anacronismo ed un dannoso arresto amministrativo - non possono che trovare applicazione anche nei confronti dell'amministrazione finanziaria e del suo *agere*, in particolar modo nella fase dei controlli tributari, che può rivelarsi un valido banco di prova per l'utilizzo dei sistemi di intelligenza artificiale.

Ecco, quindi, che l'Agenzia delle Entrate ha avviato un processo di ammodernamento delle proprie tecnologie diretto all'applicazione degli algoritmi di IA, così ingenerando svariati dubbi sulla compatibilità di un siffatto impiego con la tutela dei diritti riconosciuti ai contribuenti.

2. *L'impiego dell'intelligenza artificiale nella fase di attuazione dei tributi: l'analisi del rischio di evasione*

Nell'ambito della digitalizzazione dell'azione dell'amministrazione finanziaria, l'aspetto più interessante sembra coinvolgere la disciplina dell'analisi del rischio di evasione, nella quale l'impiego dell'intelligenza artificiale potrebbe rivelarsi centrale.

L'analisi del rischio di evasione, definibile come quell'insieme di tecniche, procedure e strumenti informatici utilizzati per l'individuazione dei contribuenti che presentano un elevato rischio fiscale - da intendersi quale rischio di operare o aver operato in violazione di norme tributarie o in contrasto con principi o finalità dell'ordinamento tributario[4] - si pone quale strumento ibrido che può fungere da ausilio sia in ottica preventiva, stimolando la *compliance*, che repressiva, coadiuvando i controlli degli uffici. Si tratta di uno strumento che, attraverso la selezione e l'individuazione dei soggetti più a rischio sui quali avviare verifiche più incisive, è destinato a fungere da filtro nello snellimento dell'attività dei funzionari, il cui ruolo direttivo e decisionale dovrebbe comunque essere conservato, a scapito di controlli interamente automatizzati.

La costruzione di un coerente ed efficace sistema di analisi del rischio necessita, da una parte, dell'istituzione, dell'implementazione e dell'interoperabilità

al legislatore per essere rimessa all'ente impositore. Sulle posizioni assunte dal Consiglio di Stato e sulla loro rilevanza in ambito fiscale si veda anche D. Conte, *Accertamento tributario e modelli predittivi del rischio di evasione fiscale: il ruolo dell'IA tra tutela dei dati personali e principio del "giusto" procedimento*, in *Rivista di Diritto Tributario*, n. 1/2024, pp. 125 ss.

[4] *Cfr.* Agenzia delle Entrate, *Informativa sulla logica sottostante i modelli di analisi del rischio basati sui dati dell'Archivio dei rapporti finanziari*, pp. 4-5.

delle banche dati e, dall'altra, dello sviluppo di idonee applicazioni informatiche di elaborazione dei dati[5].

Infatti, l'incredibile mole di dati a disposizione dell'amministrazione finanziaria, eterogenei e sostanzialmente disorganizzati, fatica ad essere oggetto di scambi completi e non consente agevolmente un'elaborazione coerente, con il conseguente rischio di creare visioni distorte e frammentate delle posizioni fiscali dei contribuenti; in questi termini, si rende quindi necessario *trasformare i dati in informazioni e le informazioni in conoscenza* (*cfr. "Relazione illustrativa del decreto legislativo 12 febbraio 2024, n. 13"*).

Introdotto dall'art. 11 del decreto legge 6 dicembre 2011, n. 201, lo strumento di analisi del rischio di evasione rimase per lungo tempo inattuato, sino alla Legge di bilancio del 2020, che ha dato nuovo impulso al sistema, attribuendo all'Agenzia delle Entrate la possibilità di avvalersi di tecnologie, elaborazioni ed interconnessioni con altre banche dati, allo scopo di individuare criteri di rischio utili all'emersione di posizioni da sottoporre a controllo e, allo stesso tempo, incentivare l'adempimento spontaneo.

La disciplina, generica e di fatto meramente autorizzativa, attribuiva all'Agenzia delle Entrate la possibilità di analizzare delle basi di dati con il generico fine di selezionare i contribuenti da sottoporre a controllo o nei confronti dei quali attivare strumenti di *compliance*, risultando del tutto deficitaria in punto di procedure da seguire e garanzie riconosciute ai contribuenti.

Le lacune procedimentali venivano colmate nella *"Relazione per orientare le azioni del governo volte a ridurre l'evasione fiscale derivante da omessa fatturazione"*, adottata dal MEF il 21 dicembre 2021, che prevedeva specifiche fasi di articolazione del processo di analisi del rischio di evasione (individuazione della platea di riferimento; scelta delle basi dati; messa a disposizione delle basi dati; analisi della qualità dei dati; definizione del criterio di rischio; scelta del criterio di analisi deterministico o stocastico; verifica della corretta applicazione del modello e del criterio di rischio; estrazione e identificazione dei soggetti connotati da rischio fiscale; test su campione della popolazione; invio delle comunicazioni; controllo; monitoraggio).

Ne emergeva uno strumento che trovava attuazione sia per le persone fisiche che per le società e gli enti, che poteva attingere ad ogni banca dati a disposizione dell'amministrazione finanziaria previa selezione delle basi di dati da sopporre ad analisi, comprendenti anche informazioni sensibili sui contribuenti.

---

[5] M. Fasola, *Le analisi del rischio di evasione tra selezione dei contribuenti da sottoporre a controllo e accertamento "algoritmico"*, in G. Ragucci (a cura di), *Fisco digitale. Criptoattività, protezione dei dati, controlli algoritmici*, Torino, 2023, p. 80.

Inevitabili le ricadute in termini di rispetto dei diritti dei contribuenti, primo fra tutti quello alla riservatezza, che sembrerebbe solo parzialmente tutelato dalla pseudonimizzazione[6], richiamata nel preambolo del decreto MEF 28 giugno 2022 e consistente nella separazione del pacchetto di dati di talune informazioni senza le quali non è possibile attribuire quegli specifici dati ad un certo soggetto, con conservazione separata di dati e riferimenti soggettivi.

I dati, sotto pseudonimo, confluiscono in un *c.d. dataset di analisi*, definito dal citato decreto come «*l'insieme dei dati selezionati per verificare, applicando tecniche e modelli di analisi coerenti con i criteri di rischio prescelti, la presenza di rischi fiscali*». e che, una volta ultimato, viene sottoposto a verifiche di qualità.

L'intelligenza artificiale e gli algoritmi svolgono il proprio ruolo centrale proprio intervenendo sui *dataset di analisi*, che vengono analizzati secondo modelli deterministici o stocastici in base alle scelte di programmazione[7].

Nel modello deterministico, i funzionari individuano un'ipotesi di rischio, che viene identificata a priori ed immessa nell'algoritmo, il quale, attraverso l'elaborazione dei *dataset*, individua posizioni che rispettino i parametri di rischio individuati *ex ante* (ad es. incoerenze tra patrimonio, flussi finanziari, reddito dichiarato, consumo e risparmio), da assoggettare a controlli ulteriori.

Nell'approccio stocastico, invece, l'impatto dell'intelligenza artificiale è più pregnante, giacché le correlazioni tra i dati dovrebbero essere estratte direttamente dall'algoritmo.

In questo *genus* procedimentale, è possibile operare sia attraverso algoritmi supervisionati che non supervisionati; nel primo caso, l'algoritmo parte dall'analisi e dall'elaborazione di dati presenti nell'archivio dei rapporti finanziari dell'Agenzia delle Entrate, relativi ad accertamenti pregressi positivi, che hanno esaurito

---

[6] La *c.d. pseudonimizzazione* dei dati, disciplinata dall'art. 4, par. 1, punto 5 del Regolamento GDPR è ontologicamente (e funzionalmente) differente alla *c.d. anonimizzazione*, giacché nella pseudonimizzazione non vi è la sostituzione o cancellazione di dati ma la mera introduzione di una chiave necessaria per la decodificazione del soggetto al quale i dati si riferiscono. Una volta rinvenuta ed applicata la chiave, ogni dato sarà correttamente associato alla persona alla quale esso si riferisce, senza possibilità di deviazioni o errori. Sul punto, tra gli altri, L. Tempestini e G. D'acquisto, *Il dato personale oggi tra le sfide dell'anonimizzazione e le tutele rafforzate dei dati sensibili*, in G. Busia, L. Liguori e O. Pollicino (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Roma, 2016, pp. 85-91. Il Garante della *privacy*, sulla pseudonimizzazione, si è espresso sull'inidoneità di questa alla tutela dell'anonimato dei contribuenti, ponendo l'accento sulla necessità di introdurre, da parte del Ministero, ulteriori misure di protezione dei dati nel rispetto dei principi di *privacy by design* e *by default* così come esplicitati dall'art. 25 GDPR.

[7] *Cfr. Relazione per orientare le azioni del governo volte a ridurre l'evasione fiscale derivante da omessa fatturazione,* adottata dal MEF il 21 dicembre 2021, pp. 21 ss.

il loro primo ciclo di vita amministrativo, estraendo autonomamente e con metodo induttivo, il profilo tipico dei soggetti a rischio, da raffrontare poi con la platea di riferimento già selezionata. Negli algoritmi non supervisionati, invece, l'algoritmo dovrebbe in via autonoma far emergere gruppi di soggetti omogenei rispetto alle caratteristiche descritte dai dati.

Si tratta di procedimenti informatici non esclusivi, che possono interferire tra loro, tanto che l'utilizzo di un algoritmo non supervisionato può costituire la fase antecedente a quella dell'utilizzo di un algoritmo supervisionato, del quale finisce per fungere da base di funzionamento.

Una volta eseguita l'analisi attraverso l'algoritmo - di ogni tipo esso sia - sarà individuato un *dataset* di controllo, consistente nell'«*insieme delle posizioni fiscali dei contribuenti, caratterizzate dalla ricorrenza di uno o più rischi fiscali, nei confronti dei quali potranno essere avviate attività di controllo ovvero attività volte a stimolare l'adempimento spontaneo*»[8].

Il D.M. 28 giugno 2022 prevede, in ogni caso, che l'intero processo di analisi sia assoggettato a controlli interni, al fine di scongiurare e limitare i rischi di ingerenze nei confronti dei contribuenti non caratterizzati dalla ricorrenza di un rischio fiscale significativo, dal momento che i *dataset* ottenuti possono tradursi in una vera e propria lista selettiva di contribuenti a rischio evasione.

3. *Il decreto legislativo 12 febbraio 2024, n. 13 e le sue criticità*

L'evidente frammentarietà della disciplina e l'assenza di precisi limiti e criteri legislativi ha imposto una razionalizzazione del quadro normativo secondo i criteri direttivi individuati dall'art. 17, co. 1, lett. *c*) e *f*) della legge delega 9 agosto 2023, n. 111, confluiti poi nell'art. 2 del decreto delegato n. 13/2024.

La novella ha esplicitato, per la prima volta, che il processo di analisi del rischio può basarsi sull'utilizzo di *machine learning* e intelligenza artificiale, precisando che l'Agenzia delle Entrate, nello svolgimento dell'attività, può utilizzare tutte le informazioni presenti nelle basi dati di cui dispone, quindi di fatto attribuendo all'amministrazione un potere assai ampio nell'ambito del trattamento dei dati per finalità di pubblico interesse, e che questa possa condividere con la Guardia di Finanza tutte le informazioni e gli strumenti informatici a disposizione, previa stipula di appositi protocolli d'intesa, sempre che ciò non contrasti con i regimi di trattamento dei dati personali, di riservatezza e di segretezza.

Inoltre, è prevista la possibilità di limitare l'esercizio dei diritti sanciti dal Regolamento (UE) n. 2016/679 con esclusivo riferimento all'attività di analisi del rischio, affidando ad un regolamento del MEF, previo parere dal Garante per

[8] Art. 1, co. 1, lett. *g*) Decreto MEF 28 giugno 2022.

la protezione dei dati personali, la disciplina di dettaglio e l'individuazione di misure adeguate a tutelare diritti e libertà dei contribuenti.

Dal contesto normativo, emerge un quadro nel quale il legislatore ha inteso attribuire all'amministrazione finanziaria, in nome della prevenzione e del contrasto all'evasione fiscale e all'abuso del diritto, una migliore allocazione delle risorse, ponendo in un piano secondario il rispetto dei diritti dei contribuenti che, pur costantemente richiamati, appaiono in concreto privi di effettiva tutela.

Tale impostazione, seppur comprensibile sotto un profilo prettamente funzionale, sembra porsi in controtendenza rispetto alle posizioni assunte dalla giurisprudenza amministrativa che, sebbene aperta al processo di automazione dei procedimenti, pone l'accento sulle numerose criticità scaturenti dall'impiego indiscriminato degli strumenti tecnologici in ambito procedimentale.

Nel caso in esame, al contrario, non appare definita alcuna garanzia in favore dei contribuenti, non essendo predeterminati persino il valore probatorio dei dati raccolti e le vie di contestazione delle risultanze, né essendo previsti limiti concreti di impiego degli strumenti di IA, sotto un profilo tanto qualitativo quanto quantitativo.

Eppure, i principi enucleati dal Consiglio di Stato in punto di trasparenza della decisione automatizzata, che dovrebbe estendersi ad ogni fase procedimentale, non paiono di complessa attuazione nell'ambito dell'analisi del rischio di evasione, essendo sufficiente - sotto il profilo della trasparenza *strictu sensu* intesa ed in ogni caso tenendo in considerazione le criticità scaturenti dal *c.d. problema della black box* per le *machine learning*[9] - una mera previsione di esplicitazione in termini non algoritmici del linguaggio di programmazione, almeno laddove dall'applicazione del sistema scaturisca l'emanazione di un atto impositivo.

Ciò che invece risulta più complesso, sin da un primo sguardo, è il coordinamento dell'esercizio del diritto di accesso con le esigenze di segretezza del procedimento tributario; sul punto, l'art. 24, lett. *b*) della L. 241/1990 esclude, in via di principio, l'esercizio del diritto di accesso disciplinato dagli articoli pre-

[9] Il *c.d. problema della black box* racchiude le opacità del processo decisionale della *machine learning* che segue un percorso caratterizzato da fattori di non-conoscibilità. Sul tema F. Pasquale, *The Black Box Society. The secret algorithms that control money and information*, Harvard, 2015. A. Venanzoni (*La valle del perturbante: il costituzionalismo alla prova delle intelligenze artificiali e della robotica*, in *Politica del diritto*, n. 2/2019, pp. 237 ss), osserva come nella problematica della *black box* risieda il paradosso delle tecnologie avanzate che, impiegate spesso per aumentare i parametri di trasparenza e delineare i *patterns* logici delle motivazioni e delle decisioni, sono tendenzialmente sovraintesi da percorsi decisionali sempre più opachi. Si veda anche D. Canè, *Intelligenza artificiale e sanzioni amministrative tributarie*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, pp. 321 ss.

cedenti nei procedimenti tributari, per i quali trovano applicazione le particolari disposizioni di settore.

Nell'ambito dell'analisi del rischio di evasione eseguita per il tramite di strumenti di intelligenza artificiale, solo l'espressa attribuzione legislativa del diritto di accesso ai dati in capo ai contribuenti sembrerebbe coerente con i canoni di legittimità enucleati dalla giurisprudenza amministrativa[10], ma tale attribuzione risulta quanto mai remota giacché andrebbe a privare di efficacia l'attività di controllo, svelando in anticipo al contribuente le successive mosse dell'amministrazione.

In assenza di una specifica indicazione legislativa sul punto, l'unico riferimento normativo appare quello dell'art. 4 del DM 28 giugno 2022, il quale rinvia il diritto di accesso ai dati che riguardano il contribuente al momento successivo alla ricezione degli inviti alla regolarizzazione della posizione fiscale ovvero al momento successivo alla consegna del PVC o della notifica dell'atto istruttorio o impositivo.

Tale posticipazione pone evidenti criticità, dal momento che viene impedito al contribuente di individuare e segnalare eventuali errori e inesattezze dei dati utilizzati dall'algoritmo, che potrebbero ingiustificatamente condurre ad un controllo, da considerare affetto da nullità derivata seguendo le regole tipiche della procedimentalizzazione[11]. A ciò deve pure aggiungersi che l'esercizio del diritto di accesso da parte del contribuente dopo la ricezione dell'atto non interrompe i termini per la proposizione del ricorso; si tratta di una questione particolarmente

---

[10] Secondo M. Fasola, *Le analisi del rischio di evasione, cit.*, p. 107, sarebbe necessario sul punto distinguere tra richieste di accesso riferite ai dati e richieste riferite all'algoritmo. I dati contenuti nei *dataset* di analisi e di controllo e riferiti all'istante sarebbero da qualificarsi come *documenti amministrativi* di cui all'art. 22, lett. *d*) della L. 241/1990 perché formati attingendo ai dati reddituali dei contribuenti; per essi, dunque, dovrebbero trovare applicazione i principi enucleati dal Consiglio di Stato nella sentenza 25 settembre 2020, n. 19, con conseguente piena accessibilità. Diversa sarebbe invece la soluzione per i dati riferiti a soggetti terzi e per gli algoritmi, con riferimento ai quali sarebbe escluso l'esercizio del diritto di accesso, come confermato dal provvedimento del direttore dell'Agenzia delle Entrate del 4 agosto 2020, nel quale sono espressamente citati i documenti di prassi interna che contengono criteri di analisi del rischio e individuazione di schemi di controllo nonché le relative metodologie di controllo.

[11] In termini M. Fasola, *Le analisi del rischio di evasione, cit.*, pp. 108-109. L'Autore, nell'evidenziare le criticità in punto di rispetto e di utilità del contraddittorio rinvia alle questioni concernenti l'accesso alle informazioni presenti nel fascicolo e reperite presso terzi che, se negato, impedisce lo svolgimento reale del contradditorio, sul quale si è espressa la Corte di Giustizia dell'Unione Europea con la sentenza 4 giugno 2020, causa C-430/2019, commentata da M. Basilavecchia, *Contraddittorio preventivo e accesso al fascicolo*, in *Corriere Tributario*, n. 8/2020, pp. 737 ss.

delicata, perché la ristrettezza dei tempi per l'impugnazione dell'atto impositivo potrebbe non collimare con i tempi necessari all'accesso: ne conseguirebbe una violazione del diritto di difesa idonea a determinare un accoglimento del ricorso pur in ricorrenza delle violazioni contestate dall'amministrazione finanziaria.

In ogni caso, svariati fattori inducono a ritenere che gli strumenti fondati sull'intelligenza artificiale acquisiranno un ruolo fondamentale nell'esercizio dell'attività istruttoria, essendo in grado di acquisire ed elaborare un volume di informazioni che tende ad essere sempre più ampio, con ricadute in punto di riservatezza e protezione dei dati personali; non si potrà cadere però nell'errore di ritenere che la decisione algoritmica possa sostituire l'intervento umano, e ciò sia per ragioni etico-concettuali che per espressa previsione di legge. Si pensi, sul punto, al dettato dell'art. 3-*bis* della legge n. 241/90 che consente alle amministrazioni pubbliche di servirsi di strumenti informatici e telematici per conseguire maggiore efficienza, attribuendo così a questi un ruolo puramente ancillare ed accessorio, ma anche all'art. 22 del GDPR, che prevede, su richiesta dell'interessato, la sostituzione dei processi decisionali automatizzati con processi diversi.

È evidente come l'utilizzo di sistemi di intelligenza artificiale porti con sé delicati problemi di bilanciamento tra interesse pubblico e diritti dei contribuenti, tanto da aver indotto parte della dottrina a riflettere sul rischio di sconfinamento verso una "*società della sorveglianza*"[12], che potrebbe essere arginato da una parte attraverso la tutela della libertà negativa dei contribuenti di non utilizzare le tecnologie digitali, il cui impiego sarebbe sempre da configurarsi come un diritto e mai come un obbligo[13], e dall'altra con l'applicazione rigorosa del principio della riserva di legge[14].

---

[12] D. Conte, *Accertamento tributario e modelli predittivi, cit.*, parla della possibilità che venga ad affermarsi un potere pubblico che *"vede chiunque senza essere visto. Una sorta di "grande fratello" che, in nome dell'interesse collettivo al pagamento delle imposte, finirebbe per controllare ogni aspetto della vita dei contribuenti".* Per l'Autrice, che si pone in una posizione conforme a quella espressa dal Garante della Privacy nel Parere n. 453 del 22 dicembre 2021, la menzionata pseudonimizzazione dei dati non costituirebbe una garanzia efficace per i contribuenti, attesa la loro identificabilità.

[13] Fatta eccezione per quei soggetti dotati per presunzione legislativa di un'organizzazione di mezzi adeguata a fronteggiare la costante evoluzione tecnologica, non comprendenti certamente le persone fisiche. L'eventuale obbligo di utilizzo delle tecnologie digitali da parte di tutti i contribuenti, infatti, potrebbe generare fenomeni di c.d. digital divide (R. De La Feria e A. Grau Ruiz, *The Robotisation of Tax Administration*, in A. Grau Ruiz (a cura di), *Interactive Robotics: Legal, Ethical, Social and Economic Aspects*, Berlino, 2022, 115 ss.) soprattutto in un Paese come l'Italia nel quale permane un'ampia platea di cittadini che rimane esclusa dal processo di digitalizzazione della società (*Cfr.* Rapporto ISTAT "BES 2021. Il benessere equo e sostenibile in Italia").

[14] Sulla necessità di una tipizzazione dei casi di obbligatorietà all'utilizzo delle

Rebus sic stantibus, sembrerebbe mancare un contrappeso a quello che rischia di tradursi in uno strapotere statuale, giacché il *focus* principale del legislatore, allo stato, appare dotare l'amministrazione finanziaria di poteri pregnanti nella lotta all'evasione fiscale e all'abuso del diritto, *costi quel che costi*, e ciò anche a sacrificio dei diritti dei contribuenti che tanto hanno faticato a trovare una positivizzazione.

tecnologie digitali in capo ai contribuenti e dei poteri riconosciuti all'amministrazione finanziaria in tal senso, l'Organizzazione per le cooperazione e lo sviluppo economico (OECD, *Taxation for design,* 2014) sostiene l'inutilità dell'introduzione di nuove disposizioni, mentre la dottrina (F. Farri, *Digitalizzazione dell'amministrazione finanziaria e diritti dei contribuenti*, in *Rivista di diritto tributario*, n. 6/2020, p. 132) appare ragionevolmente di indirizzo contrario, sostenendo che diversamente non sarebbero rispettati i principi costituzionali.

Sezione III
IA, IMPRESE E MERCATI

La regolazione del mercato dell'intelligenza artificiale: dall'AI act all'intervento pubblico per lo sviluppo tecnologico

di **Lorenzo Rodio Nico**

1. *Inquadramento dell'Intelligenza Artificiale e mercato tecnologico*

Le tecnologie di frontiera rappresentano quella categoria di strumenti che «hanno il potenziale di sconvolgere lo status quo, alterare il modo in cui le persone vivono e lavorano, riorganizzare i pool di valore e portare a prodotti e servizi completamente nuovi»[1]. Tra tutte le nuove tecnologie l'Intelligenza Artificiale[2] sembra essere quella che più si avvicina al concetto di tecnologia di frontiera atteso che, come altre tecnologie che hanno cambiato il corso della storia, anch'essa rappresenta un evidente punto cardine nel progresso globale.

Si tratta, quindi, di una tecnologia in grado di poter ridefinire gli assetti socio-economici globali, di trasformare significativamente le catene del valore e i macrosettori economici, ciò primariamente grazie alla capacità di elaborare grandi quantità di dati, automatizzare processi complessi e fornire supporto decisionale ed è uno strumento in grado di provocare quello che è stato definito «il grande balzo storico dell'inizio del terzo millennio»[3].

---

[1] Tra le diverse definizioni, quella fornita da McKinsey Global Institute, J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, A. Marrs, *Disruptive technologies: Advances that will transform life, business, and the global economy*, Maggio 2013, risulta essere quella che meglio riesce ad inquadrare il concetto di tecnologia di frontiera.

[2] Che è necessario distinguere dagli algoritmi che sono, invece, «uno strumento per l'intelligenza artificiale, ma non è intelligenza artificiale» (così M. Sepe, *Innovazione tecnologica, algoritmi e Intelligenza Artificiale*, in *Rivista Trimestrale di Diritto dell'Economia*, suppl. al n. 3, 2021, pp. 204-205).

[3] Così S. Mattarella, *Messaggio di Fine Anno del Presidente della Repubblica*

L'influenza di questa fattispecie di tecnologie, quindi, si riverbera in maniera totalitaria con il coinvolgimento di tutti gli attori della società, dal settore pubblico a quello privato, sia in via orizzontale che verticale. Tant'è che l'IA[4] rientra tra quelle tecnologie c.d. «distruttive»[5], in grado di attivare processi di "distruzione creativa"[6] tali da rivoluzionare la società e il mercato[7].

La particolarità dell'IA è il percorso storico assai peculiare che la caratterizza, consistente da una prima fase di ricerca risalente alla prima metà del '900[8],seguita

Sergio Mattarella, in *quirinale.it*, 31 dicembre 2023.

[4] Per una definizione puntuale di Intelligenza Artificiale si rinvia all'AI Act (Regolamento (Ue) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), art. 3, punto 1) che la identifica quale «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali». Tale definizione, seppure sia stato spesso evidenziato come non ne esista una univoca (cfr. *ex multis* S. J. Russell, P. Norvig, e E. Davis, *Artificial Intelligence: A Modern Approach*, 4° ed., Londra, 2016; S. Bringsjord, N. S. Govindarajulu, voce *Artificial Intelligence*, in *The Stanford Encyclopedia of Philosophy*, Stanford, 2020; J. Turner, *Robot Rules. Regulating Artificial Intelligence*, Londra, 2019, p. 7 ss.; F. Donati, *Intelligenza Artificiale e giustizia*, in Rivista AIC, n. 1, 2020, p. 415; M. U. Sherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies and Strategies*, in *Harvard Journal of Law & Technology*, 2, 2016, p. 359; C. Casonato, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo*, 2019, p. 102; A. D'Aloia, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *Rivista di BioDiritto*, 1, 2019, p. 8; F. Raso, H. Hilligoss, V. Krishnamurthy, C. Bavitz e L.Y. Levin, *Artificial Intelligence & Human Rights: Opportunities and Risks*, Harvard, 2018; E. Rich, K. Knight, *Artificial Intelligence*, New York, 1991), riesce comunque a fornire un'identità completa della tecnologia in esame.

[5] Directorate-General for External Policies - Policy Department (European Parliament, *Current and Emerging Trends in Disruptive Technologies: Implications for the Present and Future of EU's Trade Policy*, Bruxelles, 2017, p. 2).

[6] J. Schumpeter, *Capitalism, Socialism, and Democracy*, VI ed., Londra, 2003, pp. 81 e ss.

[7] Sul punto v. F. Capriglione, *Diritto ed economia. La sfida dell'intelligenza artificiale*, in *Riv. Trim. Dir. Ec.*, n. 3, suppl., 2021, p. 33.

[8] Sul punto cfr. W.S. McCulloch. W. Pitts, *A logical calculus of the ideas immanent in nervous activity. Bulletin of Mathematical Biophysics*, n. 5, 1943, pp. 115-133, dove gli AA. proposero il primo modello matematico di rete neurale. Successivamente,

poi da uno sviluppo scarno legato alla sua dipendenza diretta dal progresso tecnologico di altri settori (microchip e schede grafiche) e dalla potenza computazionale disponibile, che non ne ha permesso una adeguata sperimentazione iniziale[9].

Solo a partire dal 2010, l'accesso e l'archiviazione di enormi quantità di dati[10] impiegabili per l'apprendimento delle macchine e l'impiego di *hardware* in grado

---

cfr. A.M. Turing, *Computing Machinery and Intelligence*, Mind, 1950. Si ritiene che la nascita della materia di studio sull'Intelligenza Artificiale sia avvenuta nel 1956 al Dartmouth College, università statunitense situata ad Hanover grazie all'iniziativa di McCarthy (sul punto cfr. D. Crevier, *Ai: The Tumultuous history Of The Search For Artificial Intelligence*, New York, 1993, pp. 48-50; si rinvia anche a P. Mariani, D. Tiscornia (a cura di), *Sistemi esperti giuridici. L'intelligenza artificiale applicata al diritto*, Milano, 1989, p. 34).

[9] Il termine "Intelligenza Artificiale", però, fu coniato solo nel 1955 (J. Mccarthy et al., *A Proposal for the Darmouth Summer Research Project on Artificial Intelligence*, 31 agosto 1955, p. 2, consultabile all'indirizzo http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf) e «la sfida che si posero gli scienziati con l'IA era di riuscire a costruire un cervello che oltre ad avere un software duttile avesse anche un hardware implementabile a piacere […] in altri termini, immaginarono di poter creare ciò che oggi chiamiamo un'Intelligenza Artificiale (IA), con l'obiettivo ultimo di simulare, e possibilmente superare, il funzionamento del cervello umano» (così G. Maira, *Intelligenza umana e intelligenza artificiale*, in *federalismi.it*, n. 7, 2021, p. 7). Sul punto è interessante osservare anche come, in quegli anni, si sia sviluppato un filone di ricerca e sperimentazione sull'impiego della tecnologia in ambito giudiziario, dall'automazione della giustizia alla sperimentazione di strumenti di ausilio per i giudicanti e gli avvocati, sino ad arrivare ad ipotesi di giustizia predittiva, teoricamente impensabile per quegli anni (V. *ex multis* A. Harris, *Judicial Decision Making and Computers*, in *Vill. L. Rev.*, 12, 1967, p. 272; R. Lawlor, *Forum: Computers and Automation in Law*, in *Cal. B.J.*, n. 40, 1965, p. 30 ss.; C. Hayden, *How Electronic Computers Work: A Lawyer Looks Inside the New Machines*, in *Modern Uses of Logic in Law*, n. 62, p. 112 ss.; C. Morris, *Hospital Computers in Court*, in *Modern Uses of Logic in Law*, n. 4, p. 61 ss.; D. Hensley, *Punched Cards Produce Progress in Probate Court*, in *A.B.A.J.*, n. 48, 1962, p. 138; E. Adams, *EDP Aid to the Courts*, in *Proceedings of the Conference on Edp Systems for State and Local Governments*, 1964; A. Ellenbogen, *Automation in the Courts*, in *A.B.A.J.*, 1964, p. 655 ss.; J. Spangenberg, G. Neumann, *Data Processing: A Modern Tool to Help Improve Judicial Administration*, in *Mass. L.Q.*, n. 50, 1965; J. Davis, *Automatic Data Processing and the Judge Advocate General's Corps*, in *Military L. Rev.*, n. 23, 1964.

[10] Il valore economico (G. Luchena, S. Cavaliere, *Il riutilizzo dei dati pubblici come risorsa economica: problemi e prospettive*, in *Rivista giuridica del Mezzogiorno*, n. 1, 2020, pp. 151-169) e sociale dei dati è aumentato in maniera esponenziale. A evidenziare l'importanza dei dati è proprio il legislatore, principalmente quello europeo, che negli ultimi anni ha dato il via a numerose iniziative (Regulation (Eu) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive

di accelerare i processi di apprendimento dell'I.A[11], sono riusciti a rappresentare una svolta per lo sviluppo di questa tecnologia.

In sostanza, il percorso di sviluppo dei sistemi di IA è stato contrassegnato sì da un lungo ed iniziale andamento altalenante ma, oggi, la sua crescita può definirsi *tout court* rapida ed esponenziale[12].

Alla luce dell'espansione repentina che questa tecnologia ha avuto negli ultimi anni e delle sue potenzialità future, uno sviluppo concreto (e corretto) dell'IA, può permettere un posizionamento efficace (di *leader*) degli Stati sulla frontiera tecnologica a livello globale. In particolare, per i paesi già sviluppati e industrializzati, si può arrivare a ipotizzare anche uno spostamento in avanti della frontiera tecnologica a garanzia di una consistente crescita economica.

Conseguentemente, l'IA, come le altre tecnologie di frontiera hanno la caratteristica di determinare la nascita (rapida) di nuovi mercati o lo sviluppo di quelli già esistenti, richiedendo interventi normativi tempestivi per regolarne l'utilizzo.

L'adozione diffusa dell'IA, però, solleva criticità sulla tassonomia e sul metodo di utilizzo della stessa, nonché problematiche in tema di trasparenza, responsabilità e neutralità delle decisioni automatizzate. Le sfide in tal senso sono numerose e, tra queste l'effetto *black box*, ovvero la difficoltà di comprendere il processo decisionale interno dei sistemi, e i c.d. "pregiudizi" algoritmici, derivanti dall'addestramento dei modelli su dati che possono contenere *bias* impliciti, ne rappresentano solo alcune.

La regolamentazione del mercato dell'IA non solo deve garantire un uso etico e sicuro, ma anche promuovere l'innovazione e lo sviluppo economico, ciò attraverso l'adozione di quadri normativi robusti ma, allo stesso tempo, flessibili, atteso che l'importanza di regolare un nuovo mercato non si ferma solo alla tutela dell'individuo, ma coinvolge anche la stabilità economica, gli impatti sociali e la competitività nel mercato globale.

(EU) 2020/1828 (Data Act) volte, soprattutto, alla protezione dei dati (personali e non), alla loro tracciabilità e al loro sfruttamento per fini commerciali (V. Falce, *Strategia dei dati. Traiettorie orizzontali e applicazioni verticali*, in V. Falce (a cura di), *Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato*, Torino, 2023, 5 e S. Landini, *Circolazione dei dati, data analytics e tool di intelligenza artificiale nel settore assicurativo*, in V. Falce, U. Morera (a cura di), *Dall'*open banking *all'*open finance*. Profili di diritto dell'economia*, Torino, 2024, p. 95 ss).

[11] C. Böhm, R. Noll, C. Plant, B. Wackersreuther, A. Zherdin, *Data Mining Using Graphics Processing Units*, in Computer Science, vol. 5740, Berlino, 2009.

[12] In merito è stato osservato che «l'innovazione tecnologica digitale, in particolare quella legata agli sviluppi dell'intelligenza artificiale, segue una traiettoria esponenziale» (così M. Sepe, I*nnovazione digitale, tra rischi di deriva algocratica e possibili rimedi*, in *Rivista trimestrale di diritto dell'economia*, supplemento al n. 4, 2023, p. 237).

La tecnologia in esame, infatti, ha il potenziale di migliorare significativamente la produttività e la crescita economica. Ciò, tuttavia, introduce nuove sfide, come il mutamento del mercato del lavoro e la concorrenza sleale. Un mercato regolato potrebbe garantire un equilibrio quale risultato della combinazione della supervisione nazionale e sovranazionale.

I sistemi di IA, specialmente quelli utilizzati in aree critiche come la sanità e la finanza, devono aderire a elevati standard di trasparenza e responsabilità. Il potenziale dell'IA di facilitare attività criminali, denominato AI-Crime, sottolinea la necessità di una regolamentazione che prevenga l'uso improprio promuovendo al contempo l'innovazione.

L'approccio europeo sul punto, che mira a bilanciare l'integrazione del mercato con lo sviluppo responsabile dell'IA, è un esempio di ricerca di equilibrio o di «ritmo»[13].

Una posizione regolatoria proattiva diviene quindi essenziale purché conservi una flessibilità e un'adattabilità tali da poter tenere il passo con i rapidi avanzamenti tecnologici.

Pertanto, possono rilevarsi due aspetti che contraddistinguono l'attuale contesto: in primo luogo, vi è la regolamentazione dell'IA che, a livello europeo, è sì avvenuta in tempi ragionevoli se rapportata alla velocità di diffusione della tecnologia, ma che presenta numerose criticità; in secondo luogo, emerge come il settore privato sia la colonna portante dello sviluppo della tecnologia in esame e, solo nei tempi più recenti, si è potuto osservare un ingresso dell'IA nella programmazione economica europea[14] e statale, ma tali iniziative potrebbero non essere adeguatamente sostenute da un apparato normativo troppo restrittivo in termini di libertà di sviluppo.

2. *Governare l'Intelligenza Artificiale: AI Act, regolamentazione del mercato…*

Per affrontare le sfide poste dall'IA diviene necessario un intervento legislativo equilibrato, al fine di sviluppare una regolamentazione che possa garantire livelli elevati di trasparenza e spiegabilità dei sistemi, identificare e mitigare i pregiudizi e promuovere l'equità e l'inclusione assicurando che gli utenti possano anche comprendere e contestare le decisioni della stessa.

---

[13] G. Marchant, *Addressing the Pacing Problem*, in G. Marchant et al. (eds), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem*, Springer Netherlands, 2011.

[14] M. Papazoglou, J. Torrecillas Jodar, M. Cardona, E. Calza, M. Vazquez-Prada Baillet e R. Righi, *Mapping EU level funding instruments to Digital Decade targets*, M. Lopez Cobo, G. De Prato (edited by), Publications Office of the European Union, Luxembourg, 2023.

Tale intervento, però, non appare di semplice attuazione[15], poiché una *governance* eccessivamente restrittiva può anche divenire un freno per lo sviluppo e la crescita economica.

A quanto esposto può aggiungersi un ulteriore aspetto: se la normazione avviene in maniera errata o è troppo permissiva, può ingenerare, invece, effetti negativi; pertanto, regolare la tecnologia e promuoverne lo sviluppo è, di fatto, una questione di equilibrio.

L'adozione dell'AI Act rappresenta una delle più importanti iniziative a livello globale (ed europeo) in materia di regolamentazione specifica di una singola fattispecie tecnologica. Se, però, l'atto rappresenta un passo importante verso lo sviluppo di un quadro normativo che favorisca l'innovazione responsabile e la tutela dei mercati coinvolti, ciò non garantisce che tale iniziativa non rappresenti, invece, una limitazione alla ricerca e allo sviluppo tecnologico.

Sul punto i *policymaker* e i regolatori svolgono ruoli fondamentali, difatti «al primo competono le scelte in materia di libertà e responsabilità nello sviluppo dell'intelligenza artificiale; al secondo appartengono i compiti di tradurre tali scelte in regole applicabili in un contesto di mercato; ciò disciplinando quella nuova commistione tra uomo e macchina che, al presente, condiziona la formulazione dell'offerta e della domanda di capitali, di servizi bancari e di strumenti finanziari»[16].

La capacità di elaborare una *governance* e regolare nuovi mercati prima di altre economie può rendere la tecnologia emergente fruibile al pubblico più rapidamente, evitare correttivi *ex post* a tecnologie già commercializzate e diffondere i prodotti all'interno del mercato o esportarli, con un conseguente vantaggio tecnologico ed economico per le imprese private e per lo Stato che lo ha promosso.

Viceversa, anche il mercato può influenzare le scelte del regolatore e tale fenomeno può osservarsi nelle tre diverse politiche di intervento adottate rispettivamente dagli Stati Uniti, dalla Cina e dall'Unione Europea per il mercato tecnologico. I primi hanno un «approccio tecno-libertario […] incentrato sulla primazia del libero mercato tecnologico e dunque del libero esercizio del potere tecnologico ed economico»[17]; la seconda opera un profondo controllo statale sulle tecnologie[18]

---

[15] Riconosciuta come una «situazion(e) di più complessa sistemazione […] nelle sue diverse modalità applicative incidenti sul campo economico» (G. Luchena, *Orizzonti del Diritto dell'economia: un'introduzione oggetto, metodo, dottrine*, in *Rivista trimestrale di diritto dell'economia*, n. 4, 2023, p. 428).

[16] Così M. Pellegrini, *L'intelligenza artificiale nell'organizzazione bancaria: quali sfide per il regolatore?*, in *Rivista Trimestrale di Diritto dell'Economia*, n. 3, 2021, p. 431.

[17] N. Abriani, G. Schneider, *Diritto delle imprese e intelligenza artificiale Dalla Fintech alla Corptech*, Bologna, 2021, p. 19.

[18] Cfr. G. Finocchiaro, *Intelligenza artificiale. Quali regole?*, Bologna 2024, p. 107 ss.

mentre la terza ha un approccio mediano che punta alla creazione e/o produzione di tecnologie anche nella tutela dei diritti e dei principi sulla quale fonda in maniera diversa «rispetto alle opzioni più radicali improntate al *laissez-faire* statunitense e all'iperstatalismo cinese, prospettando la possibilità di una mediazione tra le esigenze di promozione dell'integrazione del mercato digitale europeo e di una effettiva incorporazione, nel funzionamento di questo stesso mercato, dei valori fondanti le tradizioni costituzionali dell'Unione e degli Stati membri»[19].

La difficoltà di regolare una tecnologia di frontiera si rileva proprio dal lungo percorso legislativo europeo che ha portato all'adozione del Regolamento europeo dell'IA. L'*iter* ha visto un concatenarsi di numerosi atti di *soft law* e, in particolare, di atti di *pre-law*, e *para-law*[20] che hanno posto le basi per una prima idea di *governance* europea di IA, la cui origine può rinvenirsi[21] nella pubblicazione delle "raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica"[22] (CLRR), documento con il quale è stato sottolineato il possibile

---

[19] N. Abriani, G. Schneider, *o.c.*, p. 20. Per un approfondimento sulle convergenze e divergenze tra le iniziative degli Stati Uniti e dell'Europa cfr. E. Chiti, B. Marchetti, *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, in *Rivista della regolazione dei mercati*, n. 1, 2020.

[20] A. Poggi, Soft law *nell'ordinamento comunitario*, in *Annuario 2005. L'integrazione dei sistemi costituzionali europeo e nazionali. Atti del XX Convegno Annuale. Catania, 14-15 ottobre 2005*, Padova, 2007, p. 369 ss. e L. Senden, *Soft Law in European Community Law*, Oxford, 2004, p. 478 ss. Quello della *soft law* viene ritenuto un «sistema affidabile di *enforcement* in assenza del quale (i nuovi diritti sostanziali e procedurali legati all'impiego delle nuove tecnologie) resterebbero soltanto delle prescrizioni senza alcuna pretesa di vincolatività» (così A. Pajno, M. Bassini, G. De Gregorio, M. Macchia, F.P. Patti, O. Pollicino, S. Quattrocolo, D. Simeoli e P. Sirena, *AI: profili giuridici – Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in *Rivista di Biodiritto*, vol. 3, 2019, pp. 210-211).

[21] Nel 2017 il Consiglio europeo ha posto in evidenza la necessità «di far fronte alle tendenze emergenti» tra cui «questioni quali l'intelligenza artificiale» (Consiglio europeo, *Riunione del Consiglio europeo (19 ottobre 2017) – Conlusioni,* EUCO 14/17, 2017, p. 8).

[22] Gazzetta Ufficiale U.E., P8TA(2017)0051, *Norme di diritto civile sulla robotica, Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica* (2015/2103(INL) (2018/C 252/25), 18 luglio 2018.Tra le iniziative precedenti può richiamarsi CEPEJ, *The CEPEJ European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment. Presentation note*, 2018 (in merito cfr. *ex multis*, F.C. Gastaldo, *Lo statuto della giustizia digitale nella carta etica della CEPEJ*, in *iusinitinere.it*, 2 aprile 2021; C. Barbaro, *Uso dell'intelligenza artificiale nei sistemi giudiziari: verso la definizione di principi etici condivisi a livello europeo?,* in *Questione giustizia*, n. 4, 2018; S. Quattrocolo, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea,*

impatto dei processi delle decisioni automatizzate[23]. Solo quattro anni dopo, nel 2021, la Commissione europea ha elaborato la proposta di Regolamento sull'Intelligenza Artificiale[24], poi definitivamente approvata a giugno 2024.[25]

---

gli spunti per un'urgente discussione tra scienze penali e informatiche, in *Legislazione Penale*, 2018). Le iniziative successive sono, invece, state molto più numerose: le "*Ethics Guidelines for Trustworthy Artificial Intelligence*", hanno rappresentato il primo passo per uno sviluppo uniforme dell'IA in Europa (N.A. Smuha*, The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence*, in *Computer Law Review International*, vol. 20, 2019, pp. 97-106). Successivamente, con il *White Paper on Artificial Intelligence - A European approach to excellence and trust*, sono state avanzate le prime ipotesi di regolamentazione per lo sviluppo dell'IA per tutti gli ambiti applicativi (pubblici, economici e privati) e sull'adattabilità della normativa vigente all'epoca per far fronte ai rischi derivanti dall'impiego dei sistemi di IA. *Ex multis* possono richiamarsi anche: Commissione europea, *Plasmare il futuro digitale dell'Europa*, COM(2020) 67 final, 19 febbraio 2020 e Commissione Europea, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, COM(2021) 118 final, 9 marzo 2021; Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate, 2020/2012(INL); Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, 2020/2014(INL); Risoluzione del Parlamento europeo del 20 ottobre 2020 sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale, 2020/2015(INI); Progetto di relazione del Parlamento europeo sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale, 2020/2016(INI); *Piano d'azione per l'istruzione digitale 2021-2027 - Ripensare l'istruzione e la formazione per l'era digitale*, COM(2020) 624 final, 30 settembre 2020).

[23] Id., punto Q.

[24] Commissione Europea, *Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (Legge sull'Intelligenza Artificiale) e modifica di alcuni atti legislativi dell'Unione*, COM(2021) 206 final, 21 aprile 2021, iniziativa già anticipata nel 2019 dalla presidente Von Der Leyen (in U. Von Der Leyen, *Orientamenti politici per la prossima Commissione europea 2019 – 2024*, 2019, pp. 14-15). In merito si cfr. *ex multis* V. Lemma, *Intelligenza Artificiale e sistemi di controllo: quali prospettive regolamentari?*, in *Rivista Trimestrale di Diritto dell'Economia*, supplemento al n. 3, 2021, pp. 319 ss.; C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal*, n. 3, 2021; G. Di Rosa, *Quali regole per i sistemi automatizzati intelligenti?*, in *Riv. Dir. Civ.*, n. 5, 2021, pp. 823 ss.; L. Floridi, *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, in *Philosophy & Technology*, n. *34*, 2021, pp. 215–222.

[25] Pubblicata il 12 luglio con il numero 2024/1689.

Con l'AI Act, le autorità europee mirano a preparare il mercato dell'Unione garantendo l'introduzione di prodotti di IA che siano sicuri, affidabili[26] ed etici[27]. Per fare ciò, il Regolamento fonda su un sistema basato sul rischio[28] che permette di classificare le IA attraverso dei criteri di valutazione predeterminati. Tale si-

[26] La proposta di regolamento, oltre che una presa d'atto di tutti i rilievi sollevati in precedenza dalla stessa Unione Europea, è anche il risultato della consultazione pubblica dei portatori di interesse del settore pubblico e privato (compresi governi e autorità locali) che stata avviata congiuntamente alla pubblicazione del Libro bianco sull'intelligenza artificiale (19 febbraio 2020), ed è terminata in data 14 giugno 2020. Attraverso questa consultazione l'Unione ha raccolto osservazioni e pareri sul Libro bianco per un totale di 1215 contributi attraverso i quali si è avuta una risposta pressoché univoca sulla necessità di dover colmare le lacune legislative e di adottare una normativa nuova e, al contempo, è stato posto in evidenza il bisogno di una regolamentazione semplice e proporzionata coadiuvata da una definizione precisa e restrittiva del concetto di intelligenza artificiale distinguendole a seconda della pericolosità ("rischio") (cfr. *Shaping Europe's digital future, Consultation results 17 July 2020, White Paper on Artificial Intelligence: Public consultation towards a European approach for excellence and trust*, reperibile all'indirizzo https://wayback.archive-it.org/12090/20210304034028/https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence).

[27] Come stabilito in Consiglio europeo, *Riunione straordinaria del Consiglio europeo (1 e 2 ottobre 2020) – Conclusioni*, 2020, 6, e in Parlamento europeo, *Quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate*, P9_TA(2020)0275, 2020, pubblicato in GUUE, C 404/63, 6 ottobre 2021. Altresì, si punta alla riduzione della frammentazione normativa, motivo per cui è prevista anche l'istituzione di un apposito comitato europeo per l'Intelligenza Artificiale che favorisca il coordinamento tra Stati e Unione (v. J. Andraško, M. Mesarčík, O. Hamuľák, *The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework*, in *AI and Society*, n. 36, 2021, p. 623 ss.). Sul punto si è rilevato come il Regolamento tenti di presentarsi come "preciso e elastico" così da affrontare al meglio la capacità evolutiva dei sistemi di IA. Per poter rimanere al passo, la Commissione (art. 4) punta a rafforzare la propria posizione con la possibilità di adottare atti delegati per aggiornare e modificare il contenuto dell'Allegato I per seguire l'andamento dello sviluppo dei prodotti di IA così da evitare che la lentezza del processo legislativo «diventi freno all'evoluzione della tecnologia e del suo uso all'interno del territorio dell'Unione, mettendo così a rischio la capacitò competitiva stessa dell'Unione a livello globale» (così testualmente F. Pizzetti, *La proposta di Regolamento sull'IA della Commissione Europea presentata il 21.4.2021 (COM (2021) 206 final) tra Mercato Unico e competizione digitale globale*, in *Diritto di Internet*, n. 4, 2021, pp. 594-595).

[28] G. De Gregorio, P. Dunn, *The European risk-based approaches: Connecting constitutional dots in the digital age*, in *Common Market Law Review*, vol. 59(2), 2022, pp. 473 ss.

stema deve essere adattabile a seconda della portata dei rischi che possono essere generati da un singolo sistema di IA con una previsione espressa di divieti sull'utilizzo di determinati sistemi e a stabilire i vincoli di sviluppo per gli operatori e gli annessi obblighi di trasparenza[29].

A seconda del livello di rischio assegnato, i sistemi di IA devono rispettare una serie di requisiti obbligatori nonché seguire delle procedure di valutazione della conformità prima di poter essere immessi sul mercato.

Fra le priorità individuate dalla Commissione, viene in evidenza in primo luogo quello del rispetto dei diritti fondamentali, tant'è che la tutela di questi ultimi è un requisito per determinare se un'IA è, o meno, ad alto rischio[30].

Con tale scelta si mira a ridurre le possibilità che si verifichino fenomeni diffusi di discriminazione algoritmica, anche attraverso l'utilizzo di *dataset* che siano sottoposti ad una sorveglianza umana attiva durante l'annotazione e la catalogazione.

Vengono individuati essenzialmente due livelli di rischio: pratiche di IA vietate (che comporta il divieto di determinate pratiche o usi dei sistemi di IA (art. 5) e ad alto rischio (artt. 6 e ss.), in continuità con l'approccio prudenziale europeo che nel caso di specie si applica attraverso una limitazione dell'accesso al mercato di quei prodotti ritenuti troppo pericolosi il cui impatto non può essere mitigato[31]. In merito, è stato rilevato come l'approccio strategico e regolatorio dell'Unione nei confronti dell'I.A sembri subire, in parte, le influenze dalla crisi del 2008. Ciò potrebbe aver portato la Commissione a porsi nei confronti dell'IA come una sorta di seme di una possibile tecno-crisi, «che si aggiunge a quelle già esistenti ed è destinata a interagire con queste in modi non ancora del tutto prevedibili» decidendo, «nello stesso tempo, di sostenere e di alimentare tale fattore»[32]

---

[29] Si consideri, a titolo esemplificativo, che la *Directive on Automated Decision Making* in vigore in Canada dal 2019 (e costantemente sottoposta ad aggiornamento obbligatorio semestrale) prevede, tra i requisiti che devono essere posseduti da un sistema di IA, che venga garantita una spiegazione (comprensibile) agli individui investiti da una decisione ottenuta in maniera automatizzata (punto 6.2 "Trasparency" della *Directive on Automated Decision Making*, aggiornata al 1.04.2021 e consultabile all'indirizzo https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592).

[30] «Un sistema di IA di cui all'allegato III non è considerato ad alto rischio se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale» (art. 6, c. 3, AI Act).

[31] K. Garnett, D.J. Parsons, *Multi-Case Review of the Application of the Precautionary Principle in European Union Law and Case Law*, in *Risk Analysis*, n. 37,2017, p. 502.

[32] Testualmente E. Chiti, B. Marchetti, *Divergenti?*, cit., pp. 31 e 33. Gli Autori hanno altresì evidenziato come l'intervento legislativo posto in essere dalla

che influenza direttamente anche l'iniziativa normativa[33].

Occorre porre in luce che la tecnologia in esame, se non gestita e regolata nel modo corretto (o con una corretta flessibilità), potrebbe portare ad affrontare una nuova crisi che coinvolgerebbe tutti i settori[34].

2.1 *(segue) … e il* risk-based system

Proprio questo timore nei confronti dell'IA ha portato la Commissione a sviluppare un sistema basato sul rischio[35].

Commissione rispecchi la politica industriale europea anche in un'ottica di innovazione tecnologica sostenibile.

[33] La possibilità di poter utilizzare l'IA in innumerevoli settori potrebbe avvicinarla a quella che è stata definita una «crisi multidimensionale» (E. Chiti, B. Marchetti, *o.l.c.*, 4) così come lo è stata quella del 2008 (sul punto cfr. E. Chiti, A.J. Menéndez, P.G. Teixeira (a cura di), *The European Rescue of the European Union? The Existential Crisis of the European Political Project*, in *Arena Report No 3/12* e *Recon Report No. 19*, 2012; J.H. Weiler, *Europe in Crisis – On 'Political Messianism', 'Legitimacy' and the 'Rule of Law'*, in *Singapore Journal of Legal Studies*, 2012, p. 248 ss.; G. Majone, *The Deeper Euro-Crisis or: The Collapse of the EU Political Culture of Total Optimism*, in *EUI Working Paper LAW*, n. 10, 2015).

[34] Tale attenzione emergeva già prima della pubblicazione della proposta di Regolamento (cfr. F. Rodi, *Gli interventi dell'Unione europea in materia di intelligenza artificiale e robotica: problemi e prospettive*, in G. Alpa (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020, pp. 187-210; L. Parona, *Prospettive europee e internazionali di regolazione dell'intelligenza artificiale tra principi etici,* soft law *e* self regulation, in *Rivista della Regolazione dei Mercati*, n. 1, 2020, p. 70 ss.; M. Zanichelli, *Ecosistemi, opacità, autonomia: le sfide dell'intelligenza artificiale in alcune proposte recenti della Commissione europea*, in A. D'Aloia (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, 2020, pp. 67-87; A. Adinolfi, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, p. 13 ss.; A. Amidei, *La governance dell'intelligenza artificiale: profili e prospettive di diritto dell'Unione europea*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Torino, 2020, p. 571 ss.; A. Celotto, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Analisi Giuridica dell'Economia*, n. 1, 2019, p. 47 ss.; G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del Diritto*, n. 2, 2019, pp. 199 ss.; G. Proietti, *Intelligenza artificiale: una prima analisi della proposta di regolamento europeo*, in *Diritto bancario*, 2021; G. Di Rosa, *Quali regole per i sistemi automatizzati?*, in *Riv. Dir. Civ.*, n. 5, 2021, p. 823; M. Craglia (a cura di), *Artificial Intelligence - A European Perspective*, Lussemburgo, 2018).

[35] Sul punto cfr. G. Lemme, *La proposta di Regolamento europeo sulla intelligenza*

La circostanza che oggi il Regolamento preveda solo due livelli di rischio rinviene da una modifica sostanziale rispetto a quanto originariamente previsto nella proposta che, invece, distingueva tre livelli di rischio «i) un rischio inaccettabile - ad esempio quelle che violano i diritti fondamentali e non sono immettibili nel mercato -; ii) un rischio alto; iii) un rischio basso o minimo»[36].

La scelta di rimuovere la classificazione a "rischio basso o minimo" introduce un regime residuale nel quale dovrebbero ricadere tutti quei sistemi di IA non classificabili nei primi due e, pertanto, dovrebbero essere disciplinati (oltre che dalle previsioni generali dell'AI ACT) anche da altri strumenti giuridici unionali e/o nazionali[37].

Durante il suo *iter* legislativo, il Regolamento non è rimasto esente da critiche. Se per un verso si è posto in evidenza come esso possa portare alla creazione di categorie normative astratte e non adeguate ai singoli sistemi immessi nel mercato; per altro verso, è stata lamentata una assenza della figura umana e del rapporto uomo-macchina, che dovrebbe essere proprio il primo soggetto da tutelare[38] e una certa «vaghezza e lacunosità»[39] sul controllo esercitabile nello sviluppo dei sistemi che la proposta relega ad un controllo interno del fornitore.

Numerosi sono anche i rilievi sollevati dalle stesse autorità di regolazione sulla proposta di Regolamento, in particolare in merito alla definizione di IA fornita dalla Commissione, che è stata ritenuta troppo stringente, necessitando piuttosto di un «un approccio adattivo ed evolutivo»[40].

---

artificiale e la gestione dei rischi: una battaglia che può essere vinta?, in *Rivista trimestrale di Diritto dell'economia*, A. Canepa, G.L. Greco (a cura di), *Liber amicorum Laura Ammannati*, suppl. al n. 1, 2024, spec. p. 259.

[36] Commissione europea, *Proposta di regolamento*, cit., punto 5.2.2, p. 14.

[37] Come potrebbe essere l'applicazione del Regolamento sulla sicurezza generale dei prodotti (Regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio del 10 maggio 2023 relativo alla sicurezza generale dei prodotti, che modifica il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio e la direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, e che abroga la direttiva 2001/95/CE del Parlamento europeo e del Consiglio e la direttiva 87/357/CEE del Consiglio (Testo rilevante ai fini del SEE) per le IA immessi sul mercato come beni di consumo.

[38] Entrambe le problematiche sono state sollevate da G. Contissa, F. Galli, F. Godano e G. Sartor, *Il Regolamento Europeo sull'Intelligenza Artificiale. Analisi informatico-giuridica*, in *i-lex*, vol. 14, fasc. 2, 2021, pp. 32 e 33.

[39] C. Grieco, *Sorveglianza e controllo. Il modello di governance nella nuova proposta di regolamento sull'IA*, in *i-lex*, vol. 14, fasc. 2, 2021, pp. 95-99.

[40] Comitato delle Regioni, 147ª *Sessione Plenaria del CDR, 1.12.2021 - 2.12.2021. Parere del Comitato europeo delle regioni - Approccio europeo in materia di intelligenza artificiale - Legge sull'intelligenza artificiale*, in Gazzetta ufficiale dell'Unione Europea C

Dall'altra parte anche l'approccio basato su elenchi è stato oggetto di pareri negativi, poiché ritenuto a rischio di «generalizzare una serie di impieghi (dell'IA)», e ciò deriverebbe dalla circostanza che «il rispetto dei requisiti stabiliti per l'IA ad alto e medio rischio[41] non riduce necessariamente i rischi di un pregiudizio alla salute, alla sicurezza e in generale ai diritti fondamentali associati a tutta l'IA ad alto rischio»[42].

Anche il sistema basato sul rischio, sul quale si fonda il Regolamento, non appare pienamente condivisibile. Come lo stesso termine Intelligenza Artificiale indica, si tratta di sistemi "intelligenti" (tenendo comunque conto della macrodistinzione tra IA forte e IA debole), in grado di apprendere in maniera più o meno autonoma. In via teorica, tutti i sistemi di IA dovrebbero intendersi ad "alto rischio", non distinguendo per il settore in cui essi debbano essere impiegati ma proprio perché la tecnologia è intrinsecamente ad alto rischio. Se l'IA non fosse stata considerata una tecnologia ad alto rischio sin dal principio, sarebbe stato sufficiente applicare una normativa già vigente[43], senza elaborare un apposito regolamento.

Altresì, è stato rilevato che l'A.I. Act ha un orientamento esplicito agli obiettivi del mercato interno e si allontana dalla più tradizionale legislazione dell'UE in materia di sicurezza che esplicitamente tutela determinati diritti (su tutti quello della privacy del GDPR). In particolare, l'«AI Act può talvolta sembrare più

97/60, 28 febbraio 2022, p. 2.

[41] Il "rischio medio" è stato poi rimosso nella versione definitiva del Regolamento.

[42] Parere del Comitato economico e sociale europeo sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, 2021/C 517/09, p. 2.

[43] Nel *corpus* di norme Europee applicabili e adattabili ai sistemi di IA possono citarsi, in maniera esemplificativa e non esaustiva, la Direttiva 2001/95/CE in materia di sicurezza dei prodotti e di responsabilità per danno da prodotti difettosi (che prevede norme specifiche volte a regolare diverse categorie di prodotti; la Direttiva 2000/43/CE sull'uguaglianza razziale; la direttiva 2000/78/CE sulla parità di trattamento in materia di occupazione e di condizioni di lavoro; le direttive 2004/113/CE e 2006/54/CE sulla parità di trattamento tra uomini e donne per quanto riguarda l'accesso a beni e servizi e in materia di occupazione; la direttiva 2005/29/CE sulle pratiche commerciali sleali; la direttiva 2011/83/CE sui diritti dei consumatori; il Regolamento 2016/679 sulla protezione dei dati personali e sulla privacy; la Direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giudiziarie (relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati) e la Direttiva (UE) 2019/882 sui requisiti di accessibilità dei prodotti e dei servizi.

vicino a strumenti orientati al mercato, come la legge sui mercati digitali, che a strumenti espressi in termini di diritti fondamentali, come il GDPR»[44].

Alla luce di ciò il regolamento che, se *prima facie* può sembrare meramente tassonomico e in linea con gli altri regolamenti europei in materia digitale, ha una concreta portata economica.

Sul punto possono richiamarsi due circostanze esemplificative.

In primo luogo, nell'AI Act, viene fatto esplicito divieto di immissione sul mercato(art. 5, c. 1, lett. D) «di un sistema di IA per effettuare valutazioni del rischio relative a persone fisiche al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità; tale divieto non si applica ai sistemi di IA utilizzati a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa»[45]. Il riferimento appare esplicito nei confronti dei c.d. Risk Assesment Tools che vengono impiegati (principalmente negli Stati Uniti, ma anche in Spagna e Inghilterra) per la valutazione del rischio degli imputati e che negli anni sono stati oggetto di studio e di critica[46]. Tali strumenti, che secondo l'AI Act non dovrebbero essere

---

[44] Così tradotto M. Almada, N. Petit, *The EU AI act: a medley of product safety and fundamental rights?*, in *Robert Schuman Centre for Advanced Studies Working Paper*, n. 59, 2023, pp. 11-12.

[45] Art. 5, c. 1, lett. d).

[46] Cfr. *ex multis* C. Slobogin, *Preventive lustice: How Algorithms, Paro le Boards and Limiting Retributivism Could End Mass Incarceration*, in *Wake Forest L. Rev.*, n. 97, 2021; S. Zottola, S. Desmarais, E. Lowder, S. Duhart Clarke, *Evaluating Fairness of Algorithmic Risk Assessment Instruments: The Problem With Forcing Dichotomies*, in *Criminal Justice and Behavior*, n. 49, 2021; G. Vincent, J. Viljoen, *Racist Algorithms or Systemic Problems? Risk Assessments and Racial Disparities*, in *Crim. & Behav.*, n. 47, 2020, p. 1576; J. Skeern, C. Lowenkamp, *Using Algorithms to Address Trade-Offs Inherent in Predicting Recidivism*, in *Behav. Sci. & L.*, n. 259, 2020; T.H. Cohen, C. Lowenkamp, K. Bechtel e F.W. Flores, *Risk Assessment Overrides: Shuffling the Risk Deck Without Any Improvements in Prediction*, in *Crim. Just., Sc Behav.*, n. 49, 2020, p. 1609; F. Basile, *Intelligenza Artificiale e Diritto Penale: Quattro possibili percorsi di indagine*, in *Diritto Penale e Uomo – DPU*, 29 settembre 2019; B. Garrett, J. Monahan, *Judging Risk*, in *Calif. L. Rev.*, vol. 108, 2020, p. 439 e ss.; A. Natale, *Introduzione. Una giustizia (im)prevedibile?*, in *Questione Giustizia*, fasc. 4, 2018, pp. 3 ss.; J. Dressel, H. Farid, *The Accuracy, Fairness, and Limits Of Predicting Recidivism*, in *Sci. Advances*, n. 4, 2018; J.M. Eaglin, *Constructing Recidivism Risk*, in *Emory L. J.*, n. 67, 2017; G. Zara, *Tra il probabile e il certo. La valutazione del rischio di violenza e di recidiva criminale*, in *Diritto penale contemporaneo*, 20 maggio 2016; R. Berk, J. Hyatt, *Machine learning Forecasts of Risk to Inform Sentencing Decisions*, in *Fed, Sent'g Rep.*, n. 27, 2015, p. 222 ss.; P.B.

immessi sul mercato, sono allo stato attuale (in Europa) meri algoritmi di calcolo statistico e non sistemi di "Intelligenza Artificiale" assoggettabili al Regolamento europeo. Con l'entrata in vigore di quest'ultimo, è molto elevata la probabilità che le imprese produttrici perdano interesse nel finanziamento della ricerca su tali strumenti, portando ad una situazione di stallo nel loro sviluppo e nell'effettuare il salto da algoritmo a sistema intelligente. Ciò a discapito sia della ricerca tecnologica in sé, sia anche di coloro che subiscono gli effetti di tali applicativi, che potrebbero beneficiare da un miglioramento della stessa attraverso la tutela normativa.

In secondo luogo, il Regolamento sembra tenere conto, solo in parte, del c.d. "cambiamento tecnologico" che caratterizza tecnologie digitali, la cui peculiarità risiede in una instabilità evolutiva[47] a cui deve far fronte il legislatore attraverso aggiornamenti e sperimentazioni normative (le c.d. *sandboxes*), che comunque sono state inserite nell'AI Act. La questione sorge sulla fattibilità di tale approccio. Dalla proposta al regolamento definitivo hanno preso piede (in meno di tre anni) le *General-Purpose Artificial Intelligence* (GPAI) che hanno già raggiunto il mercato *mainstream* (Chat GPT su tutti) e tali fattispecie sono state inserite direttamente all'interno dell'AI Act (art. 51) ma tale approccio appare insostenibile nel lungo termine anche solo in riferimento alle stesse GPAI.

Questo perché, come è stato evidenziato, se la *governance* si elabora «nelle prime fasi dello sviluppo tecnologico» si «potrebbero perdere informazioni importanti sulle tecnologie di IA di uso generale e sul loro impatto sulla società, portando a soluzioni inadeguate ai problemi legali»; se, invece, si agisse tardivamente la regolamentazione sarebbe «adottata solo una volta che gli effetti negativi di queste tecnologie saranno già manifesti, con conseguenze potenzialmente catastrofiche»[48].

È probabile che tali "conseguenze catastrofiche" rappresentino uno dei principali motivi dell'azione regolatoria preventiva che è stata posta in essere, nonché della c.d. "*regulatory brutality*"[49] posta in essere attraverso il Regolamento, tesa alla quasi totale inosservanza da parte del legislatore europeo dei sistemi giuridici degli Stati membri[50] nella regolamentazione delle tecnologie digitali.

Imrey, A.P. Dawid, *A Commentary on Statistical Assessment of Violence Recidivism Risk*, in *Stat. & Pub. Pol'y*, vol. 2, 2015.

[47] S. Hooker, *The Hardware Lottery*, in *Communication of the ACM*, n. 64, 2021, pp. 58 ss.

[48] M. Almada, N. Petit, *The EU AI act*, cit., p. 14.

[49] V. Papakonstantinou, P. de Hert, *The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of 'Act-ification', 'GDPR Mimesis' and 'EU Law Brutality'*, Londra, 2024.

[50] Sul punto può richiamarsi il parere circostanziato (C(2024) 7814) che la

Invero, le conseguenze di tali scelte potrebbero anche spingere le imprese a rinunciare al progresso e alla ricerca a favore di un "*dumbing down*" o "*de-AI-ing*" dei propri prodotti al solo fine di evitare l'adeguamento alla normativa[51], il tutto a discapito del mercato e del progresso tecnologico, che sono, invece, costantemente attenzionati nella programmazione economica europea.

3. Governance *e incentivazione tecnologica*

Come si è già avuto modo di accennare, tra attività legislativa e progresso tecnologico vi è una interconnessione che, però, quando trattasi di IA, diviene più sinergica.

Per porre in evidenza l'importanza di tale rapporto, è utile osservare quello che è l'approccio statunitense sul punto. Negli ultimi anni, difatti, parallelamente all'evoluzione della legislazione sull'IA in Europa, gli Stati Uniti hanno introdotto una serie di atti che non solo favoriscono lo sviluppo e la ricerca in materia ma, altresì, sembrano allontanarsi, almeno in parte, dalla impostazione liberista che ne caratterizza l'economia anche in materia tecnologica, trattandosi, in prevalenza, di misure di sostegno delle imprese delle attività economiche domestiche. Tra le iniziative possono citarsi il *National Artificial Intelligence Initiative Act* del 2020 che promuove e sovvenziona gli sforzi di innovazione dell'IA nelle principali agenzie federali, per guidare la ricerca e lo sviluppo americani nella tecnologia dell'IA e sostenere l'uso della medesima tecnologia nell'apparato pubblico. Il successivo *Blueprint for an AI Bill of Rights*[52] del 2022, invece, ha in-

---

Commissione europea ha trasmesso all'Italia, il 5 novembre 2024, in merito al Disegno di Legge 1146/2024 "Disposizioni e delega al Governo in materia di intelligenza artificiale". Nel parere, che sembra avere un approccio di tipo "demolitorio" nei confronti dell'iniziativa italiana, sono sollevate diverse questioni critiche, che vanno dalla mancanza di coerenza nelle definizioni e nei riferimenti tra l'AI Act e il Disegno di Legge, sino a problematiche più profonde, come le limitazioni proposte per sistemi di IA non considerati ad "alto rischio" e la problematica della possibile introduzione di due sistemi normativi distinti (italiano ed europeo) che potrebbero danneggiare l'approccio europeo sul coordinamento normativo(per i punti principali si rinvia a Legislatura 19ª - 4ª Commissione permanente, *Parere approvato dalla commissione sugli emendamenti relativi al Disegno di Legge n. 1146*, in Resoconto sommario n. 214 del 27/11/2024, reperibile all'indirizzo https://www.senato.it/japp/bgt/showdoc/19/SommComm/0/1435866/index.html?part=doc_dc-allegato_a:1.

[51] L. Floridi, *On the Brussels-Washington Consensus About the Legal Definition of Artificial Intelligence*, in *Philosophy & Technology*, vol. 36, 2023, p. 4.

[52] The White House, *Blueprint for an Ai Bill Of Rights Making Automated Systems Work For The American People*, Washington, ottobre 2022.

trodotto una serie di principi guida e non vincolanti per lo sviluppo sicuro e protetto dell'IA. Negli Stati Uniti, la complessità insita nella forma di Stato federale ha reso difficile l'attuazione di una politica unificata sull'intelligenza artificiale e, ad oggi, non esiste una legge generale sull'IA ma, tra le iniziative più recenti e significative, può richiamarsi l'ordine esecutivo sullo "Sviluppo e uso sicuro, protetto e affidabile dell'IA", emesso il 30 ottobre 2023[53] che, però, rappresenta comunque un atto programmatorio non vincolante.

Si denota, quindi, come la regolamentazione dell'IA negli Stati Uniti consista in varie iniziative anche a livello federale[54] che, però, non riconducono ad una strategia centralizzata, lasciando libertà quasi assoluta alle imprese che sviluppano questo tipo di *software*; tant'è che nei diversi documenti citati l'obiettivo generale è quello del mantenimento della posizione di *leadership* nel campo IA a livello globale[55].

Di pari passo con la politica di *governance*, i finanziamenti pubblici costituiscono uno dei mezzi principali statunitensi utilizzati per garantire uno sviluppo costante nel settore dell'IA tant'è che a partire dal 2015 si è avuto un notevole incremento degli stessi[56].

---

[53] J.R. Biden Jr., *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, Washington, 30 ottobre 2023.

[54] Che spesso affrontano solo aspetti specifici, come il California Consumer Privacy Act (Civil Code, Civ Division 3, Obligations Part 4, Title 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100]), che disciplina l'IA nel processo decisionale automatizzato.

[55] L. Fabiano, *Il Liberal-protezionismo digitale statunitense fra difesa della leadership nel mercato tecnologico e sicurezza nazionale*, in *DPCE-online*, n. 3, 2023, p. 2339.

[56] Ad esempio, nel dicembre 2021, la National Science and Technology Council ha pubblicato un documento (The Networking & Information Technology R&D Program and the National Artificial Intelligence Initiative Office, *Supplement to the President's fy2022 budget*, dicembre 2021, consultabile all'indirizzo https://www.whitehouse.gov/wp-content/uploads/2021/12/FY2022-NITRD-NAIIO-Supplement.pdf) sullo stanziamento di fondi pubblici per il settore di ricerca sviluppo dell'IA per i dipartimenti di Networking and Information Technology Research and Development (NITRD) e il National Artificial Intelligence Initiative. Secondo il report per l'anno 2021 le sole agenzie governative non dedicate alla difesa degli Stati Uniti hanno stanziato fondi pari a 1.53 miliardi di dollari per la ricerca e sviluppo, con la prospettiva di aumentare dell'8.8% per il 2022. Ciò dimostra l'interesse degli Stati Uniti al finanziamento della ricerca nel settore pubblico e non soltanto a quello militare e della difesa (per un confronto tra i diversi approcci cfr. C. Cath, S. Watcher, B. Mittelstadt, M. Taddeo, L. Floridi, *Artificial Intelligence and the "Good Society": the US, EU and UK approach*, in *Science and Engineering Ethics*, n. 2, 2018, pp. 503 ss.)

Il bilancio per l'anno fiscale 2025[57] ha introdotto un nuovo regime di investimenti strategici per scienza e tecnologia (S&T), facendo seguito all'Executive Order 13859[58], con il quale era stato richiesto un approccio standardizzato per tenere conto in modo accurato degli investimenti in ricerca e sviluppo nell'IA in tutto il governo federale, e nel quale si sintetizzava la strategia generale statunitense in materia con il «promuovere i progressi nella tecnologia e nell'innovazione, proteggendo al contempo la tecnologia, l'economia e la sicurezza nazionale americane per garantire che l'America continui a guidare il mondo nell'innovazione e che le scoperte scientifiche e tecnologiche vadano a beneficio di tutta l'America»[59].

La strategia statunitense conferma come gli investimenti, la programmazione degli interventi e la propensione al rischio per lo sviluppo tecnologico non siano prerogative del solo mercato privato ma, al contrario, siano conseguenza di un preventivo intervento pubblico. L'efficacia di quest'ultimo deriva non solo dal mero stanziamento di fondi e dalla creazione delle "condizioni giuste" per l'innovazione ma, soprattutto, dalla «capacità dello Stato di prefigurare lo spazio di opportunità, la volontà di impegnarsi nelle attività di ricerca più rischiose e dall'esito più incerto e la supervisione del processo di commercializzazione»[60]. Sono numerose le imprese fondate negli Stati Uniti che oggi ricoprono una posizione dominante (o monopolistica) nel mercato globale perché hanno promosso e sviluppato tecnologie di frontiera anche grazie all'intervento pubblico.

La politica interventista statunitense, quindi, si discosta molto da quella europea e fonda su un minore controllo in materia di sviluppo e commercializzazione

---

[57] The White House - Office Of Management And Budget, Budget of the U.S. Government Fiscal Year 2025, Washington, 2024, https://www.whitehouse.gov/wp-content/uploads/2024/03/budget_fy2025.pdf. A scopo esemplificativo, il bilancio prevede 202 miliardi di dollari per la ricerca e lo sviluppo anche per finanziare lo sviluppo dell'IA e gestirne i rischi. Altresì il bilancio stanzia 99 miliardi di dollari nella ricerca di base e applicata per guidare lo sviluppo di tecnologie, prodotti e servizi all'avanguardia del futuro.

[58] Executive Order 13859 of February 11, 2019, *Maintaining American Leadership in Artificial Intelligence*, in *Federal Register*, Vol. 84, No. 31, February 14, 2019.

[59] *Ibidem*, 1. Sul punto cfr. anche The Select Committee on Artificial Intelligence of The National Science and Technology Council National Artificial Intelligence, *Research and Development Strategic Plan 2023 Update*, May 2023. Sullo stato degli investimenti cfr. Artificial Intelligence Research and Development Interagency Working Group Subcommittee on Networking & Information Technology Research & Development and the Subcommittee on Machine Learning & Artificial Intelligence of the National Science & Technology Council, *2020–2024 Progress Report: Advancing Trustworthy Artificial Intelligence Research and Development*, July 2024.

[60] M. Mazzucato, *Lo stato innovatore*, Bari, IIa ed., 2020, p. 103.

dell'IA e un'incentivazione alla ricerca anche a livello pubblico. Tali scelte appaiono divergenti rispetto alle strategie unionali.

Innanzitutto, negli ultimi anni, a far data dalla crisi pandemica, la Commissione europea ha dato il via ad una politica di flessibilizzazione degli aiuti di Stato, con una visione programmatoria volta a favorire un nuovo intervento pubblico dinamico anche, e soprattutto, per la crescita del mercato tecnologico interno.

Tra le diverse iniziative, su tutte, deve segnalarsi la comunicazione n. 414/2022 della Commissione europea, con la quale sono stati fissati i nuovi orientamenti semplificatori in materia di concessione di aiuti di Stato a favore della ricerca, dello sviluppo e dell'innovazione[61]. Tali orientamenti prevedono che per la concessione degli aiuti debbano verificarsi determinate condizioni: l'effetto di incentivazione (l'impresa svolge attività ulteriori rispetto a quelle che essa non svolgerebbe o svolgerebbe in modo limitato qualora l'aiuto non vi fosse stato); rapporto di causa-effetto (l'attività di RSI deve aver luogo solo dopo la concessione dell'aiuto); sviluppo sia tangibile per il mercato (se il mercato da solo non fornisce uno sviluppo tangibile o è presente un fallimento di mercato, lo Stato può intervenire).

Sullo stesso filone si posiziona la modifica al Regolamento generale di esenzione per categoria[62] del 2023 con la quale è stato precisato che gli aiuti alla ricerca industriale in qualsiasi ambito industria e settore, possono essere esentati dall'obbligo di notifica, con la specificazione dell'IA tra le tecnologie compatibili con la concessione degli aiuti. Ciò, insieme alla comunicazione sulla strategia europea di sicurezza economica del 2023[63], che punta alla promozione della base economica e della competitività nel mercato europeo, e alle raccomandazioni sui settori tecnologici critici per la sicurezza economica[64], tra cui l'intelligenza artifi-

---

[61] Communication from the Commission Framework for State aid for research and development and innovation 2022/C 414/01, C/2022/7388, GU C 414 del 28.10.2022.

[62] Regolamento (UE) 2023/1315 della Commissione del 23 giugno 2023 recante modifica del regolamento (UE) n. 651/2014 che dichiara alcune categorie di aiuti compatibili con il mercato interno in applicazione degli articoli 107 e 108 del trattato e del regolamento (UE) 2022/2473 che dichiara compatibili con il mercato interno, in applicazione degli articoli 107 e 108 del trattato sul funzionamento dell'Unione europea, alcune categorie di aiuti a favore delle imprese attive nel settore della produzione, trasformazione e commercializzazione dei prodotti della pesca e dell'acquacoltura (Testo rilevante ai fini del SEE).

[63] Comunicazione congiunta al Parlamento europeo, al Consiglio europeo e al Consiglio sulla "Strategia europea per la sicurezza economica" JOIN/2023/20 final, 20 giugno 2023.

[64] Raccomandazione (UE) 2023/2113 della Commissione del 3 ottobre 2023

ciale, rappresentano alcune delle iniziative di promozione dello sviluppo dell'IA nel mercato europeo.

In tal modo, gli stati e la stessa Unione Europea divengono soggetti promotori dell'innovazione tecnologica, anche individuata quale «fattore di rivalutazione della costituzione economica»[65], ma facendo leva sugli aiuti di Stato che, però, sembrano essere sempre più incentivi e meno aiuti, lontani dalle disposizioni (rimaste immutate) dell'art. 107 TFUE che, tuttavia, almeno in taluni aiuti di carattere orizzontale, sembra aprire nuovi spazi di regolazione materiale in chiave di flessibilizzazione, consentendo, di fatto, una maggiore "apertura" verso la concessione di incentivi pubblici.

4. *Note conclusive*

La prospettiva giuridico-economica che l'Unione sta implementando, almeno a partire dalla fase neoprogrammatoria, nei confronti degli aiuti di Stato volti ad incentivare lo sviluppo tecnologico, sembra similare a quella statunitense ma confligge con le scelte di regolazione contenute nell'AI Act.

Il Regolamento europeo rappresenta un atto dovuto e necessario per garantire la tutela del mercato e, soprattutto, dei diritti fondamentali, ma non consente una totale libertà di ricerca e sviluppo così come garantita negli Stati Uniti. Pertanto, l'approccio basato sul rischio e, in particolare, il divieto di commercializzare determinati sistemi di IA non sarebbe compatibile con il regime di aiuti rivolti alla ricerca e allo sviluppo della tecnologia in esame.

Appare, quindi, contraddittorio il rapporto tra AI Act e la flessibilizzazione degli aiuti di Stato che sta caratterizzando le politiche europee in materia. La regolamentazione «prudente» della tecnologia e una semplificazione della normativa in materia di aiuti non sembrano seguire un piano coordinato che, allo stato attuale, consente di osservare una evidente contraddizione. Da un lato, una *deminutio* delle possibilità di ricerca e sviluppo derivante dall'articolazione e dai vincoli del Regolamento e dall'altro, vivaci iniziative di incentivazione economica in materia tecnologica per rafforzare la posizione europea nel mercato globale.

Sotto taluni profili, peraltro, non può omettersi di rilevare come in futuro possano emergere notevoli contrasti normativi. Si pensi, a titolo esemplificativo, alla ipotesi in cui venga concesso un aiuto per lo sviluppo di un sistema di IA che,

---

relativa ai settori tecnologici critici per la sicurezza economica dell'UE ai fini di un'ulteriore valutazione dei rischi con gli Stati membri, 11 ottobre 2023.

[65] G. Luchena, *Le crisi e il nuovo intervento pubblico nell'economia*, in E. Bani, F. Di Porto, G. Luchena e E. Scotti, Lezioni *di Diritto dell'economia*, Torino, 2023, p. 120.

durante la lavorazione, proprio a causa del c.d. cambiamento tecnologico viene poi riconosciuto dalla Commissione come un sistema a rischio inaccettabile. Ciò vanificherebbe lo sforzo della ricerca e, soprattutto, lo sforzo economico statale con il quale si è contribuito allo sviluppo.

Pertanto, appare evidente come ove un'impresa individua i sistemi di IA sui quali investire, potrebbe riservarsi di evitare i campi già vietati *ex ante* dal Regolamento e la scelta ricadrebbe su sistemi dalla commercializzazione più sicura, ovvero in un "*de-AI-ing*" dei sistemi già sviluppati al fine di garantirne la commercializzazione e il conseguente profitto, a discapito della ricerca scientifica che costituisce forse l'unico mezzo per la corsa alle tecnologie di frontiera.

Non solo, è possibile anche che la struttura dell'AI Act possa limitare lo *spillover* tecnologico di cui può beneficiare il mercato europeo, a causa della disincentivazione delle aziende extraeuropee a non importare i propri prodotti perché il regolamento è troppo stringente e il rapporto costi/benefici potrebbe non essere tale da giustificare una modifica *software* che lo renda compatibile con il mercato interno[66].

Conclusivamente, se è vero che governare l'IA è una questione di equilibrio e di ritmo, otre che di intensità regolatoria, nel caso europeo, però, da un lato non sembra essere presente un equilibrio tra regolazione e promozione della tecnologia perché l'ago della bilancia tende a favore del primo; d'altro canto, invece, sembra esservi un certo "ritmo", poiché l'AI Act è entrato in vigore in un momento storico nel quale la tecnologia è ancora in divenire e la sua commercializzazione è in grado di essere controllata in maniera più semplice.

Oggi, in un contesto in cui i prodotti disponibili si basano esclusivamente su IA deboli (*weak A.I.*) [67] - sistemi progettati per svolgere compiti specifici senza

---

[66] Per tali motivi, forse, una *sandbox* (G. Lo Sapio, *Il regolatore alle prese con le tecnologie emergenti. La* regulatory sandbox *tra principi dell'attività amministrativa e rischio di illusione normativa*, in *Federalismi.it*, n. 20, 2022, 16 ss.; o una sperimentazione normativa (S. Ranchordás, *Experimental Regulations and Regulatory Sandboxes – Law Without Order?*, in *Law and Method*, n. 1, 2021) a livello europeo per la regolazione dell'IA avrebbe permesso di affrontare preliminarmente le questioni ancora non risolte che caratterizzano l'AI Act, così come è stato fatto con l'European Blockchain Regulatory Sandbox. Sul punto, inoltre, si è posto in evidenza come «experimental regulations and regulatory sandboxes have recently been regarded as regulatory tools that can be employed to stimulate innovation» (così S. Ranchordas, V. Vinci, *Regulatory Sandboxes and Innovation-Friendly Regulation: Between Collaboration and Capture*, in *Italian Journal Of Public Law*, Vol. 16, Iss. 1, 2024, p. 113).

[67] L'Intelligenza Artificiale Forte, invece, va oltre l'essere un mero strumento e diviene una fattispecie autonoma con capacità cognitive speculari a quelle dell'essere umano. L'idea della vicinanza tra uomo e macchina risale, però, ad un periodo ben precedente rispetto anche all'invenzione del calcolatore elettronico. Ad esempio,

capacità di pensiero o azione autonoma -, il divieto aprioristico imposto dal Regolamento su talune tipologie di IA rischia di frenare prematuramente e compromettere la competitività europea nel mercato globale[68].

Proprio la leadership, inoltre, sembra essere indissolubilmente legata proprio all'intensità regolatoria che, se troppo profonda potrebbe allontanare eccessivamente l'industria privata dagli obiettivi di sovranità digitale (globale) che caratterizzano tutte le più recenti iniziative europee e, se troppo mite, potrebbe, invero, ingenerare un allentamento della proiezione europea volta a rafforzare le imprese nella competizione globale sui sistemi di intelligenza artificiale prodotti nei mercati extra UE.

Thomas Hobbes (1588-1679) paragonò il ragionamento umano al compiere operazioni matematiche affiancando la ragione ad una macchina calcolatrice e nel *Leviatano* (1651) ideò un «animale artificiale» sostenendo: «che cos'è infatti il cuore se non una molla e che cosa sono i nervi se non altrettanti fili e che cosa le giunture se non altrettante ruote che danno movimento all'intero corpo». Anche Leibniz (1646-1716), come Hobbes, riteneva che «ragionare equivalesse a calcolare».

[68] Sul punto è stato osservato che «il regolamento IA rappresenta un potenziale (ma forse solo illusorio) limite al potere delle corporation che possono influenzare le vite dei cittadini/consumatori europei e le economie dei Paesi membri» (così G. Luchena, *Tecnologie, mercati e regolazione dell'economia: il caso dell'intelligenza artificiale*, in *Dialoghi di Diritto dell'Economia*, ottobre 2024, pp. 10-11).

Riconciliare innovazione e regolamentazione: il ruolo delle *regulatory sandboxes* nell'Unione europea

di **Enza Cirone**

1. *Introduzione*

L'accelerazione dello sviluppo tecnologico ha trasformato profondamente la nostra società, sollevando perplessità rispetto alla capacità del quadro normativo di affrontare nuove sfide[1] e armonizzare i diversi approcci regolatori tra le giurisdizioni nazionali[2].

L'innovazione tecnologica richiede al legislatore di trovare un equilibrio, talvolta complesso, tra la promozione dell'innovazione e la tutela degli interessi

* L'Autrice desidera ringraziare i proff. Andrea Deffenu e Daniele Amoroso per l'organizzazione del convegno, nonché i proff. Corrado Chessa e Federico Cappai per gli utili commenti a valle della relazione. Per una versione estesa del contributo, si veda: E. Cirone, *Gli spazi di sperimentazione normativa nell'Unione europea: regolamentare l'innovazione tra principi e prassi applicative*, in *Rivista italiana di informatica e diritto*, 2025, pp. 1-22.

[1] Per una disamina degli approcci adottati dall'Unione europea per migliorare il processo decisionale a lungo termine e la capacità di risposta alle sfide future, v. G. Umbach, *Futures in EU governance: Anticipatory governance, strategic foresight and EU Better Regulation*, in *European Law Journal*, 2024, pp. 409-421.

[2] La regolazione è talvolta considerata nell'ottica di mitigazione dei rischi: «[regulation is an] organized attempt to manage risks or behaviour in order to address a collective problem or concern», K. Yeung, *Are human biomedical interventions legitimate regulatory policy instruments?*, in R. Brownsword, E. Scotford e K. Yeung (edited by), The Oxford handbook of law, regulation and technology, Oxford, 2017, p 11.

pubblici. Ciò comporta decisioni fondamentali riguardo all'opportunità di intervenire, quale approccio adottare, se coinvolgere gli *stakeholders* e se valutare eventuali modifiche normative.

In tale contesto[3], l'Unione europea ha adottato un approccio flessibile[4], basato sul principio di neutralità tecnologica, che garantisce libertà di scelta senza imposizioni, evitando discriminazioni tra tecnologie.

Questo approccio comporta due sfide principali: garantire normative neutrali ed eque e adattare le regole alle peculiarità di ogni tecnologia[5]. Negli ultimi

---

[3] Con riferimento all'intelligenza artificiale, Parlamento europeo 2022, Risoluzione del Parlamento europeo del 3 maggio 2022 sull'intelligenza artificiale nell'era digitale, https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_IT.html, punto 121.

[4] La Commissione, già nei primi anni Duemila, aveva mostrato un crescente interesse verso i cosiddetti metodi alternativi di regolazione. A tal proposito, basti citare il Libro bianco della Commissione sulla Governance europea del 2001 e il successivo Accordo interistituzionale del 2003, che ne ha recepito parzialmente i contenuti. Questi documenti testimoniano una tendenza che, nei vent'anni successivi, si sarebbe consolidata – sebbene non priva di contraddizioni – nell'obiettivo di migliorare sia la qualità della legislazione europea sia le procedure decisionali. Tale percorso si è inserito nel quadro più ampio delle iniziative volte alla razionalizzazione normativa, quali le proposte di Better Regulation e Smart Regulation. V. Commissione europea, *La governance Europea - Un libro bianco*, COM(2001) 428; Parlamento europeo, Consiglio, Commissione, *Accordo interistituzionale «Legiferare meglio»*, 2003/C 321/01, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32003Q1231(01), sostituito dall'Accordo Interistituzionale del 13 aprile 2016, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016Q0512%2801%29. Riguardo ai due programmi, v. European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions*, *A strategic review of better regulation in the European Union*, COM(2006) 689; European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Second strategic review of Better Regu-lation in the European Union*, COM(2008) 32; European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions,"Smart Regulation in the European Union"*, COM(2010) 543. Cfr anche M.E. Bartoloni, *La regolazione privata nel sistema costituzionale dell'Unione europea. Riflessioni sulla disciplina relativa al settore dell'innovazione*, in *Osservatorio sulle fonti*, 2021, pp. 1331-1355.

[5] Questo aspetto è chiaramente evidenziato nei Principi UNIDROIT sui Beni Digitali e sul Diritto Privato, i quali esprimono preoccupazione su questo fronte, v. https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf.

anni, sono emersi strumenti come clausole sperimentali, *sandboxes* regolatorie e politiche temporanee, noti come "spazi di sperimentazione normativa"[6], che consentono di testare innovazioni in ambienti reali, adattando le politiche[7] in maniera dinamica.

Nel 2020, il Consiglio[8] ha riconosciuto le *sandboxes* come strumenti strategici per un quadro normativo flessibile e orientato all'innovazione, generando impatti significativi per PMI e start-up. Parallelamente, la Commissione Europea, attraverso l'Agenda per l'innovazione, iniziative come il Programma Europa Digitale[9] e la Better Regulation Toolbox, ha integrato questi approcci. Quest'ultima, pur valorizzando le clausole sperimentali come strumenti flessibili, definisce le *sandboxes* come quadri sperimentali sofisticati. In realtà, le *regulatory sandboxes* si configurano come strumenti di co-regolazione più complessi rispetto alle semplici clausole sperimentali, caratterizzati da misure *ad hoc* e monitoraggio continuo. Esse consentono l'elaborazione di normative basate su evidenze tecniche specifiche, pur presentando rischi potenziali di abuso da parte degli innovatori[10] o di

---

[6] Cfr. European Law Institute (ELI) 2022, *Principles on Blockchain Technology, Smart Contracts and Consumer Protection*: "Principle 3 – Case Specific Approach: "Principle 3 – Case Specific Approach - In the application of the PRINCIPLES it should, for each Principle and in each specific case, be considered which type of BLOCKCHAIN is used and who the parties involved are, and which type of SMART CONTRACT is used, as referred to in Principle 2."

[7] Alcuni autori, tuttavia, sostengono criticamente che sia impraticabile disciplinare in modo esaustivo il futuro, S. Garben, *A taste of its own medicine: assessing the impact of the EU Better Regulation Agenda*, in *European Law Journal*, 2020, p. 93; A. de Boer, *Scientific assessments in European food law: Making it future-proof*, in *Regulatory Toxicology and Pharmacology*, 2018; S. Ranchordás, M. van't Schip, *Future-Proofing Legislation for the Digital Age*, in S. Ranchordás & Y. Roznai (edited by), *Time, Law, and Change: An Interdisciplinary Study*, Dublino, 2020.

[8] Consiglio dell'Unione europea 2020, Conclusioni del Consiglio sugli spazi di sperimentazione normativa e le clausole di sperimentazione come strumenti per un quadro normativo favorevole all'innovazione, adeguato alle esigenze future e resiliente che sia in grado di affrontare le sfide epocali nell'era digitale.

[9] Regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio del 29 aprile 2021 che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240.

[10] «[…] [T]oo often sandboxes are misunderstood, misused, or mismanaged. Regulatory agencies should use sandboxes to keep up to date with fast-paced innovation and promote market competition without sacrificing consumer protection. Real innovation-minded regulatory agencies see sandboxes as means, not ends.», D. Quan, *A few thoughts on regulatory sandboxes*, Stanford University, Stanford PACS, 2019, https://pacscenter.stanford.edu/a-few-thoughts-on-regulatory-sandboxes/.

incompatibilità con alcuni principi chiave nell'ordinamento giuridico dell'Unione europea, quali quello di legalità e di parità di trattamento.

Alla luce di quanto precede, il lavoro si snoda in tre parti: un'analisi teorica e pratica delle *regulatory sandboxes* con focus sull'AI Act [11], una valutazione della loro compatibilità rispetto ai principi fondamentali dell'UE e un approfondimento sul ruolo della coregolazione come strumento per promuovere un quadro normativo più flessibile e resiliente.

2. *Evoluzione teorica e modelli applicativi degli spazi di sperimentazione normativa in diverse realtà nazionali*

Prima di esaminarne i fondamenti teorici e le prassi applicative, è necessario definire gli spazi di sperimentazione normativa, cd. *regulatory sandboxes*[12].

Sebbene la letteratura giuridica[13], i documenti di policy[14] e le normati-

---

[11] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

[12] Il termine deriva dall'informatica dove con *sandbox* si intende uno strumento atto a testare un determinato sistema, V. K. Yordanova, *The shifting sands of regulatory sandboxes for AI*, in *Centre for IT and IP law blog*, 2019. Si consideri inoltre che, nelle Conclusioni 2020, il Consiglio dell'Unione Europea evidenzia come le regulatory sandboxes—o spazi di sperimentazione normativa—siano strumenti essenziali per consentire alle imprese di testare soluzioni innovative in un ambiente regolato ma flessibile, dove tali soluzioni non sono immediatamente soggette ai requisiti normativi tradizionali. Allo stesso modo, nella proposta di Regolamento sull'Intelligenza Artificiale e nella versione definitiva pubblicata in Gazzetta Ufficiale, si fa riferimento agli spazi di sperimentazione normativa utilizzando l'espressione inglese "regulatory sandboxes", sottolineando l'importanza di questi ambienti per favorire un continuo adattamento normativo alle trasformazioni tecnologiche.

[13] V. *ex multis,* D. A. Zetzsche, R. P. Buckley, D. W. Arner e J. N. Barberis, *Regulating,* cit; H. Allen, *Regulatory Sandboxes*, in *George Washington Law Review*, 2019; H. Allen, *Sandbox Boundaries*, in *Vanderbilt Journal of Entertainment & Technology Law*, 2020.

[14] Commissione europea 2020, *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 final; Financial Conduct Authority 2015, *Regulatory sandbox*, https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf; Financial Stability Board 2020, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions*: *Market developments and financial stability implications*, https://www.fsb.org/uploads/P091020.pdf.

ve[15] offrano una varietà di definizioni, non esiste una versione che si possa ritenere generalmente accettata, poiché, come sostenuto in dottrina[16], questi concetti variano in base al contesto giuridico nazionale e all'interpretazione che ne viene fornita.

Ai fini del presente contributo, la definizione adottata è quella accolta dal Consiglio dell'Unione europea che intende gli spazi di sperimentazione normativa come «quadri concreti che, fornendo un contesto strutturato per la sperimentazione, consentono, se del caso in un ambiente reale, di testare tecnologie, prodotti, servizi o approcci innovativi – al momento soprattutto nel contesto della digitalizzazione – per un periodo di tempo limitato e in una parte limitata di un settore o di un ambito soggetto a vigilanza regolamentare, garantendo la messa in atto di opportune misure di salvaguardia»[17]. In altre parole, si tratta di ambienti, sia virtuali che fisici, concepiti per consentire la sperimentazione temporanea di progetti tecnologicamente innovativi, con la possibilità di applicare deroghe alle normative vigenti nel settore di riferimento. Tali ambienti offrono ai promotori l'opportunità di condurre test in modo approfondito ed efficace. Un ulteriore elemento distintivo consiste nella possibilità di impiegare i risultati delle sperimentazioni come base per future e potenziali modifiche legislative.

Questa definizione così ampia mette in luce le tre principali caratteristiche[18] di questi strumenti: (i) il carattere temporaneo delle misure; (ii) l'approccio regolatorio basato sul metodo del tentativo ed errore e (iii) il coinvolgimento di diversi portatori di interesse.

---

[15] Regolamento 2024/1689, cit.; Regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio del 29 aprile 2021 che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240.

[16] D. A. Zetzsche, R. P. Buckley, D. W. Arner, J. N. Barberis, *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, in *Fordham Journal of Corporate & Financial Law*, 2017; B.R. Knight, T.E. Mitchell, *The Sandbox Paradox: Balancing the Need to Facilitate Innovation with the Risk of Regulatory Privilege*, in *South Carolina Law Review*, 2020; J. Armour, M. Sako, *AI-enabled business models in legal services: from traditional law firms to next-generation law companies?*, in *Journal of Professions and Organization*, 2020, p. 27–46.; S. Ranchordás, *Innovation-Friendly Regulation: The Sunset of Regulatory Sandboxes?,* in *Law & Policy*, 2020; I. Bar-Siman-Tov, *Temporary legislation, better regulation, and experimentalist governance: An empirical study,* in *Regulation & Governance*, 2018.

[17] Conclusioni del Consiglio 2020, cit., p. 8.

[18] Cfr. S. Ranchordás, *Innovation friendly,* cit; I. Bar-Siman-Tov, *Temporary legislation*, cit.

Sebbene il concetto di *regulatory sandbox* sia relativamente recente, numerose *sandboxes* sono già operative sia a livello europeo sia a livello globale[19]. Poiché questo articolo si propone di analizzare questi strumenti da una prospettiva giuridica piuttosto che tecnica, è opportuno menzionare alcuni esempi rappresentativi scelti da diverse giurisdizioni, ognuno dei quali rappresenta un interessante esempio di implementazione.

Il primo e più diffuso è quello delle *sandboxes* finanziarie o *fintech*, settore in cui le *sandboxes* normative hanno avuto origine. La prima *sandbox* è stata lanciata nel 2015 nel Regno Unito per iniziativa della Financial Conduct Authority (FCA)[20], seguita negli anni successivi da numerosi progetti analoghi. Il funzionamento di questa sandbox consiste nel fornire un ambiente regolatorio controllato in cui le imprese possono testare prodotti o servizi finanziari innovativi senza essere soggette immediatamente a tutte le normative vigenti. Ogni progetto approvato è monitorato dalla FCA, che fornisce supporto e guida per garantire la conformità, riducendo al minimo i rischi per i consumatori.

In Italia[21], uno strumento simile è stato introdotto con il decreto-legge 30 aprile 2019 n. 34, conosciuto come "Decreto Crescita", seguito successivamente dal decreto del Ministero dell'Economia e delle Finanze del 30 aprile 2021 n. 100. La *sandbox* italiana prevede che le imprese che desiderano testare soluzioni innovative presentino una domanda alle autorità competenti, che valutano la proposta e, in caso di approvazione, consentono l'avvio del progetto in un ambiente controllato. Durante la fase di sperimentazione, le imprese sono soggette a requisiti regolatori ridotti, ma devono fornire rapporti periodici sullo stato del progetto e sui risultati ottenuti.

Di particolare interesse è anche il programma "Sperimentazione Italia", regolato dal decreto-legge 16 luglio 2020 n. 76, specificamente dall'art. 36, che si innesta nell'ambito della cosiddetta "trasformazione digitale della pubblica amministrazione", in un'ottica multisettoriale. Tale iniziativa è stata applicata in particolare nei progetti di "*smart cities*" e, nello specifico, nel campo della "*smart mobility*"[22].

---

[19] World Bank Group, *Global Experiences from Regulatory Experiences. Finance, Competitiveness & Innovation Global Practice*, Fintech Note, no. 8, 2020 https://documents1.worldbank.org/curated/en/912001605241080935/pdf/Global-Experiences-from-Regulatory-Sandboxes.pdf, p. 5.

[20] UK Financial Conduct Authority, *Regulatory sandbox lessons learned report*, 2017, https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf

[21] Per un approfondimento sui potenziali conflitti tra le sandboxes e il sistema costituzionale italiano, si rimanda a M. Milanesi, *Lo sviluppo delle sandbox regolatorie italiane tra dubbi e opportunità*, in *Federalismi*, 2023.

[22] G. Rugani, *La promozione di strumenti di co-regolazione dell'intelligenza*

Anche altri Stati membri dell'UE hanno adottato spazi di sperimentazione normativa. In Spagna, ad esempio, è stata istituita una *sandbox* per il settore fintech, simile a quella italiana[23]. Qualsiasi soggetto interessato a proporre un progetto innovativo per il settore può presentare domanda, purché rispetti requisiti essenziali, quali la dimostrazione di fornire un contributo innovativo al sistema finanziario, la sua "natura fintech" e la sostenibilità del progetto. Il legislatore spagnolo ha dato rilievo sia al progresso tecnologico che alla protezione dei consumatori e alla stabilità dei mercati, prevedendo una adeguata politica finanziaria a contorno dell'iniziativa oltre che tutele per i consumatori e i servizi finanziari[24].

Durante l'intera fase di test, l'Autorità di vigilanza monitora il rispetto delle regole previste dal protocollo e dalla normativa, con possibilità di interrompere la sperimentazione in caso di violazioni. Inoltre, l'Autorità redige una relazione finale che, trasmessa al Comitato di coordinamento, può portare a proposte di modifica legislativa incluse nel rapporto annuale della Segreteria Generale del Tesoro e della Finanza Internazionale e presentate in Parlamento dal Ministro degli Affari Economici[25].

---

artificiale nell'AI Act, con particolare riferimento alle regulatory sandboxes, in *Quaderni AISDUE*, 2024, e dottrina *ivi* citata.

[23] M. Gomez Santos, *Régimen jurídico del "regulatory sandbox" en España*, in *Revista de Derecho del Sistema Financiero: mercati, operadores e contratos*, 2021. Per un'analisi approfondita della legge spagnola si veda F. Zunzunegui, *Aproximación al espacio controlado de pruebas, (Commentary on Spanish Regulatory Sandbox Act)*, in *Revista General de Derecho de los Sectores Regulados*, 2020 e M. Trapani, *L'utilizzo delle sandboxes normative: una ricognizione comparata delle principali esperienze di tecniche di produzione normativa sperimentali e il loro impatto sull'ordinamento*, in Osservatorio sulle fonti, 2022.

[24] Le candidature possono essere presentate durante finestre semestrali e il processo coinvolge diversi organi, tra cui la Segreteria Generale del Tesoro e della Finanza Internazionale (SGTFI) e altre Autorità pubbliche: la Banca di Spagna, la Commissione Nazionale per il Mercato dei Valori, e la Direzione Nazionale per Assicurazioni e Fondi Pensione. Il coordinamento è affidato a un Comitato specifico, mentre la valutazione preliminare dei progetti è svolta dall'Autorità competente, che firma con il proponente un protocollo contenente modalità e termini della sperimentazione in caso di approvazione. Si veda, Legge n. 7 del 13 novembre 2020 para la transformación digital del sistema financiero, https://www.boe.es/buscar/pdf/2020/BOE-A-2020-14205-consolidado.pdf.

[25] Ministerio de Asuntos Economicos y Transformaciòn Digital, Sandbox Financiero, in Tesoropublico.es. Vedi anche Banco de España, Sandbox, in : https://www.bde.es/wbe/en/noticias-eventos/blog/sandbox-el-banco-de-pruebas-de-la-innovacion-financiera.html.

La Germania ha incentivato l'uso di clausole sperimentali in vari settori, tra cui il trasporto intelligente e l'istruzione[26], a livello dei singoli Länder. L'esperienza tedesca in materia di *regulatory sandboxes* si distingue nel contesto europeo per il suo approccio strutturato e coordinato a livello nazionale. Già dal 2018, il Ministero Federale dell'Economia ha pubblicato una guida[27] che illustra il concetto di *sandbox* normativa, i suoi scopi e le modalità di funzionamento, promuovendo l'adozione di deroghe sperimentali da parte delle autorità locali.

Una caratteristica peculiare del modello tedesco è l'impiego di clausole sperimentali che permettono ai governi regionali di autorizzare temporaneamente l'applicazione di norme meno rigide per favorire la sperimentazione di progetti innovativi. Queste clausole sono incorporate nelle disposizioni legislative locali o federali e prevedono la partecipazione di vari enti governativi, garantendo così un elevato grado di flessibilità. Di conseguenza, le tempistiche, i procedimenti e i criteri di approvazione possono variare notevolmente in base alla tipologia di progetto presentato. Tra le iniziative più rilevanti[28] si segnalano quelle nel campo della mobilità intelligente, come il progetto avviato ad Amburgo, reso possibile grazie a modifiche legislative specifiche[29].

In virtù di questo approccio, la Germania ha assunto un ruolo di primo piano nello sviluppo di strumenti regolatori innovativi, investendo risorse significative e coinvolgendo attivamente sia il settore pubblico che quello privato. Questo sistema ha garantito ampie opportunità di sperimentazione per i privati, pur mantenendo un controllo sulle potenziali criticità. Va però rilevato che rimane elevata la discrezionalità delle autorità pubbliche nel concedere le autorizzazio-

---

[26] H. D. Horn, *Experimentelle Gesetzgebung unter dem Grundgesetz*, Berlin; 1989; V. Maass, *Experimentierklauseln für die Verwaltung und ihre verfassungsrechtlichen Grenzen*, Berlin, 2021; T. Freund, *Kommunale Standardöffnungs- und Experimentierklauseln im Lichte der Verfassung*, Berlin, 2023.

[27] Si veda il report *Making space for innovation. The handbook for regulatory sandboxes*, 2019 pubblicato sul sito https://www.bmwk.de/Redaktion/EN/Publikationen/Digitale-Welt/handbook-regulatory sandboxes.pdf?__blob=publicationFile&v=2.

[28] Per consultare gli altri progetti attivi: https://www.bmwk.de/Redaktion/EN/Dossier/regulatory-sandboxes.html.

[29] V. progetto "HEAT" (Hamburg Eletric Autonomous Transportation) che consisteva nel testare bus a guida autonoma per le strade di Amburgo. La deroga normativa è contenuta nella Sezione 7(2) della Legge sui Trasporti di Passeggeri che prevede, per consentire la sperimentazione pratica di nuovi modi o mezzi di trasporto, l'Autorità competente al rilascio delle licenze può, caso per caso e su richiesta, autorizzare delle deroghe alle disposizioni della Legge sui trasporti per un periodo massimo di quattro anni. Si precisa inoltre che tali deroghe non devono porsi in contrasto con gli interessi del trasporto pubblico.

ni, nell'ottica di incentivare l'innovazione senza alterare in modo permanente il quadro normativo vigente.

In Portogallo, la sperimentazione ha luogo in un'area dedicata, chiamata "Zona Franca Tecnologica", una zona geografica e tematica destinata a progetti innovativi[30].

Un altro importante esempio di spazio di sperimentazione normativa è rappresentato dalla *sandbox* normativa sviluppata dall'Information Commissioner's Office (ICO) del Regno Unito nell'ambito della protezione dei dati[31] con riferimento a tecnologie particolarmente innovative, come la realtà aumentata, oppure tecnologie di riconoscimento biometrico.

Il funzionamento della *sandbox* promossa dall'ICO prevede una fase iniziale di selezione, in cui le organizzazioni presentano le loro proposte innovative. Se accettate, le organizzazioni ricevono supporto continuo e indicazioni specifiche dall'ICO durante la fase di test. Questo approccio permette di individuare e risolvere eventuali problematiche di conformità prima del lancio ufficiale sul mercato.

La richiesta di strumenti di sperimentazione normativa è in aumento anche nel campo sanitario. Come dimostrano studi sistematici condotti in questo ambito, queste iniziative sono concentrate soprattutto nei Paesi ad alto reddito[32], dove l'obiettivo individuato è di sostenere l'adozione di nuove tecnologie, in particolare quelle legate alla salute digitale[33]. In tale contesto, guardare a esperienze extraeuropee risulta particolarmente significativo, dato che in molti Paesi terzi queste sperimentazioni hanno già trovato applicazione concreta, dimostrando sia le potenzialità di tali strumenti sia l'urgenza per l'Unione europea di sfruttare al meglio queste opportunità, colmando eventuali divari rispetto ai Paesi leader nelle tecnologie emergenti.

Un esempio concreto di *sandbox* normativa nel settore sanitario è quello di Singapore, dove il Ministero della Salute ha lanciato nel 2018 il cosiddetto *Li-*

---

[30] M. Trapani, *L'utilizzo delle sandboxes normative,* cit.

[31] Information Commissioner's Office, Regulatory Sandbox Insights Report 2024, July 2024, https://ico.org.uk/media2/migrated/4030434/regulatory-sandbox-insights-report.pdf.

[32] E. Leckenby, D. Dawoud, J. Bouvy e P. Jónsson, *The Sandbox Approach and its Potential for Use in Health Technology Assessment: A Literature Review*, in *Applied Health Economics and Health Policy*, 2021.

[33] A tal riguardo, si tenga in considerazione che la Costituzione francese dà la possibilità di adottare leggi sperimentali, sia a livello nazionale che locale. Cfr. J-H. Stahl, *L'expérimentation en droit français: une curiosité en mal d'acclimatation*, in *Revue Juridique de l' Économie Publique*, 2010.

censing Experimentation and Adaptation Programme (LEAP)[34]. Questo programma ha creato una *sandbox* dedicata alla telemedicina e alla medicina mobile, con l'obiettivo di comprendere meglio il funzionamento della nuova tecnologia, identificare i rischi potenziali e stabilire misure per mitigarli, prima di procedere con la concessione delle licenze[35], in conformità con il Singaporean Healthcare Services Act[36]. Il funzionamento del programma LEAP si basa su una stretta collaborazione tra le autorità e le imprese partecipanti, che devono rispettare criteri di sicurezza rigorosi durante l'intera fase di sperimentazione.

L'esperienza di Singapore, e in particolare la conclusione positiva della *sandbox* normativa avviata nel 2018, dimostra che questi strumenti possono essere applicati con successo anche nel settore sanitario, sebbene alcuni autori abbiano sollevato delle criticità che concernono potenziali rischi per la sicurezza dei pazienti, poca trasparenza e frizioni con alcuni principi etici[37].

In generale, gli esempi citati evidenziano come la questione delle *sandboxes* normative non sia confinata a un solo settore, ma si estenda a molteplici ambiti sociali ed economici, ciascuno con le proprie sfide e opportunità.

2.1 *Il contributo del Regolamento sull'intelligenza artificiale*

Come già anticipato in apertura, un settore rilevante per l'applicazione delle *sandboxes* normative è quello dell'intelligenza artificiale.

Un esempio interessante a questo proposito è quello della Norvegia, dove l'Autorità locale per la protezione dei dati ha istituito una *sandbox* dedicata allo

---

[34] A. Attrey, M. Lesher e C. Lomax, *The role of sandboxes in promoting flexibility and innovation in the digital age*, in *OECD Going Digital Toolkit Notes*, Paris, 2020.

[35] Per raggiungere gli obiettivi prefissati, il Ministero della Salute di Singapore ha istituito una piattaforma di cooperazione con i fornitori coinvolti per creare un ambiente sicuro per la telemedicina e la medicina mobile, adottando un approccio basato sulla valutazione del rischio. L'obiettivo finale della sandbox normativa era giungere a una regolamentazione completa della telemedicina e della medicina mobile come servizi sanitari autorizzati. Tale obiettivo è stato dichiarato raggiunto a febbraio 2021, portando alla chiusura della *sandbox*. Nella fase di transizione verso la regolamentazione ufficiale, il Ministero della Salute di Singapore ha iniziato a pubblicare l'elenco dei fornitori di servizi di telemedicina diretta che hanno dimostrato consapevolezza dei rischi e dei benefici della telemedicina, adottato misure per affrontare questi rischi e accettato di rispettare le linee guida per una pratica sicura stabilite dal Ministero.

[36] Ministry of Health of Singapore, *Regulatory sandbox - The Licensing Experimentation and Adaptation Program-me (LEAP) by MOH supports innovative healthcare services through regulatory sandboxes,* 2024

[37] J. S. Sherkow, *Regulatory Sandboxes and the Public Health*, in *University of Illinois Law Review*, 2022.

sviluppo di soluzioni di intelligenza artificiale responsabile[38]. Questa iniziativa mira a promuovere l'adozione di tecnologie di intelligenza artificiale che rispettino standard etici e siano in linea con i requisiti di protezione dei dati.

Oltre al caso della Norvegia, merita attenzione il progetto pilota di sandbox normativa istituito in Spagna[39]. Lanciato nel giugno 2022 in collaborazione con la Commissione Europea, il pilot spagnolo mirava a testare sistemi di IA ad alto rischio e a uso generale in vista dell'entrata in vigore dell'AI Act. Questo progetto, aperto anche ad altri Stati membri, rappresenta il primo tentativo di una sandbox normativa paneuropea, con l'obiettivo di condividere i risultati con l'intera comunità europea[40].

Da quanto precede, si evince come, in tale contesto, l'AI Act emerga come un caso di studio centrale per questo lavoro, rappresentando un punto di riferimento unico per l'esame delle sfide e delle potenzialità delle *sandboxes* normative[41] nel quadro normativo di diritto dell'Unione europea.

Il considerando 138 sottolinea come l'intelligenza artificiale rappresenti una famiglia di tecnologie in rapida evoluzione, richiedendo sia una supervisione normativa che un ambiente sicuro e controllato per la sperimentazione, al fine di promuovere un'innovazione responsabile attraverso l'integrazione di adeguate tutele e misure di mitigazione dei rischi. In quest'ottica, l'articolo 57 del Regolamento stabilisce che gli Stati membri provvedano affinché le autorità competenti istituiscano *almeno uno*[42] *spazio di sperimentazione normativa* per l'intelligenza

---

[38] Datatilsynet, *Regulatory privacy sandbox*, https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/.

[39] Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial, https://www.boe.es/eli/es/rd/2023/11/08/817.

[40] Il pilot si propone di chiarire i requisiti di conformità dell'AI Act, trasferire il *know-how* alle aziende partecipanti e sviluppare linee guida e standard utili a livello europeo. Le attività pratiche includono workshop, consulenze personalizzate e sessioni formative per supportare le imprese nel testare e adeguare i loro sistemi di IA ai requisiti normativi. Il progetto prevede due gruppi di lavoro: uno operativo, focalizzato sul supporto alle aziende, e uno analitico, incaricato di elaborare la documentazione e le linee guida basate sui risultati del pilot. La durata complessiva del progetto è di tre anni, con scadenza nel 2025. Il successo del pilot dipenderà dalla collaborazione delle aziende partecipanti, che dovranno condurre una valutazione di conformità, garantire il monitoraggio post-sperimentazione e presentare report al comitato di coordinamento.

[41] S. Ranchordas, V. Vinci, *Regulatory sandboxes and innovation-friendly regulation: between collaboration and capture*, in *Italian Journal of Public Law*, 2024.

[42] Sul punto, vale la pena precisare che è stato il Parlamento europeo a porre maggiore enfasi sulla necessità di incentivare le regulatory sandboxes. V. G. Rugani, *La*

artificiale, a livello regionale o locale, oppure in collaborazione con le autorità di altri Stati membri, o anche da parte del Garante europeo della protezione dei dati (par. 3).

Un aspetto fondamentale del regime normativo introdotto dall'AI Act è disciplinato dall'articolo 58, il quale stabilisce i requisiti specifici che devono essere soddisfatti dai partecipanti alle *sandboxes*. In particolare, si prevede che le autorità competenti garantiscano un monitoraggio continuo delle attività svolte negli spazi di sperimentazione, verificando che queste rispettino i principi di sicurezza e trasparenza. Si introduce inoltre l'obbligo per i partecipanti di redigere rapporti periodici che descrivano i progressi compiuti e gli eventuali rischi identificati durante la sperimentazione. Questo obbligo è volto a garantire che i sistemi sviluppati nelle *sandboxes* rispettino i requisiti normativi fin dalle prime fasi di progettazione.

Tali spazi di sperimentazione normativa sono concepiti per fornire «un ambiente controllato che promuove l'innovazione e facilita lo sviluppo, l'addestramento, la sperimentazione e la convalida di sistemi innovativi per un periodo limitato prima della loro immissione sul mercato o della loro messa in servizio» (par. 5) e possono anche includere test condotti in «condizioni reali», pur restando soggetti a controlli nell'ambito della *sandbox*.

La norma prevede, inoltre, il coinvolgimento delle autorità nazionali per la protezione dei dati e di quelle responsabili dell'accesso ai dati nelle attività di queste *sandboxes*, con compiti di supervisione entro i limiti delle loro competenze (par. 10). Restano invariati i poteri di controllo e intervento delle autorità competenti (par. 11), mentre i partecipanti alla *sandbox* sono tenuti a rispondere per eventuali danni causati a terzi durante la sperimentazione, secondo le normative vigenti (par. 12).

Le autorità nazionali competenti devono presentare annualmente una relazione all'Ufficio per l'IA, istituito dalla Commissione ai sensi dell'art. 64, e al Comitato europeo per l'intelligenza artificiale di cui all'art. 65 (composto da rappresentanti di ciascuno Stato membro), e che contiene «informazioni sui progressi e sui risultati dell'attuazione di tali spazi di sperimentazione, comprese le migliori pratiche, gli incidenti, gli insegnamenti tratti e le raccomandazioni sulla loro configurazione e, ove pertinente, *sull'applicazione ed eventuale revisione del presente regolamento*, inclusi i rispettivi atti delegati e di esecuzione, e sull'applicazione di altre disposizioni di diritto dell'Unione soggette a controllo da parte delle autorità competenti nell'ambito dello spazio di sperimentazione». A tal riguardo, si deduce, da una interpretazione letterale della disposizione, che la relazione dell'Autorità di controllo sull'andamento degli spazi di sperimentazione

---

promozione di strumenti di co-regolazione, cit., pp. 8-9.

normativa possa svolgere un ruolo propulsivo nella revisione dell'AI Act. A ciò si aggiunge che l'articolo 58, paragrafo 6, consente di raccogliere dati e risultati sperimentali che potranno essere utilizzati dalla Commissione per valutare la necessità di modificare il quadro normativo vigente, promuovendo un costante aggiornamento legislativo in linea con l'evoluzione tecnologica.

Questo implica che tali spazi di sperimentazione normativa non solo, di fatto, operano come ambienti controllati per l'innovazione, ma potrebbero anche contribuire all'evoluzione del quadro normativo dell'Unione, offrendo raccomandazioni e suggerendo adattamenti futuri.

Infine, merita menzione l'articolo 60, che consente la sperimentazione di sistemi di IA ad alto rischio[43] «in condizioni reali al di fuori degli spazi di sperimentazione normativa», ovvero senza i consueti controlli, purché vengano rispettate condizioni e garanzie specifiche. In tali casi, è richiesto il rispetto di un «piano di prova in condizioni reali», definito come «un documento che descrive gli obiettivi, la metodologia, l'ambito geografico, della popolazione e temporale, il monitoraggio, l'organizzazione e lo svolgimento della prova in condizioni reali». Sarà compito della Commissione, tramite atti di esecuzione, specificare gli elementi da includere nel piano di prova.

L'articolo 61 stabilisce che, per le sperimentazioni condotte al di fuori delle *sandboxes* normative, i partecipanti devono fornire il loro consenso informato, come indicato nel titolo dell'articolo stesso, «Consenso informato a partecipare a prove in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA». Tale disposizione è considerata dal legislatore dell'Unione una garanzia essenziale, poiché le sperimentazioni si svolgono al di fuori del quadro regolamentato delle *sandboxes*[44]. Si rileva, inoltre, che la possibilità di condurre prove in condizioni reali fuori dagli spazi di sperimentazione non era prevista nella proposta iniziale della Commissione, ma è stata introdotta dal Consiglio per incentivare un apprendimento basato su evidenze[45].

Le osservazioni sinora formulate conducono inevitabilmente a un'ulteriore indagine giuridica più approfondita sullo status normativo degli spazi di speri-

---

[43] J. Truby e altri, *A sandbox approach to regulating high-risk artificial intelligence applications,* in *European Journal of Risk Regulation*, 2023.

[44] T. Buocz, S. Pfotenhauer e I. Eisenberger, *Regulatory sandboxes in the AI Act: reconciling innovation and safety?*, in *Law, Innovation and Technology*, 2023.

[45] «With a view to creating a legal framework that is more innovation-friendly and to promoting evidence-based regulatory learning, the provisions concerning measures in support of innovation have been substantially modified compared to the Commission proposal», https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/.

mentazione normativa. In particolare, *fino a che punto questi strumenti rappresentano un equilibrio efficace tra promozione dell'innovazione e rispetto delle normative? E quali sono le conseguenze giuridiche del loro utilizzo in contesti regolatori diversificati?*

Tali interrogativi, cui si cercherà di rispondere nei paragrafi successivi, non solo aprono nuove prospettive per il diritto, ma suggeriscono anche di considerare le *sandboxes* come strumenti in grado di promuovere l'innovazione. Allo stesso tempo, queste strutture emergono come potenziali catalizzatori di un cambiamento significativo nel modo di concepire la regolamentazione in un contesto caratterizzato da rapide e costanti trasformazioni.

Le esperienze nazionali, come quella norvegese e spagnola, sembrano suggerire che il successo delle *sandboxes* dipenderà in larga misura dalla collaborazione tra autorità di regolazione e soggetti privati, nonché dall'adozione di un approccio flessibile ma rigoroso.

Sebbene, come già sostenuto in apertura, l'AI Act sia stato esaminato in questo lavoro come un caso di studio paradigmatico, è opportuno precisare che le osservazioni qui condivise non pretendono di fornire una trattazione esaustiva delle disposizioni contenute nel regolamento. L'AI Act, infatti, costituisce solo uno dei contesti applicativi possibili, scelto per la sua centralità e attualità, ma non esaurisce la varietà di scenari in cui tali strumenti regolatori potrebbero essere sperimentati, come dimostrato dall'analisi dei diversi casi pratici affrontati nel contributo.

3. *Imparare sperimentando: il percorso verso l'innovazione?*

Definire e misurare l'innovazione è complesso[46], rendendo di conseguenza difficile la sua regolamentazione. Il Manuale di Oslo dell'OCSE[47] definisce l'in-

[46] K. Garnett, G. Van Calster e L. Reins, *Towards an innovation principle: An industry trump or shortening the odds on environmental protection?,* in *Law, Innovation and Technology*, 2018.

[47] Il principio dell'innovazione, introdotto nel 2013 dal Forum Europeo del Rischio (ERF), rappresenta un tentativo ambizioso di influenzare l'agenda normativa europea. Nato sotto l'egida di un gruppo di lobby industriali che includeva settori chiave come quelli dei combustibili fossili, dell'industria chimica e, inizialmente, del tabacco, l'ERF ha rapidamente acquisito rilievo grazie al sostegno di grandi aziende e organizzazioni come la BusinessEurope. La sua affermazione è stata strategicamente sostenuta attraverso un'intensa attività di lobbying, culminata nella sua prima comparsa in un documento ufficiale dell'UE nel 2015. L'ERF ha saputo costruire una rete di alleanze che gli ha permesso di accedere a tavoli decisionali di alto livello. Particolarmente rilevante è stato il ruolo della presidenza olandese nel 2016, che ha organizzato una conferenza

novazione come «un prodotto o processo nuovo o migliorato che si differenzia significativamente dai precedenti e reso disponibile agli utenti o introdotto nell'uso interno» [48]. Questa definizione evidenzia tre requisiti centrali: la presenza di elementi di novità o miglioramento, la necessaria applicazione dell'innovazione a prodotti o processi, e accessibilità agli utenti.

Regolamentare l'innovazione è complicato poiché le nuove tecnologie possono destabilizzare i quadri normativi esistenti, evidenziando la lentezza delle risposte legislative e creando asimmetrie informative tra innovatori e regolatori. La mancanza di dialogo tra autorità e imprese aggrava questa disconnessione. Pertanto, proprio mediante le *sandboxes* normative si cerca di colmare tali lacune promuovendo una maggiore collaborazione tra legislatori e innovatori[49].

---

internazionale dedicata al tema e promosso l'inserimento del principio dell'innovazione nelle conclusioni del Consiglio Competitività. L'adozione ufficiale da parte del Consiglio ha portato la Commissione Europea a creare una Innovation Principle Taskforce, con l'obiettivo di monitorare e integrare questo principio nelle future iniziative legislative e politiche. Parallelamente, la Commissione ha avviato un dibattito accademico attraverso il programma Horizon 2020, sollevando una questione cruciale: come bilanciare il principio dell'innovazione con il principio di precauzione, spesso percepiti come in contrasto. Tuttavia, il principio dell'innovazione non è stato privo di controversie. Nel 2018, quando è stato inserito nel preambolo del regolamento di Horizon Europe, ha suscitato un ampio dibattito politico. Più di un terzo degli eurodeputati ha sostenuto un emendamento per rimuoverne il riferimento, evidenziando le tensioni tra il sostegno all'innovazione e la tutela dei principi precauzionali tradizionali. Si v. A. Saltelli e altri, *Science, the endless frontier of regulatory capture,* in *Futures*, 2022.

[48] Traduzione dell'A; Cfr. OECD/Eurostat 2018, Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation, 4th Edition, The Measurement of Scientific, Technological and Innovation Activities, OECD Publishing, Paris/Eurostat, Luxembourg, https://doi.org/10.1787/9789264304604-en.

[49] Questo fenomeno è ben illustrato dal cosiddetto dilemma di Collingridge, secondo cui all'emergere di un'innovazione i regolatori esitano a intervenire a causa della scarsa disponibilità di informazioni. Tuttavia, quando finalmente ottengono informazioni sufficienti, potrebbe essere troppo tardi, poiché la tecnologia potrebbe essere cambiata o la regolamentazione potrebbe non essere più in grado di contenere i rischi e gli effetti collaterali. In sintesi, i regolatori possono generalmente influenzare lo sviluppo di una tecnologia solo nelle sue prime fasi. Tuttavia, in questa fase iniziale, non dispongono ancora delle informazioni necessarie per comprendere pienamente l'impatto sociale della nuova tecnologia. Successivamente, quando la tecnologia è ormai radicata nella società e i regolatori hanno raccolto maggiori informazioni sui suoi effetti, potrebbe non essere più possibile influenzarne lo sviluppo. Si veda: D. Collingridge, *Social Control of Technology*, New York, 1982; A. Genus, A. Stirling, *Collingridge and the dilemma of control: Towards responsible and accountable innovation*, in *Research Policy*, 2018.

Questa direzione è sostenuta da iniziative come la Nuova agenda europea per l'innovazione[50] e il Piano industriale del Green Deal[51], che evidenziano la necessità di integrare sostenibilità, diritti umani e stato di diritto nei processi di regolamentazione. Il Consiglio dell'UE, nelle sue Conclusioni, ha identificato il principio di innovazione[52] come strategico per strumenti normativi flessibili e sostenibili, favorendo l'uso di spazi di sperimentazione normativa per gestire il progresso tecnologico in modo proattivo.

Le *sandboxes* normative, grazie alla loro natura temporanea e adattabile, consentono di affrontare sfide emergenti, riducendo il rischio di obsolescenza normativa e sostenendo la competitività delle imprese. Esse facilitano un rapido adattamento alle priorità sociali ed etiche, richiedendo ai legislatori di bilanciare valori contrastanti e coinvolgere attori non statali nel processo decisionale.

Questo approccio permette agli innovatori di testare le loro soluzioni con maggiore sicurezza e ai regolatori di comprendere meglio le nuove tecnologie, riducendo le asimmetrie informative. L'OCSE, riferendosi all'intelligenza artificiale, ha riconosciuto l'efficacia delle sandboxes normative per gestire tecnologie emergenti, soprattutto se integrate con altri strumenti regolatori[53].

3.1 *Quali sfide nell'implementazione delle* regulatory sandboxes*?*

All'idea che gli spazi di sperimentazione normativa possano favorire un'innovazione responsabile si contrappongono tuttavia alcune questioni rilevanti che meritano un approfondimento.

---

[50] Commissione europea 2022, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Una nuova agenda europea per l'innovazione, COM/2022/332 final.

[51] Commissione europea 2023, Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Un piano industriale del Green Deal per l'era a zero emissioni nette, COM/2023/62 final.

[52] F. Simonelli, A. Renda, *Study supporting the interim evaluation of the innovation principle – Final report*, Publications Office, 2019, https://data.europa.eu/doi/10.2777/620609.

[53] OECD, *Regulatory sandboxes in artificial intelligence*, in *OECD Digital Economy Papers*, Paris, 2023 https://doi.org/10.1787/8f80a0e6-en.

In primo luogo, come già evidenziato, nell'ordinamento giuridico europeo non vi è una definizione di *sandbox* normativa univoca né un quadro istituzionale che ne disciplini la creazione. Questa lacuna potrebbe creare incertezze tra i regolatori e portare a una frammentazione del mercato unico europeo, oltre a generare equivoci sulle funzioni specifiche delle *sandboxes* normative, confondendole con altri strumenti sperimentali. Tuttavia, occorre allo stesso tempo ribadire che, è proprio grazie alla loro flessibilità, che le *sandboxes* possono offrire un valore aggiunto, permettendo ai regolatori di osservare in tempo reale l'impatto delle tecnologie testate e ai soggetti regolati di operare in un contesto normativo temporaneamente adattato alle loro esigenze.

In risposta a questa esigenza, l'OCSE ha tentato di proporre per la prima volta una classificazione delle *sandboxes* normative e di altri strumenti sperimentali[54], basandosi su criteri condivisibili a livello internazionale. La classificazione proposta considera due dimensioni principali: la sfera di applicazione (privata, pubblica o ibrida) e l'ambito di intervento (specifico per norme, orientato alla tecnologia, generico/intersettoriale o legato a regtech/govtech).

A supporto di questa iniziativa, la Commissione Europea, nel luglio 2023, ha pubblicato un documento di lavoro[55] che fornisce indicazioni per distinguere le *sandboxes* normative da altri strumenti come progetti pilota, laboratori di prova e ambienti di test, evidenziando la necessità di differenziazioni chiare tra i vari approcci.

Un ulteriore aspetto critico da considerare riguarda la compatibilità delle *sandboxes* normative con il principio di uguaglianza[56]. Questi strumenti, spesso progettati per settori specifici o per affrontare sfide regolatorie mirate, sono strutturati in funzione delle esigenze dei partecipanti. Tuttavia, la loro implementazione potrebbe sollevare perplessità in relazione al principio di parità di trattamento, in quanto l'accesso privilegiato alle *sandboxes* può determinare uno squilibrio competitivo. I soggetti ammessi, infatti, beneficiano di deroghe normative che non sono estese agli altri operatori di mercato.

Questa differenziazione di trattamento potrebbe entrare in contrasto con quanto stabilito all'articolo 20 della Carta dei diritti fondamentali dell'Unione europea, in virtù del quale situazioni comparabili non devono essere trattate in

---

[54] *Ibidem*.

[55] Commission Staff Working Document, *Regulatory learning in the EU, Guidance on regulatory sandboxes, testbeds, and living labs in the EU, with a focus section on energy*, 25 July 2024, SWD(2023) 277/2 final.

[56] Conclusioni dell'Avvocato generale Maduro, causa C-127/07, *Société* Arcelor Atlantique, paragrafo 46.

modo diverso e situazioni diverse non devono essere trattate allo stesso modo, salvo che tale trattamento sia oggettivamente giustificato[57].

Tale principio risulta particolarmente rilevante nel contesto degli spazi di sperimentazione normativa, come evidenziato dalla giurisprudenza della Corte di Giustizia nel caso *Société Arcelor Atlantique*, definito dall'Avvocato Generale Maduro come una questione relativa ai «rapporti, per loro natura dialettici, tra la pratica della sperimentazione legislativa e le esigenze normative della parità di trattamento.»[58]

Nel caso di specie, la Corte non si è espressa direttamente sul tema della parità di trattamento in relazione alla legislazione sperimentale, tuttavia, pur riconoscendo le differenze concettuali tra il regime normativo[59] analizzato nel caso *Société Arcelor Atlantique* e il quadro giuridico delineato per gli spazi di sperimentazione normativa, i criteri definiti dall'Avvocato Generale Maduro offrono degli spunti di riflessione interessanti per valutare la loro coerenza con il principio di parità di trattamento.

Innanzitutto, nelle sue Conclusioni, l'Avvocato generale ha chiarito che la discriminazione derivante da norme sperimentali può essere compatibile con il principio di parità di trattamento solo se sono rispettate alcune condizioni fondamentali, segnatamente: (i) le misure sperimentali devono avere carattere transitorio e (ii) il loro ambito deve essere definito da criteri oggettivi, strettamente connessi alla materia e agli obiettivi della normativa in questione.

Applicando questi criteri agli spazi di sperimentazione normativa delineati, ad esempio, nell'AI Act, si osserva che, in primo luogo, benché il quadro normativo delle *regulatory sandboxes* sia concepito come permanente, i singoli esperimenti condotti al suo interno sono limitati nel tempo, con una durata proporzionata alla complessità e alla portata del progetto.

In secondo luogo, il regime delle *sandboxes* mira a creare un sistema giuridico che favorisca l'innovazione e risulti resiliente ai cambiamenti, mentre gli scopi delle singole sperimentazioni variano in base alla tipologia di sistema di intelligenza artificiale testato e al suo contesto applicativo.

---

[57] Corte di giustizia, Polonia/Consiglio, causa C273/04; Corte di giustizia, *Nagy*, C-21/10, para 47; Corte di giustizia, TP, C-356/12 para 81; D. Martin, *Article 20 CFR*, in M. Kellerbauer, M. Klamert e J. Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, Oxford, 2019.

[58] Conclusioni dell'Avvocato generale Maduro, cit., paragrafo 2.

[59] Il caso riguardava una direttiva che istituiva un sistema di scambio di quote di emissione, applicabile al settore siderurgico ma non a quelli dell'alluminio e della plastica.

Inoltre, il regolamento sull'IA prevede che la Commissione Europea stabilisca, tramite atti di esecuzione, criteri oggettivi per la selezione dei partecipanti agli spazi di sperimentazione normativa.

Si può dunque inferire che, qualora tali criteri si basino su parametri come il grado di innovatività e la maturità tecnologica, piuttosto che sul settore di appartenenza, i requisiti delineati dall'Avvocato Generale nel caso *Arcelor* risulterebbero soddisfatti.

Occorre infine evidenziare, come sottolineato dall'Avvocato Generale Maduro, che la Corte di Giustizia riconosce al legislatore un'ampia discrezionalità, in particolare quando le decisioni legislative implicano scelte di carattere politico, economico o sociale, oppure richiedono valutazioni di elevata complessità[60]. In questi casi, il sindacato giurisdizionale della Corte si limita alla «ricerca di un errore manifesto di valutazione nelle scelte operative»[61].

Ancora, la possibilità di istituire *sandboxes* in ciascuno Stato membro ha sollevato dubbi sul potenziale rischio di frammentazione all'interno dell'ordinamento giuridico europeo. A tal riguardo, quantomeno per la disciplina sull'intelligenza artificiale, l'AI Act cerca di rispondere a queste preoccupazioni, infatti, come già detto, l'articolo 58 dispone che la Commissione adotti atti di esecuzione «che precisano le modalità dettagliate per l'istituzione, lo sviluppo, l'attuazione, il funzionamento e la supervisione degli spazi di sperimentazione normativa per l'IA.» Inoltre, l'articolo prevede altresì che suddetti atti di esecuzione comprendano principi comuni riguardanti criteri di ammissibilità e selezione per la partecipazione alla *sandbox*, le procedure per la domanda, partecipazione, monitoraggio e uscita dalla *sandbox*, nonché per la sua cessazione, oltre ai termini e alle condizioni applicabili ai partecipanti.

Ciononostante, permangono molte incertezze sull'uso di questi strumenti, anche nel contesto dell'AI Act. Ad esempio, la portata e la natura delle *sandboxes* normative non sono chiaramente definite nel Regolamento. L'articolo 57 elenca come obiettivi delle *sandboxes* normative per l'IA: migliorare la certezza del diritto al fine di conseguire la conformità normativa, condividere le migliori pratiche, promuovere l'innovazione e la competitività, contribuire all'apprendimento normativo basato su dati concreti e agevolare e accelerare l'accesso al mercato dell'UE per i sistemi di IA.

Tuttavia, potrebbe essere necessaria una maggiore chiarezza riguardo al *design* e alla classificazione delle *sandboxes*, poiché alcune potrebbero avere una natura sperimentale mentre altre potrebbero servire principalmente come strumenti di conformità collaborativa. Invero, affinché la fase di sperimentazione possa por-

---

[60] Conclusioni dell'Avvocato generale Maduro, cit, paragrafo 35.

[61] *Ivi*, paragrafo 35.

tare a risultati validi, è necessario che gli obiettivi e le ipotesi da testare siano chiaramente definiti sin dall'inizio dell'esperimento, o addirittura precedentemente. Un esempio concreto di questo meccanismo di mutuo vantaggio può essere individuato nelle *sandboxes* adottate per il settore *fintech*. In tali contesti, le autorità di vigilanza finanziaria collaborano con start-up e istituti bancari per testare nuovi servizi digitali. Da un lato, i regolatori possono ottenere preziose informazioni sulle potenziali implicazioni normative di nuove tecnologie o di servizi di pagamento innovativi, migliorando così la certezza del diritto e adattando le norme in modo più informato. Dall'altro lato, i soggetti regolati beneficiano di un ambiente normativo più flessibile e meno oneroso durante la fase di sperimentazione, favorendo l'innovazione e l'accesso al mercato.

È essenziale che tutte le parti coinvolte comprendano quali sono gli scopi della *sandbox* normativa, per quale motivo sono state stabilite specifiche condizioni di ingresso e uscita, e se la struttura sperimentale potrebbe essere generalizzata per l'intera società. In virtù della loro natura, le *sandboxes* normative, specie quando introducono deroghe sperimentali, richiedono una chiara identificazione sia delle variabili indipendenti sia di quelle dipendenti.

Come stabilito dall'articolo 60 dell'AI Act, che disciplina il funzionamento di tali strumenti, una *sandbox* normativa può prevedere la sperimentazione di prodotti o servizi in un contesto reale. Tuttavia, in tali circostanze, il controllo sulle variabili estranee risulta intrinsecamente limitato. Di conseguenza, è indispensabile adottare misure che evitino un'interpretazione erronea dei risultati, salvaguardando così l'integrità e l'affidabilità delle sperimentazioni condotte.

A tal fine, nella formulazione e personalizzazione[62] delle ipotesi sperimentali, è opportuno utilizzare una terminologia chiara e accessibile, garantendo che tutti i soggetti interessati abbiano piena consapevolezza degli obiettivi, delle modalità e delle finalità del test. La strutturazione delle ipotesi, inoltre, dovrebbe includere l'individuazione di diverse opzioni per l'implementazione dell'intervento, accompagnata da una raccomandazione motivata sulla soluzione preferibile[63].

In buona sostanza, volendo trarre le fila di quanto sinora detto, l'approccio sperimentale delle *regulatory sandboxes*, sia per l'ambito dell'intelligenza artificiale che per altre soluzioni[64], essendo concepito per testare misure regolatorie

---

[62] Cfr. W. G. Johnson, *Caught in quicksand? Compliance and legitimacy challenges in using regulatory sandboxes to manage emerging technologies*, in *Regulation & Governance*, 2023.

[63] Ad esempio, nell'ambito di una sandbox normativa, i regolatori potrebbero valutare l'ipotesi che una riduzione degli oneri normativi, come la semplificazione delle licenze di ingresso al mercato, possa incentivare l'innovazione, in particolare da parte delle piccole e medie imprese.

[64] Ad esempio, nel settore bancario, finanziario e assicurativo, oltre che nell'ambito

in un ambiente controllato, consente di raccogliere dati empirici preziosi per orientare le future decisioni normative in modo più informato e basato sull'evidenza. Tale configurazione richiede, per sua natura, una stretta collaborazione tra il legislatore e gli innovatori, configurandosi dunque come uno strumento di coregolazione[65], meccanismo mediante il quale «un atto legislativo dell'Unione conferisce la realizzazione degli obiettivi definiti dal legislatore ai soggetti interessati riconosciuti in un determinato settore»[66]. Tuttavia, questa interazione solleva al contempo potenziali criticità, tra cui il rischio di un condizionamento (cd. *regulatory capture*) del potere legislativo da parte delle imprese partecipanti.

Per la rilevanza che questa criticità presenta nel complessivo assetto giuridico dell'Unione, si ritiene necessaria una trattazione a parte.

4. *La collaborazione tra pubblico e privato negli spazi di sperimentazione normativa*

Nell'ordinamento europeo, la coregolazione rappresenta un modello innovativo di governance, in cui attori privati partecipano alla definizione e attuazione di norme sotto la supervisione pubblica. Non è una semplice delega normativa, ma una partnership in cui gli enti pubblici fissano parametri entro cui i privati operano, garantendo il rispetto degli obiettivi generali.

Questo approccio risponde alla crescente complessità delle società moderne e alla necessità di affrontare temi tecnici specialistici, favorendo flessibilità e rapidità. La coregolazione integra il ruolo pubblico e privato, con l'UE che stabi-

---

di nuove tecnologie come la *blockchain.* Per il primo settore, v. Banca d'Italia, *Sandbox regolamentare*, https://www.bancaditalia.it/focus/sandbox/: "Attraverso lo strumento della sandbox, si persegue l'obiettivo di sostenere la crescita e l'evoluzione del mercato italiano grazie all'introduzione di modelli innovativi nel settore bancario, finanziario e assicurativo garantendo, al contempo, adeguati livelli di tutela dei consumatori e di concorrenza, preservando la stabilità finanziaria. Allo stesso tempo, le autorità responsabili per la regolamentazione potranno osservare le dinamiche dello sviluppo tecnologico e individuare gli interventi normativi più opportuni ed efficaci per agevolare lo sviluppo del FinTech, contenendo già in avvio la diffusione di potenziali nuovi rischi. Tramite la partecipazione alla sandbox, gli operatori possono testare prodotti e servizi innovativi in costante dialogo e confronto con le autorità di vigilanza, anche richiedendo eventuali deroghe normative nella fase di sperimentazione." Per le iniziative in materia di *blockchain* e *distributed ledger technologie,* v. https://digital-strategy.ec.europa.eu/en/news/launch-european-blockchain-regulatory-sandbox.

[65] Nell'Accordo Interistituzionale «Legiferare meglio» del 13 aprile 2016 tra Parlamento, Consiglio e Commissione, la coregolazione è denominata «meccanismo di regolamentazione alternativo».

[66] M.E. Bartoloni, *La regolazione privata,* , cit.

lisce quadri normativi generali e delega agli attori privati la definizione operativa attraverso codici di condotta e standard tecnici. Gli spazi di sperimentazione normativa incarnano questa filosofia, consentendo alle imprese di operare in ambienti regolati e monitorati, contribuendo allo sviluppo normativo tramite la pratica diretta.

Tuttavia, delegare funzioni regolatorie ai privati solleva questioni di legittimità, come il rischio di conflitti di interesse o norme meno chiare rispetto al processo legislativo ordinario. Per garantire efficacia, la coregolazione richiede una solida supervisione pubblica che assicuri la prevalenza dell'interesse generale, trasparenza e meccanismi di monitoraggio accessibili. L'assenza di trasparenza nelle *sandboxes* potrebbe alimentare timori di favoritismi, compromettendo fiducia e competitività.

Il controllo democratico è cruciale[67]: in un sistema rappresentativo come quello dell'UE, le decisioni devono essere adottate da soggetti legittimati. Tuttavia, un dialogo aperto e inclusivo con gli stakeholder, in linea con gli articoli 10 e 11 TUE, rafforza la trasparenza e la partecipazione democratica e, in buona sostanza, le *regulatory sandboxes* offrono l'opportunità di consolidare questo dialogo, come dimostrano le misure dell'AI Act, che includono coordinamento tra Stati membri e trasparenza tramite rapporti di valutazione e giustificazioni delle misure adottate.

Sarebbe utile una normativa quadro che definisca principi e garanzie minime per sperimentazioni in diversi contesti, prevenendo distorsioni della concorrenza e rafforzando fiducia e trasparenza nel processo regolatorio. Questo favorirebbe un'applicazione più ampia e consapevole degli strumenti sperimentali, assicurando al contempo la tutela dell'interesse pubblico.

5. *Osservazioni conclusive*

Questo contributo ha analizzato l'evoluzione dell'approccio regolatorio dell'Unione di fronte alle problematiche derivanti dall'emergere di nuove tecnologie, mettendo in evidenza le questioni poste dalla transizione da un modello tradizionale, basato sulla neutralità tecnologica, a uno strumento normativo più dinamico e flessibile.

[67] Il principio democratico-rappresentativo nell'ordinamento giuridico europeo si sviluppa su due livelli distinti: da un lato, quello garantito dal Parlamento europeo, il quale rappresenta direttamente i cittadini dell'Unione; dall'altro, quello incarnato dal Consiglio europeo e dal Consiglio, dove gli Stati membri sono rappresentati «dai rispettivi governi, a loro volta democraticamente responsabili dinanzi ai loro parlamenti nazionali o dinanzi ai loro cittadini» (art. 10, par. 2, TUE).

Attraverso l'analisi delle prassi applicative e del recente Regolamento sull'intelligenza artificiale come caso di studio, si è messo in luce il ruolo centrale degli spazi di sperimentazione normativa nel favorire un approccio legislativo più adattabile e basato su evidenze tecniche specifiche. Questi strumenti non solo rappresentano un mezzo per verificare l'efficacia delle disposizioni normative in contesti reali, ma promuovono anche un dialogo costruttivo tra regolatori e innovatori, in linea con i principi democratici e partecipativi sanciti dai Trattati.

Tuttavia, l'introduzione degli spazi di sperimentazione normativa non è priva di potenziali criticità. L'analisi ha evidenziato come tali strumenti pongano interrogativi rilevanti in merito alla trasparenza e all'equità di trattamento, sottolineando la necessità di definire criteri chiari e condivisi per la loro implementazione.

Questi ambienti regolatori permettono di sperimentare soluzioni innovative e, in taluni casi, consentono anche di introdurre deroghe mirate alla normativa vigente per testarne la validità e individuare eventuali modifiche necessarie. L'esempio delle *sandboxes* per l'intelligenza artificiale, introdotte dall'AI Act, sottolinea sia le potenzialità di questi strumenti nel promuovere un'armonizzazione normativa tra gli Stati membri, sia le questioni legate al rischio di frammentazione normativa e di una possibile "cattura regolatoria" da parte degli operatori privati.

Ciononostante, nel complesso, gli spazi di sperimentazione normativa si configurano come un'opportunità per ripensare il rapporto tra regolazione e innovazione, aprendo la strada a un modello di governance più reattivo e basato su evidenze empiriche. Tuttavia, la loro reale efficacia dipenderà dalla capacità del legislatore non solo di adottare un approccio equilibrato, ma anche di strutturare un sistema di supervisione che garantisca inclusività, trasparenza e accountability.

In particolare, nel caso del Regolamento sull'intelligenza artificiale, molto dipenderà dagli atti di esecuzione della Commissione europea. Mentre, negli altri settori, sarebbe auspicabile l'introduzione di un quadro normativo uniforme, capace di affrontare le problematiche evidenziate e promuovere soluzioni coerenti con i valori dell'Unione.

In definitiva, si ritiene che, se implementate secondo criteri oggettivi e adeguati, le *sandboxes* normative potrebbero, non solo contribuire alla definizione di un quadro normativo più resiliente e adeguato alle sfide del futuro, ma anche rafforzare alcuni valori fondamentali dell'Unione europea: trasparenza, inclusione e sostenibilità. Infatti, attraverso un approccio fondato su evidenze empiriche, questi strumenti permettono di adattare le normative alle esigenze pratiche, evitando così l'errore di costruire regole astratte, disconnesse dalla realtà e, perciò, difficilmente applicabili.

Impresa sociale e intelligenza artificiale: brevi suggestioni in una prospettiva *multi-stakeholder*

di **Lorenzo Mariconda**

1. *Diritto dell'impresa e intelligenza artificiale*

L'intelligenza artificiale (in breve, I.A.), analogamente a quanto potrebbe dirsi con riguardo alla sostenibilità[1], è uno tra i temi più in voga nell'ambito della letteratura gius-commercialistica recente[2], che se ne occupa prevalentemente esaminandone le prospettive applicative nel contesto della *corporate governance* societaria[3]. Una simile tendenza non potrà che accentuarsi all'esito dell'ormai

---

[1] Non mancando, peraltro, in proposito, Autori come N. Abriani e G. Schneider, *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corptech*, Bologna, 2021, pp. 240 ss., o M.L. Montagnani, *Intelligenza artificiale e* governance *della "nuova" grande impresa azionaria: potenzialità e questioni endoconsiliari*, in *Riv. soc.*, 2020, p. 1006, che evidenziano come proprio i sistemi di intelligenza artificiale possano assumere un ruolo fondamentale nel perseguimento di obiettivi di *sustainability* e, più in generale, nell'integrazione dei fattori *ESG*; nel dibattito americano cfr. anche il breve contributo di N. Joshi, *How IoT And AI Can Enable Environmental Sustainability*, del 4 settembre 2019, reperibile su *www.forbes.com*.

[2] In una delle trattazioni più complete in materia all'interno del panorama nazionale, ossia quella di N. Abriani e G. Schneider, *o.c.*, pp. 12 ss., nel tracciare la differenza con gli strumenti di *information technology* (IT), si sottolinea come l'avvento della società algoritmica abbia sancito «il passaggio dalla tecnologia come mezzo di connessione alla tecnologia come vero e proprio strumento decisionale».

[3] Ci si riferisce, in sostanza, a tutti gli studi relativi al complesso di soluzioni tecnologiche che, in un celebre saggio di L. Enriques e D.A. Zetzsche, *Corporate*

definitiva approvazione, a seguito di un lungo e travagliato *iter* legislativo[4], del Regolamento UE 2024/1689 del 13 giugno 2024 (cd. *AI Act*)[5], e della parallela predisposizione di un disegno di legge a livello nazionale, recante disposizioni e deleghe al Governo in materia di I.A.[6]. La normativa euro-unitaria, in particolare, ha finalmente introdotto una definizione di «sistema di intelligenza artificiale», qualificandolo come «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»[7]. D'altro canto, tale previsione sembra porsi in continuità con le considerazioni già espresse, pur in assenza di univoche indicazioni *de iure condito*, da alcuni interpreti, secondo i quali la suddetta nozione sarebbe idonea a ricomprendere un insieme di strumenti che, dopo aver svolto una fase di *training*[8], consentano di estrarre informazioni da una gran mole di dati raccolti a mezzo di dispositivi digitali (cd. *big data*), utilizzandole, poi, per il

Technologies and the Tech Nirvana Fallacy, in *HastingsLJ*, 2020, p. 59, è stato definito come *CorpTech*.

[4] La proposta originaria della Commissione Europea è, infatti, datata 21 aprile 2021.

[5] Regolamento (Ue) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale.

[6] A seguito della definitiva approvazione del disegno di legge da parte del Senato, intervenuta in un momento successivo rispetto alla discussione del paper, è stata pubblicata in G.U. la l. 23 settembre 2025, n. 132, destinata ad entrare in vigore il 10 ottobre 2025.

[7] Cfr. art. 3, n. 1), Reg. (UE) 2024/1689: tale definizione ha sostituito quella contenuta nella Proposta di Regolamento 2021/0106 (COD) del 21 aprile 2021, il cui art. 3, n. 1), definiva il sistema di intelligenza artificiale come «un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare *output* quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono».

[8] In proposito si vedano ancora le considerazioni di M.L. Montagnani, *Intelligenza*, cit., pp. 1011-1012, la quale ricorda che le tecniche di apprendimento dell'intelligenza artificiale si suddividono, a seconda della tipologia di dati utilizzati allo scopo, in «supervisionate» o «non supervisionate»: nel primo caso, tipico delle I.A. *assisted* o *augmented*, gli *input* sono classificati prima di essere immessi nel sistema, mentre la seconda modalità di *training* presuppone l'inserimento di una gran mole di informazioni non categorizzate, che spetterà, poi, alla macchina raggruppare sulla base di caratteristiche comuni.

compimento di una serie di operazioni[9]. Quando queste ultime assumano natura predittiva, ci si potrà riferire, nello specifico, ai sistemi di *machine learning*, che, dotati di un meccanismo di apprendimento automatico, basano il proprio funzionamento su algoritmi idonei non solo a riprodurre pedissequamente i compiti affidatigli, ma tali da consentirgli anche di modificare e migliorare gli *outputs* nel corso del tempo sulla base dell'esperienza[10].

Orbene, l'indagine sul rapporto tra società algoritmica e mondo dell'impresa – settore che, peraltro, è stato individuato anche a livello politico come *target* di evoluzione e sviluppo dei sistemi di intelligenza artificiale nell'ambito del contesto economico nazionale[11] – è generalmente affrontata assumendo come referente soggettivo le compagini azionarie quotate sui mercati regolamentati, rispetto alle quali già è stato sostenuto che l'adozione di strumenti *tech* debba considerarsi come requisito necessario ai fini della valutazione di adeguatezza degli assetti[12]. Tuttavia, il rapido progredire dell'innovazione tecnologica induce ad una riflessione che consenta di estendere la portata dell'analisi anche al di fuori del suo ambito di elezione e che, segnatamente, si proponga di indagare le prospettive di applicazione dell'intelligenza artificiale in un diverso contesto, qual è quello del Terzo Settore. In particolare, il contributo proverà ad esaminare il tema avendo riguardo all'impresa sociale[13], qualifica[14] che può essere ottenuta da qualunque ente privato, anche di natura societaria[15], che eserciti in via stabile

---

[9] Così L. Enriques e D.A. Zetzsche, *Corporate*, cit., pp. 65-66, che individuano i sistemi di intelligenza artificiale come l'unico strumento idoneo ad analizzare un'enorme mole di complessi *big data* «*drawing conclusions as to the probability of an event from prior knowledge of conditions related to the event*».

[10] Sulla distinzione tra i concetti di I.A. intesa quale *genus* e *machine learning* cfr. M.L. Montagnani, *Intelligenza*, cit., p. 1010 (testo e nt. 34), e N. Abriani e G. Schneider, *Diritto*, cit., pp. 23 ss.

[11] Cfr. *Programma strategico Intelligenza Artificiale 2022-2024* del Governo italiano.

[12] Si vedano, in proposito, le considerazioni di R. Santagata, *Intelligenza artificiale, adeguatezza degli assetti "tecnici" e principio di precauzione nell'amministrazione delle società quotate*, in *Riv. dir. impr.*, 2022, pp. 307 ss.; M.L. Montagnani, *Intelligenza*, cit., pp. 1015-1016; N. Abriani e G. Schneider, *Diritto*, cit., pp. 213 ss.

[13] La cui disciplina è ora contenuta nel d.lgs. 3 luglio 2017, n. 112, che ha sostituito, abrogandolo espressamente, il previgente d.lgs. 24 marzo 2006, n. 155.

[14] Che l'impresa sociale non fosse un fosse un nuovo «tipo» di ente era già stato chiarito, subito dopo l'entrata in vigore del d.lgs. 155/2006, da R. Costi, *L'impresa sociale: prime annotazioni esegetiche*, in *Giur. comm.*, 2006, I, p. 862.

[15] Non, però, quando si tratti di società unipersonale costituita da un unico socio persona fisica, in virtù dell'espressa esclusione stabilita dall'art. 1, comma 2, d.lgs.

e principale[16] un'attività d'impresa di interesse generale[17] senza scopo di lucro[18] e per finalità civiche, solidaristiche o di utilità sociale[19], adottando modalità di gestione responsabili e trasparenti e favorendo il più ampio coinvolgimento degli *stakeholders*[20]. Prima, però, di affrontare *ex professo* tale profilo, appare opportuno chiarire quale sia la prospettiva di utilizzo nel cui prisma s'intende esaminare l'intelligenza artificiale, adottando l'ormai canonica suddivisione basata sul grado di succedaneità della macchina rispetto all'agire umano.

2. *Tecnologia in funzione «servente», non «sostitutiva»*

Come noto, uno degli elementi discriminanti spesso presi in considerazione per procedere a una categorizzazione dei sistemi di intelligenza artificiale si rinviene nella valutazione dell'idoneità di ciascun algoritmo a sostituire l'essere

---

112/2017.

[16] Ai sensi dell'art. 2, comma 3, d.lgs. 112/2017, il vincolo di prevalenza si intende ottemperato qualora i ricavi provenienti dall'attività di interesse generale siano superiori al 70% di quelli complessivi dell'impresa sociale, percentuale i cui relativi criteri di computo sono stati successivamente precisati con d.m. del 22 giugno 2021 del Ministero dello Sviluppo Economico di concerto con il Ministero del Lavoro e delle Politiche sociali, reperibile sul sito istituzionale *www.lavoro.gov.it*.

[17] Il catalogo delle attività di interesse generale è inserito all'interno dell'art. 2, comma 1, d.lgs. 112/2017: sul punto, anche in comparazione con quanto previsto dal Codice del Terzo Settore per gli E.T.S. intesi come *genus*, cfr. A. Fici, *L'attività degli enti del Terzo Settore*, in Aa.Vv., *Il Codice del Terzo settore. Commento al D.lgs. 3 luglio 2017, n. 117*, a cura di M. Gorgoni, 2ª ed., Pisa, 2021, pp. 65 ss., nonché M.L. Vitali, *Riforma del terzo settore, nuova disciplina dell'impresa sociale e regole societarie*, in *ODCC*, 2020, p. 91, e G. Marasà, *Appunti sui requisiti di qualificazione degli enti del terzo settore: attività, finalità, forme organizzative e pubblicità*, in *NLCC*, 2018, pp. 673-674.

[18] Che si tratti di un divieto di lucro «soggettivo» emerge chiaramente dal testo dell'art. 3, comma 1, d.lgs. 112/2017, nel quale si prevede che, in linea generale e salvo quanto si avrà modo di precisare *infra*, l'impresa sociale deve destinare «eventuali utili ed avanzi di gestione allo svolgimento dell'attività statutaria o ad incremento del patrimonio»: non è, pertanto, difficile notare come, potendo produrre *utili* ed *avanzi di gestione*, l'ente possa realizzare un lucro «oggettivo».

[19] Cfr. art. 1, comma 1, d.lgs. 112/2017.

[20] Secondo G. Marasà, *Gli enti del terzo settore: attività e scopi*, in *Riv. dir. civ.*, 2023, pp. 1172-1173, solo valorizzando tali prescrizioni sulla gestione socialmente responsabile si potrebbe garantire, quantomeno in linea di principio, che le imprese sociali costituite in forma societaria perseguano le finalità altruistiche previste dalla legge, le quali, altrimenti, rischierebbero di rimanere un mero auspicio a fronte delle rilevanti deroghe al divieto di distribuzione egoistica dei risultati dell'attività economica.

umano nello svolgimento di compiti tipicamente riservati allo stesso, distinguendosi, all'uopo, le I.A. con funzioni serventi e quelle, invece, sostanzialmente autonome. In tale prospettiva, la presente indagine si soffermerà esclusivamente sul possibile utilizzo, nell'ambito di un'impresa sociale, di strumenti definibili come *assisted AI* – che, dunque, fungano da mero ausilio all'amministratore umano, il quale rimarrà l'unico soggetto legittimato ad assumere decisioni – o, tutt'al più, come *augmented AI*, con tale locuzione intendendosi macchine in grado di agevolare l'organo gestorio nell'esercizio delle funzioni più complesse, senza, però, surrogarsi a quest'ultimo[21]. Un approfondimento che abbia ad oggetto una *autonomous AI* che sia in grado di sostituire un membro del C.d.A.[22] – o addirittura la sua totalità, integrando l'ipotesi del cd. *Roboboard*[23] – appare, infatti, poco coerente con l'impostazione del contributo, essenzialmente per due ordini di motivi. In primo luogo, invero, si condividono le perplessità degli studiosi che ritengono irrinunciabile nella gestione dell'impresa quella componente emotiva e creativa tipica dell'essere umano, che, quantomeno secondo lo stato attuale delle conoscenze tecniche, non è traslabile su una macchina, la quale, per quanto intelligente, difficilmente potrà essere proiettata *pro futuro*, essendosi allenata su *dataset* del passato[24]. Inoltre, l'adesione a un orientamento dichiaratamente prudente, ma indubbiamente più realista, appare vieppiù da condividere in ragione del fatto che le riflessioni che s'intende sviluppare riguardano un settore – il cd.

---

[21] Adotta la medesima impostazione concettuale, ad esempio, M.L. Montagnani, Governance *societaria e* governance *dell'intelligenza artificiale*, in *Merc. conc. reg.*, 2022, pp. 272-273.

[22] In proposito cfr., *ex multis*, F. Möslein, *Robots in the Boardroom: Artificial Intelligence and Corporate Law*, in *www.ssrn.com*, 2017, pp. 1 ss.; G.D. Mosco, *AI and the Board Within Italian Corporate Law: Preliminary Notes*, in *Eur. Comp. Law. Journal*, 2020, pp. 87 ss.

[23] Si veda lo scetticismo manifestato, ad esempio, anche da E. Rimini, *Intelligenza artificiale e doveri degli amministratori*, in *Riv. corp. gov.*, 2024, p. 90.

[24] Così R. Santagata, *Intelligenza*, cit., p. 309, il quale argomentava in questo senso alla luce dell'art. 14 della Proposta di Regolamento, oggi traslato nel medesimo articolo dell'*AI Act*, che, imponendo la sorveglianza umana nell'impiego delle nuove tecnologie, confermerebbe che queste ultime «restano pur sempre *mezzo* e non *fine* del corretto esercizio della discrezionalità gestoria» [corsivo nel testo originale, *n.d.r.*]; in proposito si vedano anche le condivisibili considerazioni di L. Enriques – A. Zorzi, *Intelligenza artificiale e responsabilità degli amministratori*, in *RDS*, 2023, pp. 16 ss., i quali sottolineano come, quand'anche si utilizzi l'*escamotage* dell'amministratore-persona giuridica per legittimare l'assunzione del ruolo gestorio da parte dell'algoritmo, non si potrebbe prescindere dalla designazione di un essere umano che, di fatto, adotti la decisione prescelta dall'intelligenza artificiale, la cui autonomia, sotto il profilo giuridico, è ancora lontana a venire.

«privato sociale» – che è in evidente ritardo rispetto a quello societario dal punto di vista della digitalizzazione e dell'implementazione di sistemi ad alto tasso tecnologico[25]. D'altro canto, a differenza di quanto accennato con riguardo alle grandi imprese azionarie, è opinione diffusa che un costante adeguamento delle strutture organizzative ad ogni evoluzione tecnica non rappresenti ancora un obbligo per compagini di medio-piccola dimensione che non facciano ricorso al mercato del capitale di rischio[26] e, a maggior ragione, non potrà, quindi, ritenersi doveroso per quegli enti che svolgano la loro attività economica in funzione altruistica. Assumendo come riferimento le imprese sociali che decidano volontariamente di adottare strumenti di IT o, addirittura, di intelligenza artificiale, il lavoro si propone, dunque, di esaminare, innanzitutto, i benefici che da tale scelta potrebbero derivare nel coinvolgimento dei soggetti interessati all'attività, in un'ottica di valorizzazione di quella prospettiva *multi-stakeholder* che deve connotare l'organizzazione degli enti in questione[27]. Inoltre, si proverà a verificare se, oltre a favorire l'*engagement* delle categorie ritenute rilevanti dall'ordinamento, l'implementazione di sistemi di I.A. possa, altresì, fungere da supporto per l'organo amministrativo nell'esercizio della sua tipica funzione di contemperamento di contrapposti interessi.

---

[25] In termini statistici, i dati più aggiornati in ordine alla digitalizzazione delle istituzioni *non profit*, pubblicati nell'aprile 2024, sono consultabili sul sito dell'ISTAT all'indirizzo *https://www.istat.it/tavole-di-dati/censimento-permanente-delle-istituzioni-non-profit-2/* e si riferiscono alla situazione al 31 dicembre 2021. Dalla lettura delle *Tabelle* diffuse dall'istituto di ricerca statistica – che, ovviamente, non sono limitate all'utilizzo della sola intelligenza artificiale, ma arrivano a comprendere anche l'analisi di fenomeni di digitalizzazione ben più banali, quali l'utilizzo di una connessione internet a banda larga – emerge che, su un totale di 360.625 istituzioni senza scopo di lucro sul territorio nazionale, circa il 79,5% (ossia 286.815 entità) fanno ricorso a tecnologie digitali, con una maggiore diffusione territoriale nel Nord-Ovest (cfr., in particolare, *Tavola* n. *19*) e nel settore delle attività sportive (cfr. *Tavola* n. *20*). Ovviamente, qualora si volesse limitare l'indagine alla sola adozione di sistemi di intelligenza artificiale i numeri risulterebbero drasticamente ridotti: si pensi, infatti, che soltanto 4.128 istituzioni, pari all'1,14% del totale, hanno dichiarato, al dicembre 2021, di utilizzare le tecniche riferibili ad «altra tecnologia digitale», nella quale rientrano *IoT*, Robotica e *Blockchain*.

[26] Anzi, R. Santagata, *Intelligenza*, cit., p. 315, segnala come, in tali contesti imprenditoriali, potrebbe addirittura configurarsi un'irrazionalità manifesta della scelta gestoria mediante cui si decida di adeguare tecnologicamente gli assetti nonostante gli elevatissimi costi all'uopo richiesti, in quanto non compensata da altrettanti benefici.

[27] Con il termine *multistakeholder*, indicato dalla nota enciclopedia Treccani, in *www.treccani.it*, come neologismo della lingua italiana, si indica ciò «che mira al coinvolgimento di più soggetti interessati a un'attività».

3. *Il coinvolgimento degli* stakeholders *mediante l'impiego dell'I.A.*

La tesi secondo cui l'impiego di sistemi di I.A. consentirebbe di facilitare il coinvolgimento dei soggetti interessati all'andamento di un'attività economica – idea che in alcuni studi su grandi realtà multinazionali ha addirittura ispirato proposte di rivisitazione dei tradizionali assetti di *governance* volte a rendere la gestione societaria più orizzontale e aperta agli *shareholders*[28] – stimola una riflessione che s'interroghi sulla possibilità di pervenire a medesimi esiti anche con riguardo alle imprese sociali, che sono considerate come una delle più fulgide manifestazioni della tendenza legislativa alla valorizzazione di iniziative organizzate in una prospettiva *multi-stakeholder*[29]. A chiara dimostrazione di tale assunto può leggersi l'ultima parte dell'art. 1, comma 1, d.lgs. 112/2017, che subordina l'acquisizione della qualifica *de qua* alla circostanza che gli enti favoriscano il «più ampio coinvolgimento dei lavoratori, degli utenti e di altri soggetti interessati alle loro attività»[30]. Tralasciando in questa sede l'embrionale forma di cogestione ispirata al modello tedesco, la cui operatività è confinata a determinate imprese che superino prescritte soglie dimensionali[31], l'*engagement* delle categorie individuate dal legislatore[32] si sostanzia, ai sensi dell'art. 11, d.lgs.

---

[28] Si fa riferimento al fenomeno della cd. «*platform governance*», più aperta alla comunità.

[29] Tale approccio, d'altro canto, caratterizza anche il modello delle società *benefit*, sul quale si avrà modo di soffermarsi nel prosieguo: sulla natura volontaristica dell'impegno sociale assunto dagli *shareholders* nel contesto di tali compagini cfr. S. Rossi, *L'impegno* multistakeholder *della società* benefit, in *Rivista ODC*, 2017, pp. 1 ss.; sul *multistakeholder approach* ivi adottato si veda anche il recente contributo di M. Palmieri, *Le società* benefit, in *Giur. comm.*, 2023, I, pp. 1035-1036.

[30] Sulla prospettiva *multi-stakeholder* degli E.T.S. e, in particolare, dell'impresa sociale, si vedano le riflessioni di M. Tola, *La* governance *degli enti del terzo settore e i sistemi* multistakeholders, in *Riv. soc.*, 2019, pp. 402 ss.; sul punto cfr. anche F. Greco, *Categorie di enti del Terzo settore*, in Aa.Vv., *Il Codice*, cit., p. 338.

[31] Sulla novità introdotta dall'art. 11, comma 4, lett. *b*), cfr., in particolare, M. Tola, *o.c.*, pp. 404 ss. e M. Palmieri, *La* corporate governance *delle imprese sociali riformate. Dal* multistakeholder approach *verso la* Mitbestimmung, in *AGE*, 2018, pp. 125 ss.

[32] La categoria dei «soggetti direttamente interessati» – che, come evidenziato da M. Tola, *o.c.*, pp. 411-412 (testo e nt. 56-57), è così ampia da poter ricomprendere chiunque possa ricevere vantaggi o svantaggi dall'impresa in termini economici, di utilità, o, addirittura, morali – sembra richiamare la locuzione «altri portatori di interesse» menzionata dall'art. 1, comma 378, lett. *b*), l. 208/2015 sulle società *benefit*, con la differenza che, in quest'ultimo caso, il legislatore non ha previsto un coinvolgimento nell'impresa, ma solo che l'interesse manifestato da tali *stakeholders* debba essere oggetto

112/2017[33], nella predisposizione di meccanismi di consultazione o partecipazione[34] – da prevedersi, in forma adeguata, all'interno dei regolamenti aziendali o nello statuto[35] – che consentano di influenzare le decisioni dell'ente[36]. La determinazione delle modalità del coinvolgimento è delegata all'autonomia organizzativa, nel cui legittimo esercizio, però, il soggetto *non profit*, oltre a dover tener conto dei parametri relativi alla natura dell'attività esercitata, delle categorie soggettive rilevanti e delle dimensioni dell'impresa, dovrà assicurare il rispetto, quantomeno, di un contenuto minimo sancito dalle linee-guida ministeriali[37]. Queste ultime, in particolare, si sono ampiamente soffermate sui diritti di «informazione» e di «consultazione» degli *stakeholders*, rispetto ai quali, dunque, è opportuno analizzare il possibile impatto della transizione digitale e, in ottica futura, anche dei sistemi di intelligenza artificiale.

---

di contemperamento con le altre esigenze.

[33] Da quest'obbligo sono, però, esonerati, ai sensi del comma 5 dello stesso art. 11, gli enti religiosi civilmente riconosciuti e le cooperative a mutualità prevalente, di cui fanno parte *ex lege* le cooperative sociali (cfr. art. 111-*septies* disp. att. c.c.), le quali, allo stato attuale, rappresentano ancora la forma giuridica maggiormente diffusa tra le imprese sociali, ma che, alla luce delle tendenze più recenti di cui si dirà nelle conclusioni, non sembrano più detenere un monopolio in tal senso.

[34] In particolare, ai sensi dell'art. 11, comma 4, lett. *a*), d.lgs. 112/2017, lo statuto deve, «in ogni caso», disciplinare i casi e le modalità della partecipazione dei «lavoratori» e degli «utenti», anche tramite loro rappresentanti, all'assemblea degli associati o dei soci.

[35] Il d.m. 7 settembre 2021 – anch'esso reperibile sul sito *www.lavoro.gov.it* – con cui il Ministero del Lavoro e delle Politiche Sociali, previo parere del Consiglio nazionale del Terzo settore, ha adottato le linee-guida sul coinvolgimento degli *stakeholders* si è premurato di precisare che la scelta legislativa di fare riferimento allo statuto piuttosto che all'atto costitutivo si spiega sia per una ragione formale che per una sostanziale. Quanto alla prima motivazione, infatti, «lo statuto, in quanto atto destinato a contenere le norme sull'organizzazione e sul funzionamento dell'impresa sociale, rappresenta uno strumento maggiormente appropriato ai fini della specificazione delle forme e modalità di coinvolgimento in parola rispetto all'atto costitutivo, espressione, quest'ultimo, della volontà degli associati o dei soci di dar vita ad un'impresa sociale». Sotto il profilo sostanziale, poi, lo statuto, essendo per sua natura modificabile, può agevolmente recepire «gli adeguamenti della disciplina sul coinvolgimento che siano ritenuti necessari o opportuni anche in relazione alle evidenze applicative scaturite dalla precedente regolazione ovvero a mutamenti del contesto socio-economico di riferimento».

[36] Con particolare riguardo alle questioni che incidano direttamente sulle condizioni di lavoro e sulla qualità di beni e servizi, come precisato dall'art. 11, comma 2, d.lgs. 112/2017.

[37] Cfr. art. 11, comma 3, d.lgs. 112/2017.

Va, in proposito, evidenziato che, mentre l'esercizio delle facoltà informative degli interessati – consistenti in «un esame adeguato delle informazioni fornite e [nel, *n.d.r.*] formulare, sempre con modalità individuate dai regolamenti o statuti sociali, eventuali pareri non vincolanti da fornire all'organo amministrativo»[38] – pare assicurato già dall'impiego di semplici strumenti di IT[39], rischiando, anzi, l'adozione di dispositivi troppo evoluti sotto il profilo tecnologico di violare il principio di proporzionalità[40], l'I.A. potrebbe produrre esternalità positive se rapportata alla seconda forma di coinvolgimento. Infatti, il diritto di consultazione, solitamente appannaggio di rappresentanti nominati da organi *ad hoc*[41], può concretizzarsi, qualora si richieda l'acquisizione di un numero maggiore di pareri o valutazioni su specifiche tematiche, mediante «il ricorso a modalità più estese, anche a carattere periodico (ad esempio con cadenza annuale), come quelle telematiche (consultazione on-line degli utenti)»[42]. E allora, in tale prospettiva, se la digitalizzazione delle comunicazioni agevola la raccolta di *feedback* da parte degli *stakeholders* interpellati, l'intelligenza artificiale, intervenendo nella successiva fase di elaborazione dei dati, potrebbe consentire una loro più rapida, precisa ed efficace analisi, e, all'esito di una mappatura delle categorie di interessati, pervenire ad *outputs* che siano maggiormente rispondenti alle istanze di questi ultimi[43]. Da un punto di vista tecnico, dovendo la consultazione assumere i caratteri della «regolarità» e dell'«effettività»[44], si potrebbe immaginare che la stessa possa avvenire anche attraverso delle piattaforme di *crowdfunding*, che, seppur siano nate come mezzo di finanziamento dell'impresa, potrebbero essere utilizzate anche allo scopo di aprire dei canali di comunicazione con gli utenti e la comunità di riferimento[45].

---

[38] Cfr. § 2.2, lett *a*), d.m. 7 settembre 2021, All. n. 1.

[39] Essendo, d'altronde, previsto dallo stesso decreto ministeriale che le informazioni debbano essere rese disponibili «anche attraverso strumenti telematici e informatici idonei ad assicurare un accesso facile ed incondizionato, come ad esempio il sito internet dell'impresa o una *newsletter* informativa periodica rivolta agli appartenenti alle varie categorie o ai loro rappresentanti».

[40] Cfr., in proposito, l'orientamento dottrinale richiamato in nota 26.

[41] Nel d.m. del 7 settembre 2021, ad esempio, è citata la costituzione di appositi comitati o di assemblee speciali dei lavoratori, che, peraltro, sono abilitati anche ad esprimere pareri.

[42] Si veda, sul punto, § 2.2, lett *b*), d.m. 7 settembre 2021, All. n. 1.

[43] Cfr., ancora, N. Abriani e G. Schneider, *Diritto*, cit., p. 247.

[44] Secondo quanto prescritto dalle linee-guida, con tale terminologia deve intendersi, rispettivamente, «la stabilità della stessa [della consultazione, *n.d.r.*] nel tempo» e la «concreta idoneità della stessa a promuovere la partecipazione dei lavoratori e degli utenti».

[45] V. Cavotta, E. Grassi e L. Toschi, *Uso delle tecnologie digitali da parte degli imprenditori e innovatori sociali: potenzialità e limiti*, in *Riv. impr. soc.*, 2022, p. 32, citano,

Una volta che siano state acquisite ed elaborate le informazioni relative alle esigenze dei vari *stakeholders* – che, peraltro, possono divergere in maniera consistente tra loro –, compito dell'organo gestorio dell'impresa sociale è quello di assumere, anche sulla base dei dati raccolti, decisioni in funzione del perseguimento degli scopi istituzionali dell'ente. A tale aspetto e al ruolo che potrà essere, all'uopo, rivestito dai sistemi di intelligenza artificiale sarà, allora, dedicato il prossimo paragrafo, le cui conclusioni, come si avrà modo di vedere, trarranno spunto anche dagli studi concentratisi sul contemperamento di interessi nelle società *benefit*, modello vicino, ma non perfettamente sovrapponibile, a quello qui in esame.

4. *Le finalità dell'impresa sociale e l'impatto dell'intelligenza artificiale sul contemperamento d'interessi*

L'impresa sociale, qualunque sia la sua natura giuridica, deve perseguire finalità civiche, solidaristiche e di utilità sociale[46] ed è sottoposta a un tendenziale divieto di distribuzione egoistica dei risultati dell'attività svolta[47], in coerenza con quanto previsto, in termini assoluti, dal Codice del Terzo Settore (d.lgs. 3 luglio 2017, n. 117, e ss. mm. ii.) per gli E.T.S. intesi quale categoria[48]. La preclusione *de qua*, in realtà, subisce dei forti temperamenti nell'ipotesi in cui la condotta imprenditoriale d'interesse generale sia imputabile ad un ente organizzato nelle forme di cui al Libro V del Codice Civile[49], dal momento che il legislatore con-

ad esempio, la piattaforma *Spacehive*, che mette in comunicazione finanziatori, comunità locali e beneficiari che intendano portare avanti un medesimo progetto di sviluppo.

[46] Sulla triade finalistica, seppur con riferimento agli enti del Terzo Settore intesi quale *genus*, cfr. M. Gorgoni, *Il Codice del Terzo settore tra luci ed ombre*, in Aa.Vv., *Il Codice*, cit., pp. 43 ss.; sui rapporti tra attività di interesse generale e finalità si veda, per tutti, A. Fici, *Nozione e disciplina dell'impresa sociale dopo la riforma del terzo settore*, in Aa.Vv., *Le "nuove" imprese sociali. Tendenze e prospettive dopo la riforma del terzo settore*, a cura di L. Bobba, A. Fici e C. Gagliardi, Napoli, 2022, pp. 27 ss.

[47] Cfr., nuovamente, art. 3, comma 1, d.lgs. 112/2017.

[48] Si veda, in particolare, l'art. 8, d.lgs. 117/2017.

[49] Modello organizzativo rispetto al quale, peraltro, secondo A. Cetra, *Enti del terzo settore e attività d'impresa*, in *RDS*, 2019, pp. 678 ss., si riscontrerebbe un *favor* legislativo, dimostrato sia dalla particolare disciplina relativa alla distribuzione dei risultati sia dalla previsione di misure di sostegno finanziario.

sente sia alle cooperative[50], anche sociali[51], sia alle società «ordinarie» dotate della qualifica di cui al d.lgs. 112/2017 di introdurre delle clausole che vi deroghino, seppur parzialmente[52]. La circostanza che l'adozione di tali previsioni statutarie sia immaginata come una «facoltà» – e non un «obbligo» –, oltre ad integrare una chiara eccezione al dettato dell'art. 2247 c.c.[53], rende manifesta la differenza tra un'impresa sociale societaria e una compagine qualificabile come *benefit*[54],

---

[50] In tal caso, il comma 2-*bis* del medesimo articolo 3, d.lgs. 112/2017, aggiunto dal d.lgs. 95/2018, prevede che la ripartizione ai soci di ristorni correlati ad attività di interesse generale effettuata ai sensi dell'art. 2545-*sexies* c.c. non sarà considerabile come distribuzione, neanche indiretta, di utili ed avanzi di gestione, se lo statuto o l'atto costitutivo indica i criteri di ripartizione dei ristorni ai soci proporzionalmente alla quantità e alla qualità degli scambi mutualistici e si registra un avanzo della gestione mutualistica: in sostanza, come sottolineato da G. Marasà, *Gli enti,* cit., p. 1171, le somme percepite a tale titolo potranno sommarsi a quelle chieste quale remunerazione del capitale.

[51] Per i vantaggi derivanti dalla scelta di tale forma mutualistica, che, ai sensi dell'art. 1, comma 4, d.lgs. 112/2017, è impresa sociale «di diritto», si veda ancora G. Marasà, *o.u.c.*, pp. 1171-1172.

[52] Infatti, l'art. 3, comma 3, d.lgs. 112/2017, permette all'impresa sociale costituita nelle forme del Libro V di destinare una quota prestabilita degli utili annuali – inferiore al 50%, dedotte eventuali perdite maturate negli esercizi precedenti – alla distribuzione di dividendi ai soci «seppur in misura comunque non superiore all'interesse massimo dei buoni postali fruttiferi, aumentato di due punti e mezzo rispetto al capitale effettivamente versato»: questo spiega, nella condivisibile ricostruzione di G. Marasà, *Appunti*, cit., p. 679, perché il legislatore non abbia imposto il perseguimento delle finalità sociali in via esclusiva; tale disposizione, visti i suoi limiti imperativi e la necessità di una specifica clausola statutaria, non viene, però, considerata dogmaticamente rilevante da M. Arrigoni, *La riforma del terzo settore e la nuova disciplina dell'impresa sociale. Alcune implicazioni sistematiche*, in *Riv. soc.*, 2019, p. 84.

[53] La circostanza che l'impresa sociale possa essere costituita in forma societaria e che, anche in tal caso, lo scopo di lucro sia considerato quale elemento meramente eventuale dal legislatore, induce M.L. Vitali, *Riforma*, cit., p. 98, a sostenere che tale scelta normativa abbia sostanzialmente avallato, quantomeno con riguardo al perseguimento degli interessi di natura generale individuati nella disciplina speciale, l'idea della «neutralità» causale e teleologica del tipo societario; in termini analoghi cfr. anche M. Arrigoni, *o.c.*, pp. 84 ss.; M. Porzio, *Associazioni, fondazioni e società nell'evoluzione dell'ordinamento italiano*, in *Giur. comm.*, 2021, I, p. 225, sembra sminuire la rilevanza della previsione di legge, affermando che, comunque, ci si trovi dinnanzi a una società di diritto speciale.

[54] Si tratta di un modello introdotto nel nostro ordinamento, ispirandosi alla legislazione nordamericana, dall'art. 1, commi dal 376 al 384, l. 28 dicembre 2015, n. 208 (*Legge di Stabilità* 2016): per alcune considerazioni generali sulla società *benefit*, si

cui è richiesto lo svolgimento di un'attività imprenditoriale[55] mirante tanto alla divisione degli utili quanto alla realizzazione di scopi di beneficio comune[56], che, specificamente indicati nell'oggetto sociale[57], devono essere perseguiti «mediante una gestione volta al bilanciamento con l'interesse dei soci e con l'interesse di coloro sui quali l'attività sociale possa avere un impatto»[58].

---

veda, *ex multis*, la recente monografia di P. Butturini, *Società benefit e diritto di recesso*, Torino, 2022, pp. 1 ss.; peraltro, la scelta del legislatore di inserire il modello all'interno di un numero così limitato di commi di una legge di stabilità è criticata da G.M. Nori, *La società Benefit un (nuovo?) mezzo per (non) fare impresa*, in *RDS*, 2021, pp. 799-800. Sull'influenza esercitata dalla legislazione del Maryland e del Delaware si vedano le interessanti notazioni di M. Palmieri, *Le società*, cit., pp. 1030 ss.; tra i contributi elaborati dalla dottrina statunitense si vedano, *ex multis*, J.H. Murray, *Social enterprise innovation: Delaware's public benefit corporation law*, in *HBLR*, (345), 2014, pp. 355-356; R. Thorelli, *Providing Clarity for Standard of Conduct for Directors within Benefit Corporations: Requiring Priority of a Specific Public Benefit*, in *Minn. L. Rew.*, (101), 2017, p. 1771, che prestano particolare attenzione alla differenza tra il *duty to «balance»* e il *duty to «consider»*.

[55] Attività che, come puntualmente segnalato da P. Guida, *La «società benefit» quale nuovo modello societario*, in *Riv. not.*, 2018, I, p. 504, non è soggetta ai ristretti limiti tipologici richiesti per l'impresa sociale, ma, purché protesa alla realizzazione di un beneficio comune, può essere liberamente scelta.

[56] Si tratta, secondo la ricostruzione di U. Tombari, *"Potere" e "interessi" nella grande impresa azionaria*, Milano, 2019, pp. 70-71, di parte dello «scopo-fine» dell'ente, frutto di una libera scelta dei soci, a vantaggio della cui autonomia – e non come rafforzamento della posizione degli *stakeholders* non finanziari – il legislatore avrebbe introdotto il nuovo modello societario; tale ultima considerazione era stata già sviluppata, peraltro con ampi riferimenti alla dottrina nordamericana, in F. Denozza e A. Stabilini, *La società* benefit *nell'era dell'*investor capitalism, in *Rivista ODC*, 2017, pp. 1-2.

[57] Sul punto si vedano le osservazioni di G.A. Rescio, *L'oggetto della società* benefit, in *Riv. dir. civ.*, 2022, pp. 462 ss.

[58] Cfr., in particolare, l'art. 1, comma 377, l. 218/2015, cit., che sembra trovare una precisazione all'interno del successivo comma 380, in cui si prevede testualmente che «la società *benefit* è amministrata in modo da bilanciare l'interesse dei soci, il perseguimento delle finalità di beneficio comune e gli interessi delle categorie indicate nel comma 376 conformemente a quanto previsto dallo statuto»: dal momento che tale obbligo di contemperamento è espressamente contemplato solo nella disciplina delle società *benefit*, U. Tombari, *L'organo amministrativo di S.p.A tra "interessi dei soci" ed "altri interessi"*, in *Riv. soc.*, 2018, p. 27 – e Id., *"Potere"*, cit., pp. 71-72 – propende, alla luce di un'interpretazione *a contrario*, per l'insussistenza di tale dovere di composizione a carico dell'organo amministrativo delle compagini *non benefit*; in senso critico rispetto a questa contrapposizione – se intesa in termini di rigida antinomia – si veda P. Montalenti, *L'interesse sociale: una sintesi*, in *Riv. soc.*, 2018, p. 318; peraltro,

Ora, benché il modello dell'impresa sociale sia distinto, sotto l'aspetto finalistico, da quello della società *benefit*[59], il richiamo a quest'ultima appare utile in quanto la stessa rappresenta comunque un'ottima cartina al tornasole per approfondire il potenziale impatto di sistemi di intelligenza artificiale sulle procedure di contemperamento di contrapposte esigenze nell'ambito di organizzazioni teleologicamente «ibride»[60]. In proposito, benché non manchino delle opinioni tendenti a promuovere l'impiego delle nuove tecnologie nell'esercizio della suddetta funzione tipicamente gestoria[61], la tesi che appare allo stato prevalente sembra orientarsi in senso opposto, evidenziando come simili decisioni «di vertice» siano connotate da un grado di discrezionalità tale da non poter essere riprodotto da alcun sistema di I.A.[62], per quanto particolarmente avan-

---

secondo A. Daccò, *Spunti di riflessione su capitalismo sostenibile e strumenti a disposizione*, in *Banca, borsa, tit. cred.*, 2022, I, p. 380, non può escludersi che nell'effettuare tale bilanciamento lo scopo di lucro risulti subordinato rispetto alle finalità sociali.

[59] E, infatti, M. Palmieri, *Le società*, cit., p. 1034 (nt. 17), evidenzia come la rigidità in ordine agli scopi altruistici che deve perseguire un'impresa sociale sembrerebbe incompatibile con l'acquisizione della suddetta qualifica da parte di una società *benefit*, in cui il contemperamento degli interessi è soggetto ad ampia discrezionalità del *management*; secondo M.L. Vitali, *Riforma*, cit., p. 98, le società *benefit*, avendo un duplice orientamento teleologico, si porrebbero dogmaticamente in posizione mediana tra le s.p.a. con scopo (esclusivamente) lucrativo e l'impresa sociale societaria non lucrativa.

[60] Sul punto, infatti, L. Enriques – A. Zorzi, *Intelligenza*, cit., p. 23, evidenziano come, pur potendosi porre la questione anche con riguardo a società lucrative «ordinarie», il problema sia enfatizzato in presenza di una duplicazione teleologica.

[61] Cfr., in proposito, N. Abriani e G. Schneider, *Diritto*, cit., pp. 232-233; seppur con riguardo allo specifico tema del rapporto tra società quotate e *stakeholders* diversi dagli azionisti, sembra argomentare nello stesso senso anche R. Santagata, *Intelligenza*, cit., pp. 312-313, secondo il quale l'utilizzo di sistemi di *machine learning* come ausilio alle decisioni gestorie potrebbe mitigare la naturale tendenza umana al perseguimento di scopi egoistici.

[62] A maggior ragione se si accoglie la tesi di G. Marasà, *Imprese sociali, altri enti del terzo settore, società* benefit, Torino, 2019, p. 15, secondo cui il legislatore non avrebbe preventivamente disposto alcuna graduazione degli scopi della società *benefit*; nel medesimo senso cfr. G.M. Nori, *La società*, cit., pp. 801-802; sulla questione si veda anche A. Daccò, *Le società* benefit *tra interesse dei soci e interesse dei terzi: il ruolo degli amministratori e i profili di responsabilità in Italia e negli Stati Uniti*, in *Banca, borsa, tit. cred.*, 2021, I, pp. 55 ss., la quale, valorizzando la comparazione con l'esperienza statunitense, evidenzia come l'adempimento del dovere di bilanciamento di interessi garantisca agli amministratori spazi di discrezionalità addirittura più ampi rispetto a quelli delle comuni compagini *for profit*, ma, allo stesso tempo, renda necessario il rispetto di più stringenti regole procedimentali, la cui eventuale violazione, non

zato[63]. All'algoritmo potrebbe essere, tutt'al più, affidata la mansione di individuare le modalità più consone a soddisfare le finalità dell'ente basandosi su una graduazione di interessi già effettuata *ex ante* dagli amministratori umani[64], nonché il compito di accentuare l'impatto sociale dell'azione istituzionale[65].

Le considerazioni appena sviluppate, pur se immaginate avendo riguardo alla società *benefit*, in cui l'operazione di bilanciamento si configura in termini di doverosità[66], sono replicabili anche quando la valutazione tra contrapposte esigenze sia richiesta ad una – analogamente «ibrida» – impresa sociale che abbia inteso

potendosi applicare la *business judgement rule*, risulterebbe assolutamente sindacabile in sede giudiziaria; concordano in merito all'osservazione secondo cui nelle società *benefit* la discrezionalità dell'organo gestorio risulterebbe incrementata anche M. Stella Richter Jr., M.L. Passador e C. Sertoli, *Tendenze e prospettive delle società* benefit, in *AGE*, 2022, pp. 229 ss.

[63] Così L. Enriques – A. Zorzi, *Intelligenza*, cit., pp. 29-30, nonché C. Picciau, *Intelligenza artificiale, scelte gestorie e organizzazione delle società per azioni*, in *Nuovo dir. soc.*, 2022, p. 1261 (testo e nt. 26), la quale sembra aderire alla tesi avanzata anche nel contesto nordamericano da M. Petrin, *Corporate management in the age of AI*, in *Col. Bus. L. Rev.*, 2019, pp. 983 ss., volta a differenziare tra le ipotesi di *administrative work*, che, essendo a carattere routinario, sarebbero integralmente delegabili a sistemi di intelligenza artificiale, e quelle di *judgement work*, le quali, invece, sarebbero di stretta pertinenza umana.

[64] Cfr. L. Enriques – A. Zorzi, *o.c.*, pp. 26 ss., i quali segnalano gli effetti positivi e negativi di tale irrigidimento; in questo senso sembrano esprimersi, con specifico riguardo alle società *benefit*, anche N. Abriani e G. Schneider, *Diritto*, cit., 232-233; d'altro canto, E. Rimini, *Intelligenza*, cit., p. 93, pone in evidenza come alcune regole o passaggi di una decisione siano solo tacitamente oggetto di comprensione e, dunque, difficilmente traslabili in un linguaggio di programmazione per un sistema di I.A.

[65] Si pensi, ad esempio, alle campagne di sensibilizzazione personalizzate mediante l'utilizzo dell'intelligenza artificiale: come giustamente evidenziato da V. Cavotta, E. Grassi e L. Toschi, *Uso*, cit., p. 31, però, la concretizzazione dei benefici offerti dalla digitalizzazione non può prescindere anche dal mettere a disposizione degli utenti – spesso appartenenti a categorie svantaggiate – un adeguato supporto che consenta loro l'utilizzo degli strumenti tecnologici fornitigli.

[66] In ordine ai parametri normativi sui quali debba fondarsi il bilanciamento si rinvia, *ex multis*, alla Circolare Assonime, *La disciplina delle società benefit*, 20 giugno 2016, n. 19, reperibile in *www.assonime.it*, pp. 22-23; S. Corso, *Le società benefit nell'ordinamento italiano: una nuova "qualifica" tra* profit *e* non-profit, in *NLCC*, 2016, p. 1021; A. Zoppini, *Un raffronto tra società* benefit *ed enti* non profit*; implicazioni sistematiche e profili critici*, in *Rivista ODC*, 2017, p. 7; E. Codazzi, *Società benefit (di capitali) e bilanciamento di interessi: alcune considerazioni sull'organizzazione interna*, in *Rivista ODC*, 2020, pp. 614-615.

derogare alla clausola di non devoluzione degli utili[67]. Anche in questo caso, invero, l'organo amministrativo sarà chiamato a considerare – nell'ottica di un loro contemperamento – tanto gli interessi di natura economica dei soci quanto le finalità istituzionali dell'ente, assumendo, poi, decisioni che, seppur connotate da minore discrezionalità in quanto vincolate al rispetto dei più stringenti limiti sanciti dal d.lgs. 112/2017[68], non potranno essere delegate a sistemi di intelligenza artificiale. Anche nel contesto dell'imprenditoria sociale, però, l'implementazione delle nuove tecnologie potrà avere un impatto nella successiva fase di esecuzione delle scelte gestorie, migliorando la qualità dei servizi offerti ai beneficiari, come dimostrato da alcune esperienze pratiche sviluppatesi in ambito nordamericano[69]. Emblematico appare, in questo senso, il caso della *Benetech*, organizzazione *non profit* statunitense, il cui *core business* è rappresentato da un'attività di conversione digitale di libri che ne consente la fruibilità da parte di categorie svantaggiate, quali soggetti affetti da cecità, ipovisione o altri disturbi come la dislessia[70]. Orbene, mentre i testi caratterizzati dalla presenza di sole parole e punteggiatura sono facilmente «traducibili» in linguaggio informatico mediante l'uso di ordinari *screen reader*, l'intelligenza artificiale si è dimostrata indispensabile per conseguire risultati altrettanto validi sui libri di matematica, una cui adeguata trasformazione, vista la presenza di grafici ed equazioni, non si sarebbe potuta, altrimenti, ottenere mediante l'impiego di ordinari strumenti di IT, ma solo con l'intervento da parte di un addetto che avrebbe, però, evidentemente richiesto un lasso temporale infinitamente maggiore per lo svolgimento del medesimo compito[71].

---

[67] In realtà, è bene sottolineare come, benché la questione si manifesti con maggiore evidenza quando l'impresa sociale abbia derogato al divieto di devoluzione degli utili, nulla esclude che eventuali contrasti possano insorgere anche tra interessi di *stakeholders* diversi dai soci – come, ad esempio, lavoratori e beneficiari dell'attività – le cui esigenze, allora, saranno da sottoporre ad attento esame da parte dell'organo gestorio.

[68] Peraltro criticati per la loro eccessiva ampiezza da G.D. Mosco, *L'impresa non speculativa*, in *Giur. comm.*, 2017, I, pp. 227-228.

[69] Di particolare interesse sul punto appare il saggio di V. Cavotta, E. Grassi e L. Toschi, *Uso*, cit., pp. 29 ss., nel quale ci si riferisce essenzialmente ad imprese operanti nel settore dell'inclusione sociale o in quello sanitario.

[70] In particolare, l'accessibilità è garantita, a seconda delle necessità, dalla conversione del testo in audiolibro, dall'utilizzo dell'alfabeto *braille* ovvero, infine, dall'utilizzo del formato o dell'evidenziazione che sia più adatta ad ogni singolo lettore.

[71] Infatti, come può leggersi sul sito internet della *Benetech* (*https://benetech.org*), l'operazione di individuazione e trasformazione di una media di circa 5.000 equazioni presenti in un testo di matematica che un essere umano riuscirebbe a condurre a termine in circa 3-4 mesi di lavoro, può essere svolta in pochi minuti dai sistemi di

5. *Lo sviluppo della cultura digitale nell'ambito dell'impresa sociale e le prospettive in ottica giuridica*

Naturalmente, sullo sfondo di tutto quanto si è detto in ordine al coinvolgimento degli *stakeholders* e all'impiego dell'I.A. nelle operazioni di bilanciamento di contrapposti interessi, si pone la questione, di evidente rilevanza pratica, relativa all'adeguatezza delle conoscenze digitali dei soggetti che sono chiamati all'utilizzo dei sistemi innovativi di cui si è discusso. Se nell'ambito delle ricerche sulle società quotate gli studiosi si sono già spinti a una declinazione del tema nella prospettiva delle specifiche competenze richieste ai componenti del C.d.A.[72] – con ragionamenti che spaziano dall'attribuzione di un *casting vote* in favore degli amministratori dotati di *expertise* tecnologica[73] sino all'istituzione di un vero e proprio comitato *tech* addetto alla gestione, al controllo e allo sviluppo dei sistemi di I.A.[74] – in questa sede ci si limiterà ad offrire alcuni spunti relativi a

---

intelligenza artificiale predisposti dagli ingegneri dell'organizzazione in questione. Tali tecnologie, consistenti in sistemi di *machine learning*, *computer visions* e reti neurali, una volta identificata l'equazione graficamente presente sul testo, a seguito di un processo di scansione, consentono di trasformarla in un codice matematico dotato di accessibilità e affidabilità. Le equazioni dal sistema considerate più affidabili sono immediatamente inserite nel *file* digitale del libro messo a disposizione dei beneficiari, mentre solo quelle più complesse sono lasciate alla revisione finale di un correttore umano.

[72] Con riguardo alle società quotate, ad esempio, R. Santagata, *Intelligenza*, cit., p. 319, conclude nel senso che, affinché gli amministratori non esecutivi possano ottemperare al loro dovere di agire informati ai sensi dell'art. 2381, comma 6, c.c., si richiede che almeno uno dei consiglieri conosca le caratteristiche tecniche del procedimento decisionale digitalizzato e, pertanto, oltre che poterne monitorare costantemente l'andamento, sia in grado di trasmettere le relative informazioni all'intero organo; in proposito, M.L. Montagnani, *Intelligenza*, cit., pp. 1014 ss., pone l'accento sulla necessità di ricorrere a sistemi di intelligenza artificiale che siano quanto più trasparenti possibili – sia con riguardo agli *input* utilizzati che al procedimento sviluppato dall'algoritmo per pervenire all'*output* – onde consentire che il loro funzionamento sia compreso da amministratori non necessariamente *tech-savvy*, ma, quantomeno, *tech-friendly*.

[73] Così N. Abriani e G. Schneider, *Diritto*, cit., p. 206.

[74] Per degli spunti in questo senso cfr., ancora, N. Abriani e G. Schneider, *o.c.*, pp. 204 ss.; L. Enriques e D.A. Zetzsche, *Corporate*, cit., pp. 93-94; R. Santagata, *Intelligenza*, cit., p. 322; M.L. Montagnani, *Intelligenza*, cit., pp. 1020 ss., sottolinea come un eventuale *tech committee* dovrebbe essere composto da soli amministratori indipendenti o, comunque, da una maggioranza di indipendenti non esecutivi, dotati di specifiche competenze in tema di tecnologia; E. Rimini, *Intelligenza*, cit., p. 98, poi, non disdegna neppure la possibilità di prevedere un *advisory board*, esterno al C.d.A., ovvero di designare un dirigente preposto all'intelligenza artificiale, analogamente a quanto

plausibili risvolti a carattere giuridico che potrebbero derivare da un progressivo sviluppo della cultura digitale degli addetti all'interno di strutture organizzative normalmente molto meno articolate, quali sono quelle delle imprese sociali.

Invero, da un punto di vista empirico, va evidenziato come dall'ultimo censimento ISTAT sul livello di innovazione degli enti *non profit*[75] emerga uno scenario assolutamente poco confortante, considerato che una delle più frequenti motivazioni addotte dalle istituzioni non lucrative per giustificare il mancato utilizzo di strumenti di IT o di altre tecnologie sia proprio quella della carenza di personale in grado di utilizzarli e dell'assenza di formazione in materia[76]. Tale *vulnus*, peraltro, non è confinato solo al settore del «privato sociale», ma trova ancora riscontro anche nei *report* statistici dedicati alla categoria delle P.M.I.[77] (alla quale spesso sono riconducibili anche le imprese di cui al d.lgs. 112/2017), benché le rilevazioni più recenti dimostrino come siano in crescita le organizzazioni con un numero di addetti compreso tra i 10 e i 249 ad impiegare mezzi di intelligenza artificiale[78] e sia sempre più diffusa, tra queste, l'attitudine all'assunzione di specialisti in materia *ICT*[79]. Il delineato quadro rende evidentemente apprez-

---

previsto per la documentazione contabile e societaria.

[75] Cfr. il Censimento permanente ISTAT sulle istituzioni *non profit* già richiamato alla nota 25.

[76] Su 73.808 istituzioni che dichiarano di non fare uso di tecnologie digitali, tralasciando una corposa parte che non le ritiene rilevanti per lo svolgimento delle proprie attività (circa il 29,8%), il 12,5% degli enti, infatti, ritiene di non avere personale dotato di capacità in questo senso e il 15,9% giustifica la mancata adozione delle tecnologie con la scarsa cultura digitale.

[77] I dati statistici sul punto – relativi all'annualità 2024 – sono stati pubblicati dall'ISTAT all'interno del *report* «*Imprese e ICT – Anno 2024*» (reperibile sul sito istituzionale *www.istat.it*) solo dopo (precisamente in data 17 gennaio 2025) la discussione pubblica del presente *paper* nell'ambito del *Workshop*.

[78] Secondo il *report* citato alla nota precedente (cfr. p. 3) e la *Tavola* n. *9a* allo stesso allegata, le tecnologie di I.A. di utilizzo più comune sono quelle che consentono l'estrazione di conoscenza e informazione da documenti di testo (*text mining*), i convertitori della lingua parlata in formati leggibili da dispositivi informatici attraverso tecnologie di riconoscimento vocale e l'intelligenza artificiale generativa di linguaggio scritto o parlato. L'aspetto interessante è che mentre le grandi imprese che utilizzano I.A., nel 51,6% dei casi sfruttano l'analisi dei dati attraverso l'apprendimento automatico (*machine learning*, *deep learning*, reti neurali) e nel 60,8% utilizzano l'I.A. per la procedura di *text mining*, tali percentuali si riducono drasticamente nelle imprese più piccole, soprattutto con riguardo al primo aspetto (ad esempio, solo il 37,6% delle imprese fino a 249 addetti che fanno ricorso ad I.A. utilizzano *machine learning*, *deep learning* o reti neurali).

[79] Cfr., sul punto, la *Tavola* n. *6*, allegata al *report*.

zabili – quantomeno su un piano teorico – gli sforzi istituzionali che, partendo innanzitutto dalla formazione dei dipendenti, intendono stimolare la transizione digitale degli enti *non profit* e quella delle P.M.I.[80]. In questo senso, deve accogliersi favorevolmente la creazione di un *Fondo per la Repubblica Digitale*[81], il cui soggetto attuatore è una s.r.l.-impresa sociale[82], che si occupa della pubblicazione di bandi aventi ad oggetto il finanziamento di progetti rivolti alla formazione e all'inclusione digitale. Una semplice ricerca sul sito internet dedicato permette di verificare come la maggior parte degli stanziamenti sia destinata proprio a P.M.I., soggetti pubblici o enti facenti parte del cd. privato «sociale» e sia essenzialmente finalizzata ad un miglioramento della preparazione tecnica della categoria di *stakeholders* rappresentata dai lavoratori. Tra le iniziative intraprese si segnalano, ad esempio, il bando denominato *CrescerAI*[83], destinato alle piccole e medie imprese[84], incluse quelle dotate della qualifica di cui al d.lgs. 112/2017, nonché quello intitolato *Digitale Sociale*, il cui dichiarato obiettivo consiste, per l'appunto, nel «sostenere progetti rivolti all'*empowerment* di conoscenze e competenze digitali di dipendenti, collaboratori stabili e volontari ("beneficiari") degli enti che operano in uno o più settori di interesse generale dell'economia sociale»[85].

Esaminando da una prospettiva più propriamente giuridica gli eventuali riflessi dell'implementazione di una cultura digitale nell'ambito dell'impresa sociale, è plausibile immaginare che la stessa possa, ad esempio, incidere positivamente

---

[80] La transizione digitale è, peraltro, una delle condizioni fondamentali individuate dal P.N.R.R. per ridurre il gap di competitività tra le P.M.I. e le grandi realtà multinazionali.

[81] Il Fondo è stato istituito nell'ambito delle politiche legate alla realizzazione del P.N.R.R. ai sensi dell'art. 29, d.l. 6 novembre 2021, n. 152, convertito con modificazioni dalla l. 29 dicembre 2021, n. 233.

[82] Interamente partecipata dall'Acri, ossia l'associazione di categoria delle fondazioni bancarie.

[83] Il bando, peraltro, gode del sostegno economico di *Google.org* – ente filantropico collegato all'omonima multinazionale – che ha costituito un nuovo Fondo volto a sostenere le organizzazioni *non profit* in Europa nello sviluppo di soluzioni basate sull'Intelligenza Artificiale che abbiano un impatto positivo sull'ecosistema imprenditoriale.

[84] I 4 progetti selezionati all'esito della valutazione sono indicati nel comunicato stampa del *Fondo per la Repubblica Digitale* del 3 ottobre 2024.

[85] Secondo quanto previsto dal bando, gli interventi potranno limitarsi, ad esempio, alla formazione digitale, di base e/o avanzata, per dipendenti, collaboratori stabili e volontari (lett. *a*), ma spingersi anche all'implementazione di una soluzione digitale volta al miglioramento dell'efficienza interna (organizzazione e processi interni) e/o esterna (servizi offerti alla collettività) (lett. *c*).

sulle modalità di gestione della rendicontazione[86], sia economico-finanziaria che sociale, di cui all'art. 9, d.lgs. 112/2017[87]. Infatti, la presenza di addetti che siano in grado di utilizzare proficuamente sistemi digitali idonei ad analizzare e catalogare un'enorme mole di dati in brevissimo tempo permetterebbe di assolvere in maniera più efficiente agli obblighi di legge ed evitare, al contempo, di ricorrere all'*outsourcing* delle relative funzioni, riducendo, così, gli oneri per lo svolgimento di tale attività[88]. Inoltre, non è escluso che la formazione o l'assunzione di personale *tech-friendly* possa gradualmente assurgere a parametro di valutazione dell'adeguatezza di quegli assetti organizzativi che ogni imprenditore operante in forma societaria o collettiva ha l'obbligo di istituire – tanto in un'ottica fisiologica[89] quanto ai fini di una tempestiva rilevazione della crisi[90] – ai sensi dell'art. 2086, comma 2, c.c.[91]. In questo senso, infatti, essenzialmente con riguardo alle

[86] In termini generali, sulla relazione tra intelligenza artificiale e operazioni di rendicontazione si vedano le considerazioni espresse nel recente saggio di C. Sertoli, *Intelligenza artificiale* versus *rendicontazione*, in *Dir. comm. dig.*, 2024, pp. 311 ss.

[87] L'impresa sociale, infatti, oltre alla tenuta del libro giornale e del libro degli inventari e alla redazione del bilancio di esercizio nel rispetto delle norme sulle s.p.a., in quanto compatibili, deve depositare presso il registro delle imprese e pubblicare nel proprio sito internet il bilancio sociale, in cui si deve tener conto «tra gli altri elementi, della natura dell'attività esercitata e delle dimensioni dell'impresa sociale, anche ai fini della valutazione dell'impatto sociale delle attività svolte» (cfr. art. 9, comma 2, d.lgs. 112/2017): tale ultimo documento, ai fini della cui redazione sono state predisposte apposite linee guida ministeriali con decreto del Ministero del Lavoro e delle Politiche Sociali del 4 luglio 2019, reperibile sul sito istituzionale *www.lavoro.gov.it*, deve, peraltro, fare menzione, ai sensi dell'art. 11, comma 3, d.lgs. 112/2017, anche delle forme e modalità di coinvolgimento degli *stakeholders*.

[88] Cfr. C. Sertoli, *Intelligenza*, cit., p. 316.

[89] Sulla circostanza che l'onere di istituire assetti adeguati non sia destinato a trovare applicazione solo «in funzione della rilevazione tempestiva della crisi dell'impresa e della perdita della continuità aziendale», ma anche nel momento di avvio, crescita e sviluppo fisiologico dell'impresa, cfr. P. Benazzo, *Il Codice della crisi di impresa e l'organizzazione dell'imprenditore ai fini dell'allerta: diritto societario della crisi o crisi del diritto societario?*, in *Riv. soc.*, 2019, p. 275.

[90] In tale ottica patologica, è, allora, utile ricordare che, ad eccezione degli enti religiosi civilmente riconosciuti, le imprese sociali, in caso di insolvenza, sono assoggettate alla liquidazione coatta amministrativa ai sensi dell'art. 14, d.lgs. 112/2017: sulle prospettive applicative dell'intelligenza artificiale nell'ambito della procedura *de qua* – pur se esaminate riferendosi al settore bancario – si vedano le recenti considerazioni di A. Blandini – M. Gigliotti, Fintech *e innovazione digitale, prospettive applicative nella liquidazione coatta amministrativa*, in *Banca, borsa, tit. cred.*, 2024, I, pp. 710 ss.

[91] Che l'obbligo in questione sia assurto a paradigma comune a tutte le imprese

imprese sociali a carattere più innovativo, la scelta di ricorrere a personale specializzato nell'uso di sistemi ad alto tasso tecnologico potrebbe contribuire all'adempimento del suddetto dovere, soprattutto qualora non s'interpreti lo stesso come circoscritto ad una mera operazione di «procedimentalizzazione», ma lo si consideri esteso anche alla corretta gestione delle risorse umane e intellettuali destinate allo svolgimento dell'attività economica[92].

6. *Conclusioni*

Si è ben consapevoli che le considerazioni qui sviluppate rappresentano degli spunti che, per quanto suggestivi, possono apparire, allo stato attuale e, pur in un contesto socio-economico in continua evoluzione, non lontani dalla mera provocazione, vista la loro difficile realizzabilità pratica, quantomeno nel breve periodo. Ovviamente, solo il decorso del tempo consentirà di verificare l'*an* e il *quomodo* dell'effettiva diffusione di sistemi di intelligenza artificiale – che dovrà, comunque, essere logicamente preceduta dall'implementazione dei ben più banali strumenti di IT, talvolta ancora non presenti in molti assetti organizzativi – nell'ambito del Terzo Settore[93]. Tuttavia, alla base delle riflessioni qui riportate si pone la convinzione che, al netto di disponibilità finanziarie evidentemente inferiori a quelle delle società lucrative[94], anche gli enti *non profit* e, in particolar

– quantomeno a carattere collettivo – è affermazione ormai condivisa in dottrina: sul punto si veda, *ex multis*, S. Ambrosini, *Assetti adeguati e "ibridazione" del modello s.r.l. nel quadro normativo riformato*, in Aa.Vv., *La società a responsabilità limitata: un modello transtipico alla prova del Codice della Crisi. Studi in onore di Oreste Cagnasso*, a cura di M. Irrera, Torino, 2020, p. 434.

[92] In questo senso si esprime, in termini assolutamente condivisibili, G. Scognamiglio, *Genesi e fondamento dell'art. 2086, comma 2, c.c.*, in Aa.Vv., *Gli assetti organizzativi dell'impresa*, Quaderno n. 18 – Scuola superiore della magistratura, Roma, 2022, p. 71.

[93] Molto dipenderà anche dalla forma giuridica adottata dalle «nuove» imprese sociali, considerato che, come si è detto, l'obbligo di coinvolgimento degli *stakeholders* di cui all'art. 11, d.lgs. 112/2017, non opera con riguardo alle cooperative sociali: in proposito, si segnala, però, che, benché queste ultime rappresentino ancora oggi la maggioranza degli enti di cui al d.lgs. 112/2017, il *Rapporto 2024 sul Registro Unico Nazionale Del Terzo Settore* presentato da *Unioncamere* nel maggio 2024 e pubblicato sul sito *www.unioncamere.gov.it*, ha confermato la rilevante crescita del numero delle società di capitali, delle associazioni e delle fondazioni che acquisiscono la qualifica di impresa sociale, come, peraltro, era già stato puntualmente segnalato da L. Bobba e C. Gagliardi, *Le "nuove" imprese sociali*, in Aa.Vv., *Le "nuove" imprese*, cit., pp. 75 ss.

[94] E, infatti, sempre secondo i dati di cui alla *Tavola* n. 21 allegata al censimento sullo stato della digitalizzazione delle istituzioni *non profit* (cfr. nota 25), sono ben 19.482

modo, le imprese sociali[95], che esercitano stabilmente un'attività di natura economica, possano trarre notevole giovamento dall'impiego di mezzi tecnologicamente avanzati, come dimostrato – seppur in maniera ancora embrionale – anche dall'ormai riconosciuta facoltà di svolgere in modalità telematica le riunioni degli organi sociali degli E.T.S., sia quando si tratti dell'assemblea[96], sia quando ineriscano al consiglio di amministrazione[97].

gli enti che non fanno uso di mezzi tecnologici per mancanza di risorse finanziarie.

[95] Il cambio di passo da un punto di vista culturale dovrebbe partire proprio dalla consapevolezza – ad oggi assente se si considera che, secondo il censimento ISTAT, più di 20.000 enti non utilizzano tecnologie digitali in quanto le ritengono irrilevanti per la propria attività (cfr. *Tavola* n. 21, di cui alla nota precedente) – che lo sviluppo di mezzi sempre più evoluti in questo campo potrebbe, invece, favorire una maggiore efficacia dei progetti a carattere sociale.

[96] Non è un caso, d'altronde, che l'art. 4, comma 1, lett. *d*), l. 4 luglio 2024, n. 104, abbia modificato l'art. 24, comma 4, d.lgs. 117/2017, ammettendo definitivamente, salvo divieto espresso contenuto nell'atto costitutivo o nello statuto, che anche negli E.T.S. a base associativa si possa intervenire in assemblea mediante mezzi di telecomunicazione ed esprimere il voto per via elettronica, «purché sia possibile verificare l'identità dell'associato che partecipa e vota e nel rispetto dei princìpi di buona fede e di parità di trattamento».

[97] In questo senso cfr. *Massima* del 10 maggio 2022, n. 13, Cons. Not. Milano.

Intelligenza artificiale e mercato: il consumatore digitale

di **Ludovica Serreli**

1. *Introduzione. L'ecosistema digitale*

L'evoluzione dell'attuale contesto economico e sociale ha determinato l'incremento dell'impatto dell'economia digitale – oramai *data driven* – sull'offerta di beni e servizi, oggi personalizzata attraverso lo sfruttamento dei dati, il cui valore economico quasi porta ad assimilare giuridicamente il loro scambio alla fornitura di servizi[1].

È richiesto, evidentemente, di prestare attenzione all'intelligenza artificiale[2], strumento che si nutre di dati e attraverso il quale vengono esplorate le modalità

[1] In merito, si v. la Dir. (UE) 2019/2161 del Parlamento Europeo e del Consiglio, nell'ambito della quale il legislatore europeo – dopo aver evidenziato come i contenuti digitali e i servizi digitali sono spesso forniti online nell'ambito di contratti che non prevedono il pagamento di un prezzo da parte del consumatore, bensì la cessione dei propri dati personali al professionista (Cons. 31) e che, pertanto, dovrebbe essere esteso l'ambito di applicazione della direttiva 2011/83 «per contemplare anche i contratti nel cui ambito il professionista fornisce o si impegna a fornire un servizio digitale al consumatore, e il consumatore comunica o si impegna a comunicare dati personali» (Cons. 33) – ha modificato la Dir. 2011/83/UE definendo il contratto di servizi «qualsiasi contratto in base al quale il professionista fornisce o si impegna a fornire un servizio, compreso un servizio digitale, al consumatore» (art. 4).

[2] P. Mccorduck, *Machines Who Think*, Natick, MA, 2004, sostiene che l'intelligenza artificiale ha radici piuttosto antiche e, in particolare, che è nata con il desiderio di «*forge the gods*»; idea, questa, che nel corso dei secoli è stato pensata e attuata

di realizzazione di macchine e programmi informatici in grado di risolvere situazioni e imparare dall'esperienza, anche per svolgere compiti tradizionalmente svolti da esseri umani[3].

L'avvento dei nuovi apparati informatici, che ha investito una molteplicità di settori produttivi e di consumo, ha posto le basi per la commistione delle tecnologie digitali con i mercati dell'informazione e della comunicazione, c.d. *information technology* (*IT*). Il che giustifica l'attenzione oggi riservata alla digitalizzazione delle informazioni e allo sviluppo di processi decisionali basati sull'utilizzo di algoritmi[4], i quali impongono di ripensare al rapporto tra il diritto e l'applicazione tecnico-pratica delle nuove tecnologie[5].

Nel contesto indicato, può certamente dirsi che il motore della trasformazione digitale è la disponibilità massiva di dati (c.d. *big data*)[6] ed informazioni, dai quali viene estratto valore attraverso l'impiego degli algoritmi utilizzati da macchine sempre più "intelligenti".

---

in molteplici forme, anche solo narrative. Tuttavia, fu solo a partire dagli anni '40 del secolo scorso che si concretizzò l'intento – proveniente da studiosi di differenti ambiti scientifici – di progettare un oggetto che elaborasse i dati, in qualche modo "pensante". In merito alla possibilità di costruire un "cervello artificiale", si v., tra tutti, A. Turing, *Computing Machinery and Intelligence*, in *Mind*, LIX, 236, 1950, pp. 433 ss.

[3] G. Comandé, *Intelligenza artificiale e responsabilità tra* liability *e* accountability. *Il carattere trasformativo dell'IA e il problema della responsabilità*, in *An. giur. ec.*, 2019, p. 169.

[4] Volendo utilizzare l'espressione di H. Fry, *Hello World*, Torino, 2019, p. 18, l'algoritmo è «una serie di istruzioni logiche che spiegano, un passo dopo l'altro, come portare a termine un'attività». Sul funzionamento degli algoritmi v. H.S. Stone, *Introduction to Computer Organization and Data Structures*, New York, 1971, *passim*; D. Harel, Y. Feldman, *Algoritmi: Lo spirito dell'informatica*, Milano, 2008, *passim*; P. Domingo, *L'algoritmo definitivo: La macchina che impara da sola e il futuro del nostro mondo*, Torino, 2016, *passim*; E. Finn, *Che cosa vogliono gli algoritmi. L'immaginazione nell'era dei computer*, Torino, 2018, *passim*; B. Romano, *Algoritmi al potere*, Torino, 2018, *passim*; A. Nuzzo, *Algoritmi e regole*, in *An. giur. ec.*, 2019, pp. 39 ss.

[5] Del resto, già N. Irti, *Scambi senza accordo*, in *Riv. trim. dir. proc. civ.*, 1998, p. 364, aveva osservato come «la storia del contratto non può separarsi dalla *storia delle tecnologie*, mediante le quali si determinano i rapporti di scambio».

[6] In argomento, *ex multis*, cfr. V. Mayer-Schönberger, K. Cukier, *Big Data. A Revolution that will Transform How We Think, Work, and Think*, New York, 2014, *passim*; D.E. Holmes, *Big Data. A Very Short Introduction,* Oxford, 2014; S. Borocas, A. Selbst, *Big Data's Disparate Impact*, in *California L. Rev.*, 2016, 3; V. Falce, G. Ghidini, G. Olivieri, *Informazione e Big Data tra innovazione e concorrenza*, in *Quaderni Romani Dir. Comm.*, 2018, *passim*. V. anche AGCom, *Big data, interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 2017/17/CONS*, 2018.

L'obiettivo di questa indagine è valutare l'impatto – in particolare sul mercato del consumo di servizi finanziari – dell'uso di questi algoritmi. Quanto ai sistemi di c.d. *machine learning*, si può anticipare come essi abbiano sortito incredibili effetti sull'economia e sulla finanza, e che le *fintech companies*, attraverso sistemi c.d. disintermediati, hanno rapidamente conquistato una grossa fetta di mercato. Si pensi agli *advisors* computerizzati: consulenti finanziari digitali, o piattaforme *online* per la valutazione dei rischi o la gestione del portafoglio di investimenti; o, ancora, sistemi di *trading* automatizzato che, attraverso la rapida analisi di enormi quantità di dati, sono in grado di effettuare in maniera automatica acquisti e vendite di azioni e titoli; nonché per la valutazione circa l'affidabilità creditizia delle società e delle persone fisiche.

Da una prospettiva complementare, nel contesto evolutivo delle dinamiche competitive dei nuovi mercati del digitale, la disponibilità dei *big data* e la capacità di raccolta ed elaborazione degli stessi, rappresentano un'occasione di acquisto di potere di mercato e un significativo vantaggio competitivo per quelle imprese dotate di piattaforme digitali in grado di gestire e sfruttare economicamente ingenti quantità di dati; il che solleva preoccupazioni di natura concorrenziale, soprattutto in rapporto al potere acquisito dai c.d. *tech-giants*[7]. Si fa riferimento, in particolare, a quelle condotte finalizzate alla "monopolizzazione dei dati", che inducono appunto a questionare l'idoneità dei tradizionali strumenti *antitrust*.

L'avvento di questa nuova «tecnocrazia digitale»[8] impone di ricercare un approccio che tenga in considerazione come la velocità e l'impatto dello sviluppo degli algoritmi facciano spesso sì che, nel contesto della economia digitale, sia difficoltoso trovare il corretto bilanciamento tra interessi confliggenti in tema di concorrenza, protezione del consumatore e della *privacy*, ma anche di tutela di altri diritti fondamentali e della democrazia[9].

---

[7] Emblematico, in tal senso, il caso dell'Autorità Antitrust tedesca che, nel 2019, ha imposto considerevoli restrizioni a Facebook a causa delle modalità di profilazione degli utenti. In particolare, l'Autorità aveva rilevato come Facebook ponesse in atto strategie riconducibili all'abuso di posizione dominante, consistenti nella costituzione di profili dettagliati degli utenti tramite i dati raccolti attraverso tutte le piattaforme del Gruppo (ora Meta Platforms, Inc.).

[8] Per usare le parole di G. Sciascia, *Reputazione e potere: il social scoring tra distopia e realtà*, in *Giornale dir. amm.*, 2021, p. 318.

[9] Sottolinea D. Mastrelia, *Gestione dei* bigdata *in una prospettiva orientata alla tutela della privacy degli individui*, in *Dir. ind.*, 2018, pp. 364 s., «Sebbene le preoccupazioni sulla riservatezza degli individui sono sembrate logiche, dall'altro le logiche di mercato – ed in particolare di quelle legate ai mercati dell'economia digitale – non possono non considerare che l'uso dei *bigdata* è un fattore chiave per le imprese che operano nei settori dell'economia digitale».

Dall'analisi del tema emergerà che lo studio e l'utilizzo degli strumenti di intelligenza artificiale – l'evoluzione dei quali si interseca con i rapporti tra poteri economici, nuove tecnologie e libertà – comporta sfide etiche, prima ancora che tecniche e giuridiche[10].

2. Big data *e i meccanismi di* machine learning

Con il termine "*big data*" si intende l'accumulo sistematico di enormi quantità di dati (in termini di volume, formato e varietà) all'interno di computer dotati di straordinarie capacità di memoria e calcolo. Il tema è diventato di grande attualità sia nel dibattito scientifico che in quello sociale, soprattutto in ragione degli incredibili progressi tecnologici occorsi negli ultimi anni sul versante delle telecomunicazioni, degli strumenti digitali "portatili" quali gli *smartphones*, dei sistemi di conservazione dei dati (*cloud*), nonché della creazione di computer con sempre più elevate capacità di conservazione dei dati e di calcolo.

L'accessibilità delle informazioni digitali, unite allo sviluppo di algoritmi sempre più complessi e autonomizzati – in grado di elaborare i dati raccolti attraverso le tecniche di *data mining*[11] e di profilare i gusti, le attitudini e le intenzioni future delle persone – ha reso urgente la regolamentazione in materia di intelligenza artificiale[12], culminata con l'entrata in vigore del c.d. *AI Act* il 1° agosto 2024.

---

[10] Sulla necessarietà di elaborare un quadro etico-giuridico, cfr. P. Lin, K. Abney, G. Beckey, *Robot Ethics: Mapping the Issues for a Mechanized World*, in *Artificial Intelligence*, 175, 2011, pp. 945 s.; M. Brundage, *Limitation and Risks of Machine Ethics*, in *J. Experimental Theoretical Artificial Intelligence*, 26, 2014, pp. 355 ss.; D. Roque Vitolo, *Insolvenza e Intelligenza Artificiale*, in *Ristr. aziendali*, 2022; S. Pesucci, *Critica etica al sistema di credit scoring automatizzato*, *ivi*, 2024.

[11] «I *big data* sono la materia prima dell'universo digitale, una sorta di petrolio dell'economia della conoscenza che ha valore solo se estratto e raffinato», così M. Magnani, *Fatti non foste a viver come robot*, Milano, 2020, p. 65.

[12] Necessità posta in luce sia in ambito comunitario che, a livello interno, dalle Autorità Amministrative Indipendenti (segnatamente, dal Garante Privacy, quello della Concorrenza e dall'AGCom), nonché dalla Banca d'Italia e dalla CONSOB. Per quanto attiene alle politiche UE, già nel 2010 era stata avviata una prima fase di regolamentazione attraverso l'*Agenda Digitale*, seguita, nel 2015, dalla *Strategia per il Mercato Unico Digitale*. Si v. anche il *Regolamento Generale sulla Protezione dei Dati*, entrato in vigore nel 2018; la Comunicazione della Commissione "*L'intelligenza artificiale per l'Europa*", adottata il 25 aprile 2018; e, infine, il *Codice Europeo delle Comunicazioni Elettroniche*, nell'ambito del quale, tra le altre cose, si è dato atto che lo scambio di servizi digitali avviene non solo attraverso denaro, ma anche con la cessione dei dati personali (v. Considerando n. 16). Con specifico riferimento ai *Big Data*, l'UE ha per la prima volta disciplinato la materia attraverso la Comunicazione della Commissione "*Verso una florida economia basata sui*

Sul versante economico e sociale, la rete internet ha assunto un ruolo cruciale attraverso la progressiva (e massiva) espansione delle attività economiche in rete grazie all'*e-commerce* e alla promozione di beni e servizi tramite *social network*[13].

L'intelligenza artificiale è peraltro in grado di imparare con l'esperienza e si sviluppa attraverso l'utilizzo dei dati forniti – consapevolmente o no – dagli utenti delle piattaforme. C'è da domandarsi, dunque, se tale circostanza non appaia confliggente, da una parte, con la tutela della vita privata e, in generale, alla riservatezza di cui all'art. 7 della Carta dei diritti fondamentali dell'Unione Europea; e, dall'altra, con il diritto della persona fisica al controllo delle informazioni che la riguardano (art. 8 della Carta). Emerge così una doppia problematica, afferente sia alla presenza di una realtà digitale che archivia tutto e, perciò, non dimentica; sia alla fruibilità, per il soggetto che ne faccia richiesta, delle informazioni raccolte e organizzate dagli algoritmi.

Ed infatti, è stato opportunamente osservato come la questione abbia evidentemente posto il legislatore e le autorità di regolazione di fronte a problematiche in parte nuove, cui elemento determinante «è costituito dal crescente utilizzo *dinamico* dei dati e dall'effetto di "retroazione" che esso può determinare sul titolare, nel momento in cui quei dati costituiscono il presupposto per assumere provvedimenti nei suoi confronti e/o influenzarne le scelte»[14].

Vi è poi quella branca di *AI* costituita dai meccanismi di c.d. *machine learning*. Essi, quasi prepotentemente, hanno iniziato a interagire con l'essere umano grazie a due fondamentali fattori: un'enorme disponibilità di dati e *computer* sempre più

---

dati" (2014), nella quale era stata proposta una politica che mirasse alla costituzione di un'economia basata sui dati, con il suggerimento di alcune proposte di intervento. In successiva Comunicazione ("*Costruire un'economia dei dati europea*", 10 gennaio 2017), la Commissione ha proposto concrete soluzioni al fine di costituire – come esplicitato già nel titolo – un'economia dei dati UE, nell'ambito della strategia di realizzazione del mercato unico digitale. Nella stessa data è stata altresì adottata la Comunicazione intitolata "*Scambio e protezione dei dati personali in un mondo globalizzato*", la cui attenzione si focalizza, da una parte, a garantire e facilitare il commercio internazionale dei dati e, dall'altra, a tutelare la *privacy* degli individui.

[13] Stando al rapporto dell'AGCom del 2017 – relativo alla fase preliminare dell'indagine conoscitiva sui Big Data svolta, congiuntamente, dall'Agenzia Garante delle Comunicazioni, con l'AGCM e il Garante per la Protezione dei Dati Personali – per le imprese che utilizzano i *Big Data* al fine di ampliare la loro influenza sul mercato, «le piattaforme *online* assumono quindi un connotato tecnico di «piattaforma» nel senso della teoria dei mercati a più versanti, ossia di un intermediario tra agenti economici che si situano in ambito di mercato distinti e che «comunicano» attraverso la loro presenza» (p. 22).

[14] A. Punzi, *Il diritto e i nuovi orizzonti dell'intelligenza umana*, in *An. giur. ec.*, 2019, p. 22.

potenti e capaci di elaborare massivamente e velocemente grandissime quantità di informazioni digitali[15]. Gli strumenti informatici dotati di tale abilità si comportano in modo diverso rispetto agli algoritmi tradizionali. Essi si avvalgono infatti di un codice progettato al fine di creare un sistema automatico che è in grado, appunto, di imparare, per poi creare lo schema dello scenario che deve risolvere[16].

Il problema di simili sistemi è che, così come per un cervello umano, non si può schiudere la macchina per comprendere i percorsi che hanno condotto a una certa decisione[17]: essi sono spesso complicati da spiegare e poco trasparenti, perché non è dato conoscere come il computer decida l'importanza di una o più variabili; motivo per il quale si suole definire questo strumento una "*black box*"[18].

Peraltro, gli algoritmi di *machine learning* utilizzano, inevitabilmente, dati storici; circostanza che sovente porta al consolidamento di discriminazioni e pregiudizi tipici dell'essere umano (il quale, d'altronde, è il creatore della macchina e *ivi* trasferisce, sebbene involontariamente, le proprie idee e i propri pre-concetti). Tale circostanza, unita a rischi insiti nell'uso dei *big data* quali la discriminazione di prezzo[19], porta alla penalizzazione di alcune fasce di popolazione (*seu*, delle minoranze).

3. *Sviamento del processo cognitivo dell'utente digitale e personalizzazione dell'offerta commerciale al consumatore*

Ciò premesso, è appena il caso di domandarsi se ancora esistano individui in grado di orientarsi in modo *libero* nell'attuale realtà socio-economica. Il quesito

---

[15] Ad ogni modo, si tenga a mente che la tassonomia infrastrutturale del mondo digitale è molto ampia e non necessariamente contempla algoritmi di *machine learning*; in argomento, cfr. A. Perrucci, *Dai Big Data all'ecosistema digitale. Dinamiche tecnologiche e di mercato e ruolo delle politiche pubbliche,* in *An. giur. ec.*, 2019, p. 67.

[16] In argomento, si v. G. Comandé, *Intelligenza artificiale e responsabilità,* cit., p. 172: «Un profilo particolarmente problematico di IA è rappresentato da quei programmi che strutturalmente sono diretti ad adattarsi continuamente anche dopo la loro immissione in uso/circolazione in risposta ai nuovi dati che ricevono e generano. Essi integrano questi dati nei loro processi di analisi dei modelli esistenti per rivederli e svilupparne di nuovi, consentendo all'IA di eseguire in modo più efficiente ed efficace il suo compito».

[17] G. F. Italiano, *Le sfide interdisciplinari dell'intelligenza artificiale*, in *An. giur. ec.*, 2019, p. 13.

[18] Cfr. F. Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Cambridge, 2015.

[19] Si v., per tutti, M. Maggiolino, *Big data e prezzi personalizzati*, in *Conc. merc.*, 2016, pp. 95 ss.

pare sensato, considerato che gli strumenti digitali inviano, spesso aggressivamente, segnali e sollecitazioni agli utenti, che si comportano "di riflesso". I meccanismi di ragionamento e assunzione di decisioni dei consumatori sembrano, allo stato, «dare torto a Cartesio e al suo modello di un soggetto che prima acquista certezza di sé e poi si rapporta ad un mondo-oggetto esterno»[20].

Nell'epoca del consumismo[21], l'atto dell'acquisto non può più essere considerato nei soli aspetti economici; bisognerebbe tener conto dei progressi negli studi psicologici (e sociologici)[22], nell'economia comportamentale e nel *neuromarketing* al fine di interpretare nel modo corretto, *in primis*, la condotta ingannevole di cui all'art. 21 c. cons. e, segnatamente, l'idoneità della stessa ad indurre in errore il consumatore[23]. Soprattutto ove si considera che attraverso le tecnologie digitali, ogni volta che navighiamo su internet forniamo alla rete moltissimi dati inerenti ai nostri interessi e alle nostre abitudini e che tali informazioni vengono memorizzate e riutilizzate per guidare le nostre ricerche future. Gli algoritmi sono infatti in grado di anticipare e suggerire quali prodotti e servizi specifici sarà disposto ad acquistare il singolo consumatore, anche prima che egli gli scelga e, talvolta, prima ancora che si renda conto di avere bisogno[24].

---

[20] A. Punzi, *Il diritto e i nuovi orizzonti dell'intelligenza umana*, cit., 2019, p. 27.

[21] In argomento, cfr. E. Fromm, *Avere o essere?*, Milano, 2001, *passim*; Z. Baumann, *Homo consumens. Lo sciame inquieto dei consumatori e la miseria degli esclusi*, Trento, 2007; Id., *L'etica in un mondo di consumatori*, Bari, 2010; J. Baudrillard, *La società dei consumi. I suoi miti, le sue strutture*, Bologna, 2010.

[22] Ad esempio, «il prodotto può divenire un mezzo per il soddisfacimento di desideri (ad es. il desiderio sessuale, di potere sociale, o altre forme di narcisismo), che nulla hanno a che vedere con la sua funzione materiale, e che vengono simbolicamente associati ad esso attraverso il meccanismo psicologico della "proiezione". Tra i vari esempi, una strategia molto diffusa in ambito pubblicitario consiste nel presentare una minaccia futura, attraverso la creazione di un bisogno presente, e facendo leva su pulsioni negative, come l'ansia e la paura», così A.P. Seminara, *Libertà del consumatore e psicologia della pubblicità*, in *Contr. e impr.*, 2020, p. 498.

[23] Come ben si rileva *ibidem*, pp. 515 s., «Per capire la portata del fenomeno, sembra opportuno ricordare come lo sfruttamento, da parte del *neuromarketing*, delle attuali tecnologie permette oggi di testare le pubblicità su campioni di consumatori, verificando quando, e quanto intensamente, si attivino quelle zone cerebrali deputate alla stimolazione emotiva. In tal modo, una pubblicità si considera "ben riuscita" da un punto di vista sentimentale quando è in grado di emozionare più intensamente il destinatario, questo essendo l'unico criterio di giudizio della sua reale efficacia. A nulla rilevano, invece, le informazioni del messaggio pubblicitario, spesso totalmente rimpiazzate dalla pura suggestione. Questo profilo non può non considerarsi criticamente se si tiene a mente l'idea di un consumatore che agisce liberamente, in modo "attento e avveduto".

[24] A. Sharma, *How Predictive AI Will Change Shopping*, in *Harvard Business Rev.*,

Per di più, talune pratiche pubblicitarie – ormai somministrate in formato digitale – hanno un ruolo cruciale nel fuorviare il processo cognitivo del consumatore, inducendolo in errore (per esempio sulle caratteristiche o sull'utilità del prodotto) o limitandone la libertà, coinvolgendolo in processi mentali al di fuori del piano del razionale (c.d. *cognitive illusions*). Conseguenza, questa, del fatto che nel corso del processo decisionale vengono implicati il piano del sub-conscio (che ha a che fare, ad esempio, con il condizionamento dettato da fattori di tipo socio-culturale) e, addirittura, quello dell'inconscio (il quale – operando a livello più profondo – attiene alle dinamiche dell'impulsività).

Gli operatori del mercato, certamente consapevoli dei *bias* cognitivi che affettano i consumatori, sfruttano le loro «fallacie cognitive […] per indur[li] al compimento di acquisti di cui non si soppesano adeguatamente i vantaggi e gli svantaggi»[25].

Motivo per il quale è quantomai opportuno caldeggiare la commistione tra la disciplina delle pratiche commerciali scorrette[26] e la regolamentazione della nuova realtà di digitalizzazione delle informazioni[27], da valorizzare ulteriormente mediante le risultanze degli studi condotti in psicologia, poi estesi ad altri settori scientifici (come quello economico), grazie ai quali è stato possibile individuare una serie di dinamiche idonee a incidere sul processo di *decision making*[28] e che

---

18 novembre 2016, in *https//:hbr.org*, *passim*.

[25] A.P. Seminara, *Libertà del consumatore*, cit., p. 512.

[26] Il sistema normativo è quello offerto dalla Direttiva 2005/29/CE, trapiantata a livello interno attraverso il d.lgs. n. 206 del 2005 (Codice del consumo).

[27] Il Considerando 20 del Reg. (UE) 2024/1689 sottolinea la necessità di alfabetizzazione in materia di AI, al fine ottenere dai suoi sistemi i massimi benefici, «proteggendo nel contempo i diritti fondamentali, la salute e la sicurezza» nonché il controllo democratico.

[28] Sul tema, senza pretesa di esaustività, si rimanda a R. Rumiati, N. Bonini, *Psicologia della decisione*, Bologna, 2001; P. Slovic, M. Finucane, E. Peters, D.G. MacGregor, *Rational actors or rational fools: implications of the affectheuristic for behavioral economics*, in *J. of Socio-Economics*, 31/2002, pp. 329 ss.; P. Legrenzi, *Psicologia e investimenti finanziari. Come la finanza comportamentale aiuta a capire le scelte di investimento*, Milano, 2006, *passim*; C. Camarer, *La neuroeconomia. Come le neuroscienze possono spiegare l'economia*, Milano, 2008, *passim*; B. Alemanni, G. Brighetti, C. Lucarelli, *Decisioni di investimento, assicurative e previdenziali*, Bologna, 2012, *passim*; B. Alemanni, *Finanza comportamentale*, Milano, 2015; G. Gardenal, U. Rigoni, *Finanza comportamentale e gestione del risparmio*, Torino, 2016, *passim*; G. Liace, *L'investitore irrazionale*, in *Banca, borsa, tit. cred.*, 2020, p. 971. Cfr. anche Id., *Sulle emozioni e le reazioni dell'investitore irrazionale*, in *Giur. comm.*, 2020, pp. 140 s.: «Le nostre scelte, in qualsiasi campo, mutano a seconda del contesto in cui sono assunte […] Assumere decisioni in modo razionale richiederebbe l'annullamento delle

allontanano molto la figura del consumatore dal modello di riferimento dell'agente economico perfettamente razionale proprio dell'economia neoclassica[29].

Questione intrascurabile è, allora, il richiamo dell'articolo 21 c. cons., il cui riferimento alla "presentazione" del prodotto suggerisce che l'ingannevolezza possa derivare dalle concrete modalità nelle quali viene effettuata la promozione commerciale, tenendo anche conto del contesto comunicativo[30], potenzialmente idoneo a distorcere la percezione del consumatore[31].

In questo contesto si innesta il menzionato tema dello sfruttamento dei dati personali degli utenti perché se, per un verso, «abbiamo la sensazione di avere infinite possibilità di scelta», dall'altro «questa è limitata dai suggerimenti di prodotti e servizi, di notizie e di informazioni che appaiono sulle home-page e sulle bacheche, dove i dati raccolti su di noi ci guidano a prendere decisioni»[32].

---

influenze derivanti dalle emozioni. In realtà una simile impostazione non risulta essere corretta, poiché le emozioni non solo giustificano le scelte, ma predicono le decisioni di investimento degli individui e sono strettamente connesse ai processi cognitivi. Le emozioni possono accompagnare il processo decisionale e influenzarlo nei diversi momenti in cui si sviluppa. Invero, le emozioni trasmettono al decisore dei messaggi, nel senso che le scelte che ha compiuto possono provocargli un dispiacere o una sensazione di piacere. Le esperienze emotive, pertanto, vengono immagazzinate dalla memoria e possono essere adoperate successivamente, nel momento in cui si deve affrontare un "dilemma" di tipo decisionale. Le emozioni dunque, svolgono una funzione di tipo informativo».

[29] «Il modello economico neoclassico, a lungo punto di riferimento per la quasi totalità degli studi scientifici in ambito economico e giuridico e ancora oggi considerato, da una parte della dottrina, un valido strumento di analisi delle strutture di mercato e delle istituzioni che vi operano, si fonda su tre fondamentali premesse. Il primo assunto ha ad oggetto la razionalità degli individui. Questi ultimi sono considerati illimitatamente razionali: ciò significa che agli agenti economici sono attribuite – in astratto – capacità cognitive, computazionali e di memoria illimitate. Il secondo assunto riguarda l'opportunismo degli agenti, inteso come l'assenza o irrilevanza di azioni disinteressate a favore di terzi. […] Infine, il terzo assunto riguarda la forza di volontà degli agenti economici. Anch'essa – da intendersi come la capacità degli individui di adottare strategie in contrasto con i propri interessi a breve termine – è considerata illimitata dallo stesso modello», così N. Usai, *Economia comportamentale e diritto della crisi: il ruolo della "mala gestio cognitiva" nel ritardo dell'emersione delle difficoltà dell'impresa*, in *Riv. soc.*, 2022, p. 1217.

[30] Cfr. Tar Lazio, 1° agosto 2019, n. 10193, in *Foro amm.*, 2019, 7, 1329; Cons. Stato, sez. IV, 10 dicembre 2014, n. 6050, *ivi*, 2014, 12, 3112.

[31] È comunque richiesto, ai fini dell'applicazione della disciplina in esame, che il consumatore abbia subito un pregiudizio patrimoniale.

[32] D. Columbro, *Dentro l'algoritmo. Le formule che regolano il nostro tempo*, Firenze, 2022, p. 80.

Segnatamente, per gli agenti economici che operano nel digitale è pratica comune la raccolta di tutte le informazioni riguardanti la geolocalizzazione, lo stile di vita e il sistema di valori, nonché le attitudini e i comportamenti dei consumatori, poi raggruppati in *clusters* omogenei[33].

Oltretutto alcune strategie di *marketing* prevedono la ripetizione incessante di un messaggio pubblicitario, pratica certamente aggressiva se analizzata in chiave psico-emotiva[34], e pertanto idonea a pregiudicare la capacità di "resistenza" del destinatario della comunicazione[35]. Tale approccio iterativo, seppur adottato anche in contesti risalenti nel tempo, è stato mantenuto e rinvigorito attraverso i recenti progressi nella pubblicità digitale. Ed infatti, se, tradizionalmente, l'indebito condizionamento veniva ricondotto a strategie di *marketing* quali la ripetizione assillante di un messaggio televisivo, le sollecitazioni telefoniche e le visite "porta a porta", oggi bisogna fare i conti anche con altre forme di sollecitazione

[33] In proposito, si v. altresì la nozione di targetizzazione che, secondo l'Enciclopedia Treccani, è definibile come "identificazione e scelta degli obiettivi": «Nel mondo del Digital Marketing, il concetto di targeting, o targetizzazione, riveste un ruolo cruciale. […] La targetizzazione, che si origina dall'inglese "To Target = Mirare", è un processo intermedio tra la Segmentazione della domanda di mercato e il Posizionamento. Questo processo consente di individuare i cluster target, ottimizzando le risorse di marketing e evitando dispersioni di budget. La segmentazione del mercato è il punto di partenza per ogni business. Significa dividere il mercato in settori obiettivo scientifici. […] I criteri di segmentazione includono aspetti come l'area geografica, sociodemografici […], psicografici […] e comportamentali […]. La targetizzazione è la selezione di un pubblico specifico a cui indirizzare una campagna pubblicitaria, basata sulla segmentazione precedentemente effettuata. […] Un targeting efficace si basa sull'identificazione di un gruppo di consumatori che possiede caratteristiche in linea con l'offerta proposta. […] Una buona strategia di marketing permette di personalizzare l'offerta in modo che risuoni con le specifiche esigenze e desideri del gruppo target», così in *https://manthea.ch/il-targeting-nel-marketing/*.

[34] Sugli aspetti psico-emotivi coinvolti nelle decisioni economiche, si v. J.D. Hanson, D.A. Keysar, *Taking behaviouralism seriously: some evidence of market manipulation*, in *Harvard L. Rev.*, 1999, pp. 1420 ss.; A.P. Seminara, o. c., pp. 493 e 513; R. Caterina, *Psicologia della decisione*, cit., pp. 6 e 67 ss.; M. Fusi, *Pratiche commerciali aggressive e pubblicità manipolatoria*, in *Riv. dir. ind.*, 2009, I, pp. 5 ss.; J. Trzaskowski, *Behavioural Economics, Neuroscience, and the Unfair Commercial Practice Directive*, in *J. Cons. Policy*, 2011, pp. 384 ss.; Id., *Lawful distorsion of consumer economic behaviour*, in *Eur. Business L. Rev.*, 2016, vol. 27, I, pp. 25 ss.

[35] La pratica è definibile aggressiva ove, «tenuto conto di tutte le circostanze del caso, mediante molestie, coercizione, compreso il ricorso alla forza fisica, o *indebito condizionamento*, limita o è idonea a limitare considerevolmente la libertà di scelta o di comportamento del consumatore, tanto da indurlo a prendere una decisione che altrimenti non avrebbe preso» (art. 24 c. cons.).

indesiderata, come gli *spam* o i *banner* che appaiono automaticamente nel corso della navigazione in rete.

Le pratiche in questione sono, oltre che potenzialmente aggressive fisicamente (nel senso che vengono imposte ai nostri sensi), idonee a falsare la percezione del consumatore. Circostanza alla quale bisogna sommare il fatto che, attraverso lo sfruttamento dei *big data* (come la raccolta di informazioni durante dell'utilizzo delle *app* sullo *smartphone*, dei *social network* o l'accettazione dei *cookies* in qualsiasi sito web) la pubblicità viene personalizzata e aumenta, così, la probabilità che l'utente-consumatore agisca in risposta a un indebito condizionamento o, addirittura, a manipolazione.

Nello scenario descritto, pare chiaro che il volgere l'attenzione verso un dato oggetto è azione tutt'altro che volontaria, e tantomeno spontanea, soprattutto nel caso in cui venga fatto uso dei dati degli utenti dei servizi digitali in modalità «computazionale automatizzata»[36].

Per ricapitolare, le azioni e le interazioni dell'utente lasciano "tracce", che abbandonano il loro proprietario e si disperdono nel mondo digitale[37]. Esse vengono poi raccolte da sistemi di *marketing* che le elaborano per creare il profilo della nostra personalità, dei nostri gusti e delle nostre propensioni, formulando

---

[36] Cfr. il Considerando 8 della Dir. (UE) n. 2019/790, nonché il Considerando 29 del Reg. (UE) 2024/1689, ai sensi del quale «Le tecniche di manipolazione basate sull'AI 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 libera scelta. L'immissione sul mercato, la messa in servizio o l'uso di determinati sistemi di IA con l'obiettivo o l'effetto di distorcere materialmente il comportamento umano, con il rischio di causare danni significativi […] sulla salute fisica, psicologica o *sugli interessi finanziari* sono particolarmente pericolosi e dovrebbero pertanto essere vietati».

[37] Circostanza, questa, che involve una serie di problematiche, tra le quali riveste particolare importanza quella del c.d. *right to be forgotten* (diritto all'oblio). Emblematica, in tal senso, la vicenda «*Google Spain*» sulla necessarietà del bilanciamento tra il diritto all'identità (e, nel caso di specie, alla sua corretta rappresentazione) e il diritto di cronaca. Il caso, come noto, aveva coinvolto il signor Mario Costeja Gonzales, il quale si era accorto che, digitando il proprio nome sui principali motori di ricerca, compariva primariamente il *link* di una notizia relativa a un fatto piuttosto risalente; notizia che era stata pubblicata da *La Vanguardia* ed era ancora presente nell'archivio telematico della testata. Costeja aveva sostenuto che il collegamento tra la sua persona e la notizia era tale da non rappresentare correttamente la propria identità attuale. La Corte di Giustizia UE, avvalorando questa tesi, aveva disposto la deindicizzazione del *link* collegato al suo nome. In argomento, si v. Z. Zencovich (a cura di), *Il diritto all'oblio dopo la sentenza Google Spain*, Roma, 2015; C. Fusco, *Dalla sentenza «Google Spain» al Regolamento 2016/679, passando per la Carta dei diritti fondamentali di internet: l'itinerario del diritto all'oblio lungo i sentieri del web*, in *ratioiuris.it*, 2016.

anche ipotesi sulle nostre future condotte e inviando – quasi per confermare la congettura elaborata – informazioni e notizie modellate sui nostri orientamenti personali (*behavioural advertising*). In linea generale si può affermare che la pubblicità non si effettua più tramite il mero incitamento all'acquisto, bensì attraverso il costante invio di segnali personalizzati che sollecitano l'agire di riflesso del consumatore. Si fa leva, in sostanza, sul carattere emotivo della comunicazione commerciale[38].

Guardando più da vicino l'impatto delle tecnologie dell'informazione, è evidente che esse rechino la possibilità di impoverimento della capacità critica e di comprensione dell'utente. Circostanza, questa, che affetta anche le modalità di prestazione del consenso alla cessione dei dati personali, realizzata in strutturali condizioni di asimmetrie informative, le quali «inducono il consumatore – soggetto debole nelle transazioni – ad effettuare scelte in contesti di limitata informazione e d'incertezza. In particolare, l'ignoranza dei consumatori rispetto al valore dei dati ceduti determina esternalità positive per le imprese, che generano e raccolgono questi dati, mentre – con il passare del tempo e l'acquisizione di una mole ingente di dati sul singolo consumatore/utente, ben più ampio di quello disponibile allo stesso consumatore/utente – aumenta l'asimmetria informativa tra piattaforme ed utenti, a svantaggio di questi ultimi»[39].

4. *Profilazione del consumatore e* rating *bancario nel contesto della disintermediazione finanziaria*

Fatta qualche premessa in tema di profilazione, una volta precisato che esistono algoritmi in grado di creare un *alias* digitale dell'utente-consumatore, occorre riservare più attenta considerazione al tema.

Le pratiche di profilazione[40] consentono agli algoritmi di sfruttare il comportamento degli utenti in modo da apprendere le loro inclinazioni e riuscire a interagire nel modo più efficace. In altre parole, il contegno in rete del consu-

---

[38] A giudizio di A.P. Seminara, o. c., p. 496, si assiste alla sostituzione dell'*homo oeconomicus* con l'*homo consumens*: «Lungi dal voler convincere delle qualità del prodotto, la [comunicazione commerciale] punta principalmente all'emozione, limitando se non escludendo la razionalità della decisione economica».

[39] A. Perrucci, *Dai Big Data all'ecosistema digitale*, cit., pp. 71 s.

[40] L'articolo 3*bis* del GDPR definisce la profilazione come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati 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».

matore, accuratamente "osservato", e le sue preferenze, sono classificati in base alle reazioni alle sollecitazioni che gli pervengono dai propri dispositivi digitali[41].

Sul punto, pur essendo di primaria importanza l'approccio "protezionistico", sul piano della politica del diritto pare altresì opportuno sollecitare la diligenza operata dal consumatore nel corso di tutto il percorso decisionale che lo porta all'acquisto/investimento. A tal proposito, non manca chi evidenzia le nuove opportunità offerte dall'utilizzo degli algoritmi e dalle loro "potenzialità emancipative", poiché la loro capacità di elaborazione delle informazioni «potrebbe porre le premesse per un rovesciamento degli equilibri tra il soggetto e il bene: se è vero che prodotti e servizi – progettati, realizzati ed offerti in funzione dei suoi bisogni e sulla base dei dati processati ed aggiornati in tempo reale – inseguono il consumatore fin quasi a togliergli ogni libertà di decisione critica, d'altronde proprio grazie agli stessi algoritmi egli potrebbe liberarsi da una condizione di mera soggezione ed iniziare a scansionare i beni, individuarne le caratteristiche, valutarne la qualità, ricostruirne la filiera operativa»[42].

La digitalizzazione dell'informazione ha determinato la riconfigurazione dei mercati anche in ambito finanziario. A testimonianza dello stravolgimento del modello di *business* degli istituti bancari non v'è solo la straordinaria diffusione del circuito Bancomat e delle carte di credito, ma anche degli strumenti di *home* e/o *mobile banking*, che stanno determinando la chiusura di molte filiali fisiche, con conseguente riduzione del personale, ormai sostituito da *service advisors* digitali, particolarmente impiegati anche nel contesto della consulenza finanziaria.

Intermediari finanziari e assicurazioni utilizzano i dati raccolti per stimare i rischi associati a ciascuna tipologia di cliente e, di conseguenza, per offrire a ciascun *cluster* di consumatori prodotti e servizi adeguati e pervenire così a una efficiente allocazione delle risorse e del rischio; finalità, questa, che ha spinto verso l'innovazione della procedura di *rating* bancario[43].

---

[41] In argomento si rimanda a S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, in *Luiss Un. Press*, 2019, *passim*.

[42] A. Punzi, *Il diritto e i nuovi orizzonti dell'intelligenza umana*, cit., p. 33; l'A. sottolinea, ad esempio, come esistano app che consentono di valutare la salubrità del cibo incrociando i dati dell'etichetta con le ricerche effettuate da importanti Centri di ricerca, e che esistono strumenti che, attraverso l'utilizzo della fotocamera, consentono di valutare la forma e la qualità dei prodotti, così da riconoscere frodi o altri difetti. Cfr. anche Id., *«Ragionevolmente attento ed avveduto». La responsabilità del consumatore nell'economia della conoscenza*, in *Scritti in onore di Marcello Foschini*, Padova, 2011, pp. 529 ss.

[43] Il *credit scoring* è quella procedura attraverso la quale viene affidato a ciascun potenziale cliente un punteggio basato sulle proprie caratteristiche. Così, chi intenda richiedere un finanziamento a una banca o ad altro intermediario finanziario, viene

Di qui l'attenzione riservata al c.d. ecosistema *Fintech*, contesto nel quale vengono offerti – in maniera altamente digitalizzata – servizi di finanziamento, pagamento, investimento e consulenza, sovente caratterizzati da disintermediazione; si tratta di «un insieme di società accomunate dallo sviluppo di attività basate su nuove tecnologie informatiche e digitali, che vengono applicate in ambito finanziario»[44].

Dal momento che i sistemi finanziari forniscono alcuni servizi essenziali come l'allocazione di capitale, la facilitazione delle transazioni e la gestione del rischio, la *Fintech* è uno strumento in grado di offrire opportunità economiche e migliorare la vita delle persone. D'altra parte, invero, essa reca ingenti rischi correlati alla *cybersecurity*, alla protezione dei dati personali, alla lotta contro il riciclaggio, nonché alla discriminazione e all'equo accesso ai finanziamenti[45]; sorge altresì il pericolo di c.d. *social scoring* (quantomeno indirettamente, dato che allo stato è pratica vietata entro i confini UE[46]), poiché oggi risulta quasi inevitabile una valutazione dell'individuo tramite la sua solvibilità[47].

---

sottoposto a una valutazione sul merito di credito che si risolve nella traduzione alfanumerica della capacità di far fronte agli obblighi finanziari: il punteggio ottenuto può determinare il tasso di interesse (che è normalmente correlato alla finalità di remunerare il rischio di insolvenza), ma anche altre condizioni contrattuali, quali l'ammontare del prestito e i tempi previsti per il suo rimborso, o le garanzie richieste. Sul piano regolatorio in tema di *rating* bancario e profilazione della clientela, la disciplina di riferimento è il Regolamento (UE) n. 575/2013 del Parlamento Europeo e del Consiglio del 26 giugno 2013 relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il Regolamento (UE) n. 648/2012; nonché la Direttiva 2013/36/UE del Parlamento Europeo e del Consiglio del 26 giugno 2013 sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la Direttiva 2002/87/CE e abroga le Direttive 2006/48/CE e 2006/49/CE.

[44] *Lo sviluppo del Fintech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, in *Quaderni Fintech Consob*, 1° marzo 2018, p. 9.

[45] P.P. Pirani, *Gli strumenti della finanza disintermediata*: Inizial Coin Offering e blockchain, in *An. giur. ec.*, 2019, 328 s.; S. Pesucci, *Critica etica*, cit., p. 2.

[46] Sebbene nell'esperienza europea si rinvengano meccanismi che, pur non determinando l'attribuzione di veri e propri punteggi di carattere generale dei cittadini e degli operatori economici, permettono comunque l'adozione di decisioni amministrative automatizzate che sfruttano informazioni ottenute tramite l'utilizzo di vari *database*; in argomento, v. G. Sciascia, *Reputazione e potere: il social scoring tra distopia e realtà*, in *Giornale dir. amm.*, 2021, cit., p. 321.

[47] S. Pesucci, o. c., 1; l'A. sottolinea, alla pag. seguente, come «tutto il nostro sistema europeo, dal modello bancario a quello dei mercati, dalla gestione del lavoro a quello della semplice circolazione dei cittadini membri, può essere riletto e valutato

La tecnologia finanziaria ha un ruolo sempre più determinante nelle decisioni degli istituti finanziari in ordine all'offerta dei tassi di interesse, premi assicurativi, o anche nell'automatizzazione del procedimento di *credit scoring*. Proprio con riferimento alla valutazione del merito creditizio, si evidenzia come mentre, tradizionalmente, gli intermediari finanziari indagavano – si può dire in forma statica – sulla storia creditizia del cliente (da lui fornita o acquisita tramite le banche dati), nonché sulla capacità reddituale e di rimborso dello stesso, oggi è possibile estrarre dati anche dall'utilizzo dello *smartphone*, dei *social network*, o di altri dispositivi digitali ("*all data is credit data*"). Dati che, sovente, hanno poco o nulla a che vedere con il sistema creditizio, quali le preferenze di spesa (tipologia di acquisti e geolocalizzazione) e le abitudini dell'utente[48].

In proposito, sebbene il Regolamento UE 679/2016 non osti, di per sé, all'utilizzo dei dati *social* per profilare un individuo al fine di valutarne il merito creditizio[49], le informazioni che il finanziatore ha il dovere di raccogliere debbono essere «adeguate»[50] anche sotto il profilo qualitativo: vale a dire che dovrebbero essere limitate – come impone l'articolo 20, par. 1, della Direttiva 2014/17/UE – al profilo attinente alle spese, al reddito e alle altre informazioni riguardanti la situazione economico-finanziaria del consumatore.

Dei rischi legati all'utilizzo di tecniche totalmente "robotizzate" è ben consapevole (anche se, forse, non sufficientemente reattivo) il legislatore comunitario; l'attuale impianto legislativo e, in particolare, la lettura in combinato disposto dell'art. 22 GDPR con il Considerando 71 del medesimo Regolamento[51], prevede – in riferimento alle domande di credito senza interventi umani – il diritto del consumatore dei servizi bancari a non essere soggetto in modo esclusivo a decisione di tipo automatizzato e impone agli intermediari bancari l'utilizzo

attraverso il filtro del *Credit Scoring*».

[48] Sul difficile bilanciamento tra GDPR e gestione automatizzata del *credit scoring*, si v. il caso "*Schufa*" (C-634/21/SCHUFA Holding (Scoring), nell'ambito del quale la Corte ha stabilito che l'articolo 22, par. 1, GDPR deve essere interpretato nel senso che il calcolo automatizzato, da parte di una società che fornisce informazioni commerciali, di un *tasso di probabilità basato su dati personali relativi a una persona* e *riguardanti la capacità di quest'ultima di onorare in futuro gli impegni di pagamento*, costituisce un «processo decisionale automatizzato relativo alle persone fisiche»; motivo per il quale deve trovare applicazione la disposizione in questione qualora da tale tasso di probabilità *dipenda in modo decisivo la stipula, l'esecuzione o la cessazione di un rapporto contrattuale* con tale persona da parte di un terzo, al quale è comunicato tale tasso di probabilità.

[49] Cfr. articolo 22, par. 2, lett. a) e par. 4; articolo 9, par. 2, lett. a).

[50] Il riferimento è alla lettera dell'articolo 124*bis* TUB.

[51] F. Bagni, *Uso degli algoritmi nel mercato del credito: dimensione nazionale ed europea,* in *Oss. sulle fonti*, p. 915.

di «appropriate» tecniche di profilazione, tali da ridurre al minimo il margine d'errore e da evitare il rischio che si pervenga a esiti discriminanti o, addirittura, a pratiche di *behavioural scoring*[52].

D'altra parte, la valutazione circa l'affidabilità dei potenziali clienti, l'utilizzo massivo di dati, le tecnologie di intelligenza artificiale e, in generale, l'impiego degli algoritmi di *machine learning* hanno anche permesso a banche e altri intermediari finanziari di "conoscere" meglio gli utenti che con essi si interfacciano; il che ha reso possibile disegnare una via per la prevenzione dei rischi e la predisposizione di modelli statistici[53].

Sebbene lo sviluppo di simili sistemi ponga una serie di problematiche afferenti alla tutela del consumatore, sia circa la libertà di scelta nell'atto di acquisto/investimento, sia con riguardo alla regolamentazione in tema di dati personali e trasparenza informativa, v'è chi ha posto in evidenza come l'utilizzo dei dati *social* sia, oramai, imprescindibile[54].

Ciò detto, è comunque necessario che la procedura di valutazione dell'affidabilità del cliente – soprattutto se condotta in forma automatizzata – sia presa in considerazione insieme a due fattori di debolezza del consumatore: la standardizzazione della contrattazione e le asimmetrie informative che, già da tempo, hanno indotto alla modificazione dell'approccio del legislatore, europeo e nazionale, soprattutto con riguardo ai doveri informativi del professionista.

Analogamente, c'è da domandarsi quali siano gli effetti della tecnologia finanziaria, in chiave economica e comportamentale, sul diritto della crisi e, per quel che qui interessa, sulla situazione di sovraindebitamento del consumatore. Le

---

[52] Evidenzia G. Sciascia, *Reputazione e potere,* cit., 323, «nel settore del credit scoring non esistono regole […] dettagliate, sicché l'elaborazione dei dati creditizi individuali non è sottoposta ad alcuna forma diffusa di controllo o validazione, e la bontà delle metodologie è valutata da parte dell'industria solo in rapporto all'effettiva capacità ed efficacia predittiva: questa caratteristica può determinare non soltanto il ricorso sistematico a metodi poco trasparenti o a dati non necessariamente robusti, ma anche il consolidarsi di bias metodologi particolarmente difficili da intercettare e correggere, come quelli di tipo razziale […]». Sul c.d. *creditworthiness by associations*, cfr. M. Hurley, J. Adebayo, *Credit Scoring in The Era of Big Data*, in *18 Yale J.L. & Tech.*, 148, 2016, pp. 150 ss.

[53] In dottrina si è rilevato come l'utilizzo dei *big data* abbia apportato ingenti benefici al settore finanziario, sia in ambito bancario (nel quale, appunto, si riscontra una semplificazione del processo di valutazione del merito creditizio), che in quello degli investimenti (nel quale è possibile ottenere in modo rapido ed efficace analisi e *report* delle quotazioni in borsa delle azioni). Cfr. D. Mastrelia, *Gestione dei* bigdata, cit., p. 366; cfr. anche P. Pia, *La consulenza finanziaria automatizzata*, Milano, 2017, *passim*.

[54] F. Mattassoglio, *Innovazione tecnologica e valutazione del merito creditizio dei consumatori. Verso un* Social Credit System?, Milano, 2018, pp. 21 s.

attuali riflessioni socio-economiche unite agli studi comportamentali[55], sono in grado di spiegare – differentemente dalla dottrina classica del diritto fallimentare, anch'essa fondata sul modello dell'operatore razionale – una serie di dinamiche afferenti al diritto della crisi, quali la tendenza del consumatore a indebitarsi eccessivamente anche per sostenere spese non indispensabili, le difficoltà a riconoscere e far emergere tempestivamente la propria crisi finanziaria o, ancora, le condotte riconducibili al c.d. *moral hazard* e alla (meno grave, dal punto di vista del dolo) sovrastima delle proprie capacità intellettive e di gestione della crisi patrimoniale e finanziaria (c.d. *overconfidence bias*), prima che essa divenga irreversibile. In sostanza, gli individui paiono ottimisti circa la capacità di tenere sotto controllo la situazione che attraversano.

È chiaro che non si potrà non tener conto di queste circostanze nell'ambito del bilanciamento di responsabilità tra intermediario finanziario e cliente, considerate non solo le menzionate distorsioni comportamentali nelle quali quest'ultimo incappa inconsapevolmente (e incolpevolmente), ma anche lo squilibrio di competenze e di consapevolezza tra le parti coinvolte.

5. *Rischi e aspetti problematici insiti nell'utilizzo delle nuove tecnologie. Conclusioni*

Come si è visto, dunque, la contaminazione tra tecnologie digitali e dell'informazione, le neurotecnologie e gli strumenti di intelligenza artificiale, costituiscono i pilastri della "quarta rivoluzione industriale". Se, da una parte, essa ha recato con sé indubbi benefici e opportunità[56], quali innovazione, crescita economica e benessere, di contro non può che constatarsi come il fattore umano abbia perduto il controllo sulle conseguenze della incontrollata circolazione delle informazioni personali degli utenti che si interfacciano con tali tecnologie.

---

[55] *Ex multis*, si v. G.S. Becker, *The Economic Approach to Human Behavior*, Chicago, 1976; E.-M. Sent, *Behavioral economics: How Psychology Made Its (Limited) Way Back Into Economics*, in *History of Political Economy*, 2004, pp. 735 ss.; C.F. Camerer, G. Loewenstein, *Behavioral economics, Past, Present, Future*, in C.F. Camerer, G. Loewenstein, M. Rabin (a cura di), *Advances in Behavioral Economics*, New Delhi, 2006, pp. 3 ss.; F. Heukelom, *Behavioral Economics: A History*, New York, 2014, *passim*; E. Angner, *Economia comportamentale. Guida alla Teoria della scelta*, Milano, 2017, *passim*.

[56] I sistemi di *credit scoring* basati sull'utilizzo dei dati raccolti da *social network* potrebbero essere impiegati per estendere il mercato del credito ai c.d. *unbanked*; circostanza che potrebbe portare nuove opportunità di inclusione finanziaria a soggetti che, altrimenti, farebbero fatica a partecipare attivamente alla vita economica, come ad esempio i migranti extracomunitari.

L'uso dei dati forniti dalle persone e scambiati tra operatori economici ingenera altresì il rischio di immissione, seppur non intenzionale, di pregiudizi nel ragionamento algoritmico[57]. Ed invero, il contesto sociale di appartenenza e il *bias* individuale del programmatore hanno grande peso nella progettazione delle tecnologie predittive. Per individui che non si trovano al vertice della piramide del privilegio, i rischi correlati a questa dinamica sono molto seri e potrebbero costituire una questione vitale, dall'accesso al credito alla detenzione preventiva; si pensi altresì ai sistemi di giustizia[58] o, addirittura, di polizia *predittiva*[59], in grado di mettere alla prova anche gli ordinamenti di democrazia liberale.

È chiaro che tali circostanze recano con sé, come conseguenza, l'incremento del rischio di disuguaglianze economiche e sociali. Generalmente, infatti, gli algoritmi di *machine learning* funzionano molto bene per i *clusters* di popolazione sui quali e per i quali sono stati sviluppati, ma se vengono applicati in un contesto diverso – come una differente area geografica, un'altra etnia o simili fattori di discrimine – esiste un alto rischio che si incappi in errori e distorsioni.

Con specifico riferimento al settore finanziario, il GDPR si dimostra inadeguato ad arginare le potenziali discriminazioni esito del *credit scoring*, dato l'ampio rilievo attribuito al consenso dell'interessato, che rende legittimo l'uso di algoritmi profilanti (v. il par. 2, lett. c) del già menzionato articolo 22). Invero, il principio del consenso informato – prestato dal consumatore senza troppo riflettere, per avere immediato accesso ai servizi digitali – si rivela difficilmente compatibile con l'utilizzo dei *big data*, la cui tecnologia «non consente di circo-

---

[57] Problema, questo, fortemente legato all'utilizzo dei *dati sensibili*, quali origine razziale, etnia, convinzioni politiche e religiose, orientamento sessuale o, ancora, i dati relativi alle proprie condizioni di salute.

[58] Al limite dell'inquietante il caso di Eric Loomis, imputato afroamericano, condannato a sei anni di reclusione sulla base di un algoritmo "Compas" che lo classificava come soggetto ad alto rischio di recidiva sulla base di una serie di informazioni fornite dal sistema. La Corte Suprema del Wisconsin nel 2016 ha confermato la sentenza e affermato la legittimità della procedura, sostenendo che la mancata conoscenza da parte dell'imputato sul funzionamento dell'algoritmo non violasse il suo diritto a un equo processo. F. Benassi, *ChatGPT, l'evoluzione dell'intelligenza artificiale e la sua applicazione in campo giuridico – Spunti per un dibattito*, in *ilCaso.it*, p. 4, evidenzia il rischio dell'utilizzo di algoritmi e sistemi di *ML* nell'amministrazione della giustizia, soprattutto in riferimento al potenziale aumento delle diseguaglianze e dell'iniquità per mezzo della base basi dati utilizzata dalla macchina, «la cui formazione potrebbe essere influenzata da dati storici inadeguati o da fattori discriminanti».

[59] Per il quale si rimanda a J. Chan, L.B. Moses, *Is Big Data Challenging Criminology?*, in *Theoretical Criminology*, 20, 1, 2016, pp. 21 ss.; B.J. Jefferson, *Predictable Policing: Predictive Crime Mapping and Geographies of Policing and Race*, in *Annals of American Association of Geographers*, 108, 1, 2018, pp. 1 ss.

scrivere lo scopo per cui un dato è raccolto e trattato, potendo essere riutilizzato per fini diversi rispetto a quelli originari col c.d. *repurposing dei dati*»[60].

Peraltro, l'utilizzo di tecniche algoritmiche nel settore bancario non è immune dai possibili esiti discriminatori, specie se avviene tramite lo sfruttamento dei cc.dd. *dati aggregati*. L'algoritmo, cioè, pur essendo in grado di individuare e di avvalersi correttamente delle informazioni reperite, è nondimeno progettato per prediligere meccanismi di ottimizzazione in termini di *performance*; vale a dire che quando nei modelli viene immesso lo scopo di massimizzazione di un obiettivo (profitto, sicurezza, ecc.), non è affatto infrequente che si pervenga a correlazioni illegittime tra dati[61]. Viene dunque da chiedersi se un modello completamente automatizzato di valutazione del merito di credito sia eticamente sostenibile. Il ruolo dell'umano non può limitarsi a «nutrire» il sistema dell'algoritmo, ma dovrebbe essere anche (e soprattutto) finalizzato ad assicurare una valutazione critica tanto delle modalità di raccolta dei dati, quanto dei meccanismi di elaborazione delle informazioni e di decisione proposti dalla macchina[62].

Quale ruolo, dunque, si vuole affidare alle intelligenze artificiali? Il sistema algoritmico «*organizza gerarchicamente l'informazione, indovina ciò che ci interessa, seleziona i beni che preferiamo e si sforza di sostituirci in numerosi compiti. Siamo noi a fabbricare questi calcolatori ma in cambio loro ci costruiscono*»[63]. È dunque governabile?

Sarebbe necessario riflettere *in primis*, su quali siano le modalità più adatte a regolare gli effetti che gli algoritmi producono sulle relazioni interpersonali; e, in secondo luogo, sulla capacità dell'operatore umano di adattare questa nuova realtà *IT* agli istituti giuridici tradizionali. Tali obiettivi comportano importanti sfide per il giurista, al quale spetta l'arduo compito di pervenire a una soluzione ai nuovi conflitti sorti tra interessi contrastanti: se sono da guardare con favore l'innovazione e la competitività, è al contempo necessario garantire trasparenza e sicurezza nella raccolta dei dati e nei processi decisionali automatizzati[64].

---

[60] G. Mattarella, Big Data *e accesso al credito degli immigranti*, cit., 709. Cfr anche F. Mattassoglio, *Innovazione tecnologica,* cit., p. 155.

[61] Si v. Federal Trade Commission, *Big data: a tool for inclusion or exclusion*, FTC, Jan. 2016, consultabile sul sito web istituzionale.

[62] F. Benassi, o. c., p. 24, sottolinea che «[l]'interpretazione dei dati e la contestualizzazione delle informazioni sono compiti che richiedono il giudizio umano, il quale può essere determinato e influenzato da fattori che l'intelligenza artificiale non è in grado di considerare».

[63] D. Cardon, *Che cosa sognano gli algoritmi. Le nostre vite ai tempi dei big-data*, Milano, 2016, *Introduzione*.

[64] «*Se vuole raccogliere le sfide dell'innovazione, il giurista è costretto ad osservare l'intelligenza delle macchine e abituarsi ad interagire con esse in modo da poter aggiornare, se*

Da un lato, quindi, si colloca la menzionata problematica della trasparenza, poiché è necessario garantire la conoscibilità (e la tracciabilità) delle fasi procedurali che inducono l'algoritmo ad effettuare una scelta; dall'altro, poiché a tali algoritmi vengono affidate operazioni che comportano un livello sempre crescente di responsabilità nell'influenzare o prendere decisioni o, ancora, nell'effettuare transazioni finanziarie, si pone la questione della responsabilità[65].

Emerge un approccio (troppo?) neutro del legislatore europeo, il quale – probabilmente al fine di non disincentivare il processo di innovazione – ha finora evitato di introdurre regole più stringenti per regolare l'utilizzo degli algoritmi. Si deve tuttavia condividere l'opinione di chi ha evidenziato la necessità di introdurre specifiche regolamentazioni di settore, con la previsione di principi che si riferiscano in maniera puntuale alle tecniche algoritmiche e di profilazione[66]; ci si auspica, così, che nel futuro prossimo gli algoritmi possano pervenire a "deliberazioni" nella maniera più oggettiva, trasparente e non discriminatoria possibile.

De iure condendo, dal momento che agli algoritmi vengono assegnate operazioni comportanti un livello sempre crescente di autonomia nell'influenzare decisioni o nell'eseguire transazioni finanziarie, per le quali è spesso difficile (se non impossibile) spiegare al consumatore chi e secondo quali criteri ha effettuato la scelta, al legislatore è richiesto di supplire alla mancanza di puntuali soluzioni positivizzate circa i profili di responsabilità civile da errore dell'algoritmo. «Infatti nella gestione della responsabilità legata all'*AI* il livello di imprevedibilità di

---

non addirittura rideclinare, alcuni dei suoi princìpi. Non basta più proclamare valori come la dignità umana e la conoscenza o auspicare un bilanciamento tra diritti parimenti tutelati e potenzialmente in conflitto. La sfida è comprendere a quali condizioni sia giusto intervenire sull'algoritmo o comunque fissare limiti alla sua azione. […] Ecco che, per poter interagire con l'algoritmo, e, quando necessario, fissare dei limiti alla sua azione, il giurista – sia esso legislatore, giudice, regolatore – da un lato deve tornare a pensare alcune grandi questioni che il metodo giuspositivistico riteneva estranee al suo ambito di indagine […], dall'altro deve riuscire, per dir così, a entrare dentro le macchine, a leggerne gli ingranaggi, a capirne i linguaggi», così A. Punzi, *Il diritto e i nuovi orizzonti dell'intelligenza umana*, cit., p. 32.

[65] Sulla centralità che rivestono «la qualità, la quantità dei dati, il contesto di raccolta, le modalità di selezione» nella delimitazione dei nuovi sistemi di responsabilità civile connessa alle intelligenze artificiali, si v. G. Comandé, *Intelligenza artificiale e responsabilità*, cit., pp. 169 ss. e, in part., pp. 171 s., il quale chiarisce che «l'operatività della IA […] pone l'esigenza di un riporto di rischi e dei costi tra una pluralità di attori (sviluppatori, integratori, produttori e distributori di dati, gestori di telecomunicazioni…) con implicazioni significative sulle modalità di ripartizione dell'onere finanziario. In queste ipotesi e in particolare per la r.c. è stata argomentata la possibilità di ricostruire una responsabilità solidale e multipla in capo a tutti i soggetti che concorrono allo sviluppo di una intelligenza artificiale».

[66] F. Bagni, *Uso degli algoritmi*, cit., 2021, p. 926.

azioni e comportamenti degli agenti artificiali autonomi assume una dimensione diversa dal solito quando un sistema che impara dai dati ambientali, per esempio, può agire in modi che i suoi sviluppatori non hanno alcun modo di prevedere». E ciò assume maggiore portata laddove tali sistemi sono addestrati per modificare le loro funzioni e continuare ad apprendere, perché tale circostanza rende difficoltosa l'individuazione di un agente cui ricondurre la responsabilità[67].

In conclusione, parendo difficile poter prescindere da un uso sempre maggiore di dati personali (nel settore finanziario e non), si pone, urgente, il tema della responsabilizzazione etica della società digitale[68] e di quella individuale, che può essere assicurata solo con un'efficace educazione digitale (e finanziaria), oltre che attraverso una efficace regolamentazione. È necessario essere consapevoli dei nostri limiti e del fatto che molte delle nostre scelte derivano da fattori ambientali e dalle stimolazioni che riceviamo attraverso comunicazioni personalizzate. A fronte di tali considerazioni, emerge come il problema non riguardi la sola gestione e protezione dei dati personali degli utenti: concerne, invero, i temi della democrazia, dell'uguaglianza e della libertà in senso lato, essendo tali meccanismi decisionali in grado di determinare conseguenze "vitali" per i destinatari del ragionamento algoritmico.

Se – nell'ottica di "collaborazione", e non competizione, tra individui e macchine intelligenti – si saprà controllare il progresso tecnologico, piuttosto che subirlo, l'essere umano sarà in grado di condizionare positivamente l'esito di questo percorso di cambiamento (forse) senza precedenti.

---

[67] *Ivi*, p. 178.

[68] In questo senso pare opportuno riportare le considerazioni di D. Mastrelia, *Gestione dei* bigdata, cit., p. 372, che si ritiene di condividere: «Nel bilanciamento di interessi fra il diritto alla privacy e uso dei bigdata non vi è una prevalenza assoluta dell'uno sull'altro. Il diritto alla privacy deve essere un diritto garantito in un ecosistema digitale "ipersorvegliato" mentre i *bigdata* rappresentano una risorsa importante per la ricerca, per l'industria e per il mercato. Le soluzioni "orientate alla privacy" dell'uso dei *bigdata* […] rappresentano un'ottima soluzione per tutelare la riservatezza degli individui ed al contempo consentire l'uso dei *bigdata*. Bisognerà, in altre parole, utilizzare i *bigdata* – frutto della modernità – abbracciando un antico valore di civiltà: l'etica».

La responsabilità nella produzione di alimenti e l'impatto dell'IA

di **Riccardo Lazzardi**

1. *Una premessa sistematica*

Una categoria del danno da cose, la cui logica fuoriesce da quella codicistica, riguarda il cosiddetto danno da prodotto difettoso[1]. Le norme di questa disciplina – originariamente contenute nella Direttiva 85/374/CEE – sebbene siano oggi inserite nel codice del consumo, mirano alla tutela non solo del consumatore, ma dell'utilizzatore, categoria dal carattere più generale, consistente in chi fa uso di un bene o un servizio[2], che può pure non coincidere col consumatore. In tal senso, quando è stata introdotta, obiettivo del legislatore non era quello

[1] Sul danno da prodotto difettoso vd., senza pretesa di esaustività, F. Busoni, *Art. 115 – Prodotto*, in G. Vettori (a cura di), *Commentario al codice del consumo*, Padova, 2007, p. 830 ss.; U. Carnevali, *La responsabilità del produttore*, Milano, 1979, p. 342 ss.; Id., *«Produttore» e responsabilità per danno da prodotto difettoso nel codice del consumo*, in *Resp. civ. prev.*, 10, 2009, p. 1943; G. D'Amico, *Il contratto o i contratti*, in *Riv. dir. civ.*, 3, 2023, p. 419 ss.; G. Germanò, M.P. Ragionieri ed E. Rook Basile, *Diritto agroalimentare. Le regole degli alimenti e dell'informazione alimentare*, Torino, 2019, p. 50 ss.; A. Legnani, *Prodotti difettosi. La responsabilità per danno. Commento al d. P.R. 24 maggio 1988, n. 224*, Rimini, 1990, p. 160; P. Perlingieri, *Manuale di diritto civile*, Napoli, 2022, p. 545 ss.; A. Stoppa, *Responsabilità del produttore*, in *Dig. disc. priv.*, Torino, 1998, p. 132; P. Trimarchi, *Rischio e responsabilità oggettiva*, Milano, 1961, p. 268.

[2] L'utilizzatore può coincidere con il consumatore, ma può anche essere un soggetto diverso, specie quando si parla di un bene o servizio acquistato da terzi. In particolare, vd. Cass. civ., 29/05/2013, n. 13548, in *Onelegale*, secondo cui l'utilizzatore va inteso «in senso lato e, quindi, indubbiamente ad una persona fisica […] ma non esclusivamente al "consumatore" o utilizzatore non professionale».

di tutelare il consumatore, bensì quello di armonizzare le legislazioni degli Stati membri in materia di responsabilità da prodotto difettoso, onde evitare che approcci diversificati potessero dare vita a misure restrittive della libera circolazione delle merci, trattandosi, quindi, di uno scopo di tutela della libertà economica[3]. Ciò emerge da diversi indici presenti nella normativa, i quali potrebbero sfuggire dal momento che è confluita nel codice del consumo. Segnatamente, questa stabilisce che il produttore è responsabile «del danno cagionato dai difetti del suo prodotto[4]», aggiungendo poi che il prodotto si considera difettoso quando «non offre la sicurezza che ci si può legittimamente attendere[5]», tenendo conto di una serie di circostanze[6], tra cui, ad esempio, l'uso cui il prodotto può ragionevolmente essere destinato, o altri comportamenti che si possono attendere da parte degli utenti, come nel caso di un giocattolo per bambini che presenta pezzi smontabili e facilmente ingeribili; il bene, per come concepito, non è destinato ad essere mangiato, tuttavia questo è un comportamento che ci si può ragionevolmente aspettare in relazione all'uso.

È per mezzo della segnalazione del profilo di insicurezza che l'utilizzatore può ragionevolmente attendersi determinate conseguenze derivanti da un uso anche

---

[3] L'obiettivo di un efficiente funzionamento del mercato interno è sempre stato alla base delle direttive in tema di prodotti, almeno fino a quando iniziarono i lavori della Commissione per una direttiva sulla responsabilità per danno da prodotto; in quella fase si notò invero come differenti regimi giuridici nazionali in tema di responsabilità per danno da prodotto sono suscettibili di creare distorsioni della concorrenza nel mercato comune. Così U. Carnevali, *Prevenzione e risarcimento nelle Direttive comunitarie sulla sicurezza dei prodotti*, in *Resp. civ. prev.*, 2005, p. 4. Vd. il *Considerando* n. 1 della Direttiva 85/374/ CEE, il quale recita, segnatamente, che «il ravvicinamento delle legislazioni nazionali in materia di responsabilità del produttore per i danni causati dal carattere difettoso dei suoi prodotti è necessario perché le disparità esistenti fra tali legislazioni possono falsare il gioco della concorrenza e pregiudicare la libera circolazione delle merci all'interno del mercato comune determinando disparità nel grado di protezione del consumatore contro i danni causati alla sua salute e ai suoi beni da un prodotto difettoso».

[4] Vd. per ulteriori approfondimenti F. Busoni, *Art. 114 cod. cons. – Responsabilità del produttore*, in G. Vettori (a cura di), *Commentario al codice del consumo*, cit., p. 835 ss.

[5] F. Busoni, *Art. 117 – Prodotto difettoso*, in G. Vettori (a cura di), *Commentario al codice del consumo*, cit., p. 835 ss.

[6] Tra le quali: il modo in cui il prodotto è stato messo in circolazione, la sua presentazione, le sue caratteristiche palesi, le istruzioni e le avvertenze fornite; l'uso al quale il prodotto può essere ragionevolmente destinato e i comportamenti che, in relazione ad esso, si possono ragionevolmente prevedere; il tempo in cui il prodotto è stato messo in circolazione. Vd. F. Busoni, *o.u.c.*, p. 835 ss.

diverso da quello normale; in tal senso sarebbe da evidenziarsi un rapporto tra difetto e obbligo informativo: il difetto sarebbe tale dal momento in cui non si osserva l'obbligo informativo, potendo infatti accadere che, benché provenienti da due produttori diversi, due prodotti siano identici, cioè realizzati nello stesso modo, ma uno sia considerato difettoso, mentre l'altro no, laddove solo per uno siano state condivise le informazioni sul livello di sicurezza[7].

C'è allora una nozione profondamente diversa da quella di vizio di bene che si può trovare in materia di garanzia dei vizi nella vendita, proprio in ragione del fatto chee un prodotto può essere difettoso senza essere viziato, in quanto è sufficiente che presenti un livello di sicurezza inferiore a quella attesa[8]. È possibile invero che il produttore venga ritenuto responsabile a prescindere dal difetto di fabbricazione in senso stretto, e anche nel caso in cui il danno sia derivato da un suo uso improprio, se ragionevolmente prevedibile, essendo necessario adottare un accorgimento funzionale ad evitare l'uso anomalo ma prevedibile. Questa è, in definitiva, la nozione di difetto che viene presa in considerazione.

È doveroso peraltro rammentare le novità derivanti dalla normativa euro-unitaria, che, rappresentando un indice del costante interesse da parte del legislatore sulla tematica, necessitano almeno di un cenno. Si intende far riferimento, anzitutto, al Regolamento 2023/988, relativo alla «sicurezza generale dei prodotti» e, in particolare, alla recentissima Direttiva (UE) 2024/2853, destinata a sostituire la Direttiva 85/374/CEE.

1.1 *La prova*

Ai sensi dell'art. 118 cod. cons[9]., una volta provato danno, difetto e rapporto di causalità, il produttore si libera in casi tassativi, tra cui, ad esempio, nell'ipotesi

---

[7] Sulle problematiche e sul coordinamento fra disciplina della responsabilità del produttore e sicurezza generale dei prodotti vd. F. Cafaggi, *Danno al prodotto e funzioni della responsabilità del produttore, in Riv. crit. dir. priv., 1988,* in *Riv. crit. dir. priv.*, 1988, p. 447; L. Mansani, *Gli oneri di informazione sulla sicurezza dei prodotti*, in *Nuova giur. civ.*, II, 1996, p. 269.

[8] Sulla vendita dei beni di consumo vd. C. Chessa, *I termini nella vendita dei beni di consumo*, in V. Buonocore, A. Luminoso e G. Fauceglia (a cura di), *Codice della vendita,* Milano, IV, p. 1396 ss.; V. Barba, *La conformità del bene venduto al contratto*, in G. Vettori (a cura di), *Contratto e responsabilità*, Padova, 2013, vol. II, p. 1147 ss.; T. Dalla Massara, *La «maggior tutela» del consumatore: ovvero del coordinamento tra codice civile e codice del consumo dopo l'attuazione della direttiva 2011/83/UE*, in *Contr. impr,*, 2016, p. 743 ss.

[9] F. Busoni, *Art. 118 cod. cons. – Esclusione della responsabilità*, in G. Vettori (a cura di), *Commentario al codice del consumo*, cit., p. 845 ss.

in cui il difetto non esisteva quando il prodotto è stato messo in circolazione, perché manipolato magari in una fase successiva, e, per quanto qui ritenuto di maggiore interesse, nell'ipotesi cosiddetto rischio da sviluppo, sussistente allorquando lo stato delle conoscenze tecniche e scientifiche, nel momento in cui il produttore ha messo in circolazione il prodotto, non permetteva ancora di considerarlo come difettoso[10]. La giurisprudenza, sul punto[11], ha avuto modo di notare come non si debba parlare di responsabilità oggettiva[12], bensì di responsabilità presunta, stante la previsione espressa che reca la possibilità di dare prove contrarie ulteriori rispetto al caso fortuito. In particolare, prendendo in considerazione il rischio da sviluppo[13], la norma ci dice che questo non è sopportato dal produttore; introdurre a livello sistematico una esimente di tal genere significa che dei danni prodotti sino al momento in cui non vi siano riscontri che ne evidenzino la pericolosità non si risponde. Non ci si può quindi far carico di ciò che

[10] Come nota C. Del Federico, *Intelligenza artificiale e responsabilità civile. Alcune osservazioni sulle attuali proposte europee*, in *Jus civile*, 2023, p. 1029 ss. si tratta di uno strumento di armonizzazione minima, come si legge nel *Considerando* n. 14 della proposta, focalizzato su strumenti posti in relazione alla prova del nesso di causalità e della colpa, che tiene conto dei futuri sviluppi tecnologici, normativi e giurisprudenziali, al fine di valutare l'opportunità di armonizzare altri aspetti delle domande di risarcimento dei danni.

[11] Così Cass. civ., 07/04/2022, n. 11317, in *Onelegale*, secondo cui «la responsabilità da prodotto difettoso ha natura non già oggettiva bensì presunta, in quanto prescinde dall'accertamento della colpevolezza del produttore ma non anche dalla dimostrazione dell'esistenza di un difetto del prodotto, e ai sensi del D.Lgs. n. 206 del 2005, art. 120 (c.d. codice del consumo) incombe al soggetto danneggiato dare la prova del collegamento causale, non già tra prodotto e danno, bensì tra difetto e danno; e che, una volta fornita tale prova, a norma dell'art. 118 c.p.c., incombe sul produttore fornire la c.d. prova liberatoria, consistente nella dimostrazione che il difetto non esisteva nel momento in cui il prodotto veniva posto in circolazione o che all'epoca non era riconoscibile in base allo stato delle conoscenze tecnico-scientifiche»; in senso conforme, Cass. civ., 20/11/2018, n. 29828, in *Onelegale*, la quale ha rilevato che «la responsabilità da prodotto difettoso integra pertanto un'ipotesi di responsabilità presunta (e non già oggettiva), incombendo sul danneggiato che chiede il risarcimento provare gli elementi costitutivi del diritto fatto valere, e in particolare l'esistenza del "difetto" del prodotto, nonché del collegamento causale tra difetto e danno».

[12] Non pare superfluo ricordare come per G. Osti, *Scritti giuridici*, vol. I, Milano, 1973, p. 10, «la distinzione tra responsabilità subiettiva e obiettiva riposa sull'estensione dell'impedimento: mentre per l'impossibilità obiettiva non v'è possibilità di porre in essere la prestazione da parte di nessuno, per la responsabilità subiettiva la prestazione, sebbene non possa essere eseguita dal debitore, potrebbe essere eseguita da altri».

[13] Vd. A. Bertolini, *La responsabilità del produttore*, in E. Navarretta (a cura di), *Il Codice della responsabilità civile*, Milano, 2021, p. 2638.

non era conoscibile, in questo senso ancora meglio evidenziandosi la *ratio* della norma, che, come detto, mira non tanto alla tutela del consumatore, quanto alla libera circolazione delle merci[14]. Pare emergere così l'intenzione della disciplina di porsi in contrasto col principio di precauzione, che nel dubbio impone di fermarsi, pena l'imputazione del rischio.

La Direttiva (UE) 2024/2853 ripropone pedissequamente la fattispecie all'art. 11. L'art. 18 lascia, tuttavia, un margine di discrezionalità agli Stati membri, laddove manifestino la volontà di «mantenere[15] […] le misure esistenti in base alle quali gli operatori economici sono responsabili anche se dimostrano che lo stato oggettivo delle conoscenze scientifiche e tecniche al momento dell'immissione del prodotto sul mercato», ovvero di introdurle *ex novo* o modificarle[16].

Vanno peraltro tenute in considerazione altre normative che possono venire in rilievo, come quella sulla sicurezza dei prodotti di cui agli artt. 102 ss. cod. cons., la quale dispone, all'art. 104 cod. cons., l'obbligo di segnalazione, richiamo e ritiro per il produttore laddove, successivamente alla commercializzazione, emerga un profilo di insicurezza del prodotto. È opportuno nondimeno distinguere: un conto è la responsabilità da prodotto difettoso, che opera nella fase antecedente alla commercializzazione, un altro è l'obbligo di garantire la sicurezza dei prodotti, che viene in rilievo nella fase successiva[17]. Dal momento in cui, a seguito della

---

[14] Come si noterà a breve, se la scienza, poi, facendo il suo corso, ne accerta la pericolosità, può al massimo sorgere un obbligo di ritirare dal commercio il bene. Vd. L. Cabella Pisu, *Ombre e luci e luci nella responsabilità del produttore*, in *Contr. impr.*, 2008, p. 617 ss., che sottolinea la «finalità di garantire una concorrenza non falsata tra gli operatori economici, di agevolare la libera circolazione delle merci e di evitare differenze nel livello di tutela dei consumatori».

[15] In tal caso notificandone «il testo alla Commissione non oltre il 9 dicembre 2026».

[16] Queste misure «a) sono limitate a specifiche categorie di prodotti; b) sono giustificate da obiettivi di interesse pubblico; e c) sono proporzionate, in quanto sono idonee a garantire il raggiungimento degli obiettivi perseguiti e non vanno al di là di quanto è necessario per raggiungerli. Lo Stato membro che intenda introdurre o modificare una misura di cui al paragrafo 2 notifica alla Commissione il testo della misura proposta e fornisce una motivazione del modo in cui tale misura è conforme al paragrafo 3. La Commissione ne informa gli altri Stati membri. Entro sei mesi dal ricevimento di una notifica a norma del paragrafo 4, la Commissione può formulare un parere sul testo della misura proposta e sulla relativa motivazione, tenendo conto di eventuali osservazioni ricevute da altri Stati membri. Lo Stato membro che intenda introdurre o modificare tale misura la sospende per sei mesi a decorrere dalla notifica alla Commissione, a meno che quest'ultima non esprima il suo parere prima di tale termine».

[17] Per U. Carnevali, *Prevenzione*, cit., p. 11 ss. possono esserci prodotti che,

commercializzazione, si accerta che il prodotto è insicuro e vengono disattese le misure poc'anzi richiamate, il produttore può essere chiamato a risponderne civilmente, ma non in base alla speciale disciplina consumeristica, bensì secondo la categoria generale della responsabilità aquiliana di cui all'art. 2043 c.c.. Si hanno dunque due ambiti diversi, la cui violazione genera una responsabilità differenziata: se da un lato si deve garantire la sicurezza in qualsiasi momento, dall'altro per un prodotto che si scopre insicuro vanno adottate precauzioni al fine renderlo sicuro, per mezzo del ritiro dal mercato oppure del richiamo per operargli le opportune modifiche[18]. Seguendo tale logica, degli eventuali danni discendenti dall'inadempimento di siffatti obblighi si risponderebbe in base all'art. 2043 c.c.; diversamente, alcun danno risulterebbe risarcibile per i fatti verificati prima che il prodotto manifestasse la sua insicurezza[19].

Emerge quindi la differenza di disciplina, non ravvisandosi interferenze con quella del prodotto difettoso, poiché per quest'ultima il prodotto risulta insicuro già al momento della messa in circolazione: tale evidenza risultava dallo stato delle conoscenze tecniche e scientifiche[20], diversamente dalla disciplina sulla sicurezza, in cui il prodotto si scopre insicuro solo successivamente all'immissione in commercio.

---

pur presentando dei rischi – i quali ne determinano, per ciò solo, la pericolosità – non risultano difettosi: conseguentemente, è possibile (salvo ipotesi eccezionali) ritenere che un prodotto sicuro sia anche un prodotto non difettoso (ma non viceversa).

[18] Segnatamente, è la parte quarta del codice del consumo a dettare la normativa: per l'art. 104 cod. cons. «il produttore immette sul mercato solo prodotti sicuri […] adotta misure proporzionate in funzione delle caratteristiche del prodotto fornito per consentire al consumatore di essere informato sui rischi connessi» e, in particolare, fa controlli a campione e prevede misure di ritiro, richiamo, nonché di informazione per l'insicurezza dei prodotti. In particolare, per A. Albanese, *La sicurezza generale dei prodotti e la responsabilità del produttore nel diritto italiano ed europeo*, in *Eur. dir. priv.*, 4, 2005, p. 1002, la violazione di questi obblighi, «oltre a determinare sanzioni penali o amministrative, può peraltro rendere il produttore civilmente responsabile dei danni che siano eventualmente derivati dall'uso del prodotto anche in ipotesi che sarebbero altrimenti sottratte alla responsabilità oggettiva prevista dall'art. 114 cod. cons.» (poiché, ad esempio, si è dimostrata l'esimente del rischio da sviluppo).

[19] L'esistenza di un dubbio scientifico, secondo questa impostazione, non esclude la possibilità di rilevare una colpa del produttore che non ne abbia tenuto conto. Pertanto, il rischio di danno può assumere rilevanza giuridica in base all'art. 2043 c.c. all'esito di un giudizio di bilanciamento o includendo nel modello di condotta anche il dovere di non ignorare tale specie di rischio. Vd. sul punto R. Montinaro, *Dubbio scientifico, precauzione e danno da prodotto*, in *Resp. civ.*, 11, 2012, p. 725.

[20] Restando peraltro fuori dal campo di operatività del rischio da sviluppo.

Sarà interessante verificare poi come si comporterà il legislatore nel recepire la nuova direttiva, la quale si mostra sensibile alla definizione di prodotto difettoso nell'ottica dell'implementazione tecnologica. L'art. 7 della Direttiva (UE) 2024/2853, confermando quanto oggi disposto dall'art. 117 cod. cons., stabilisce che un prodotto è considerato difettoso se non offre la sicurezza che ci si può legittimamente attendere, tenuto conto di tutte le circostanze; tra queste, particolare rilevanza è riservata al software e agli aggiornamenti di questo, che costituiscono una deroga all'esonero della responsabilità di cui all'art. 11 della Direttiva (UE) 2024/2853.

1.2 *La norma di chiusura*

La normativa di cui all'art. 127 cod. cons. prevede in chiusura che «le disposizioni del presente capo non escludono né limitano i diritti che sono attribuiti al danneggiato da altre leggi». Sembrerebbe sussistere l'intenzione del legislatore di prevedere una clausola attraverso cui la produzione di beni insicuri possa, talvolta, rientrare in altre discipline nazionali, magari più rigorose sotto al profilo della responsabilità del produttore. In dottrina, ad esempio[21], si è fatto ampio riferimento allo svolgimento di attività pericolose, per la pericolosità derivante dalla insicurezza dei prodotti, soggiungendo il maggior rigore di cui alla fattispecie dell'art. 2050 c.c. Si è posto dunque il problema del concorso tra responsabilità del produttore per prodotto difettoso e responsabilità per lo svolgimento di attività pericolose. Come è stato opportunamente osservato[22], la responsabilità per

[21] Sul rischio ad esempio legato all'utilizzo dell'intelligenza artificiale, che opera come un sistema in grado di apprendere, vd. M. Scotto Di Carlo, *La responsabilità connessa all'utilizzo dei sistemi di intelligenza artificiale*, in *Danno resp.*, 4, 2024, p. 421 ss., il quale ritiene plausibile attrarre il danno eventualmente cagionato dall'elaboratore nell'orbita di quello scaturente dallo svolgimento di un'attività pericolosa, la definizione della quale risente dell'evoluzione della scienza e della tecnica. Altresì, F. Di Lella, *Le attività pericolose nel settore bio-medico. Spunti per una rilettura dell'art. 2050 c.c.*, Pisa, 2020, p. 47, per le attività nel settore biomedico, intende la fattispecie codicistica come «connaturata, inevitabile ed immanente nell'attività, ovvero presente nei mezzi – macchine, materiali, attrezzi o attrezzature complesse – considerati non semplicemente come cose statiche, ma nel dinamismo che li rende strumenti indispensabili all'esercizio della stessa». Conformemente A. Cioni, *L'influenza*, cit., p. 956 ss.

[22] Cfr. P. Trimarchi, *Rischio*, cit., p. 48, che definisce la responsabilità di cui all'art. 2050 c.c. come una «responsabilità oggettiva per rischio evitabile». Sul punto, M. Scotto Di Carlo, *La responsabilità*, cit., p. 421 ss. osserva che la responsabilità ai sensi dell'art. 2050 c.c. non è fondata sulla colpa, come evidenzia il collegamento tra l'imputazione del fatto dannoso e l'oggettiva causazione del pregiudizio nell'esercizio di un'attività pericolosa. Peraltro, il carattere obiettivo della responsabilità *de qua* sembra

attività pericolose è più rigorosa in quanto il riferimento alla totalità delle misure indurrebbe a ritenere questa una responsabilità oggettiva in cui si introduce una posizione qualificata dall'onere di adottare ogni tipo di misura, anche quelle forse sproporzionate; ciò significa che l'unico modo per liberarsi dalla responsabilità sarebbe dimostrare il caso fortuito. Opinare in tal modo significherebbe farvi rientrare pure l'onere di farsi carico del rischio da sviluppo.

Ulteriore corollario porterebbe quindi a condividere il coinvolgimento, in una fattispecie così architettata, del principio di precauzione, che onera il produttore, nell'ipotesi di sospetto circa il difetto di un prodotto, di adottare un freno consistente nel non mettere in circolazione il prodotto, quantomeno nell'attesa che la scienza faccia il suo corso. Su tali assunti, v'è chi ritiene[23] – valorizzando la norma per cui sono fatte salve le disposizioni che attribuiscono ulteriori diritti all'utilizzatore del prodotto difettoso – che questi possa far valere la responsabilità di cui all'art. 2050 c.c., ipotizzando quindi un concorso di responsabilità tra la disposizione codicistica e quella consumeristica.

Questa interpretazione è stata in verità esclusa dalla giurisprudenza comunitaria[24], che ha avuto modo di evidenziare come le disposizioni che rimangono fatte salve non possono essere quelle nazionali che configurano in capo al produttore un regime di responsabilità di natura oggettiva, derogatorio e più gravoso di quella prevista dalla direttiva, perché ciò significherebbe vanificare l'intento uniformante di quest'ultima. Non avrebbe senso, quindi, prevedere una direttiva per standardizzare i regimi di responsabilità, configurando così un regime

---

trasparire dalla prova liberatoria che dovrebbe fornire l'esercente per essere liberato dalla responsabilità, che consiste nella dimostrazione del «fatto tecnico», ossia dell'adozione della organizzazione preventiva di tutti gli accorgimenti tecnici idonei ad evitare il danno.

[23] Sul rinnovato interesse per il severo regime di responsabilità contemplato dall'art. 2050 c.c. cfr. E. Al Mureden, *La conformità dei prodotti agli standard tecnici tra tutela del consumatore e limiti alla responsabilità del fabbricante*, in *Act. jur. iber.*, 17, 2022, p. 892–911.

[24] Vd. Corte di Giustizia (causa C-183/00), in *curia.europa.eu*, la quale ha avuto modo di rilevare che «l'art. 13 della direttiva del Consiglio 25 luglio 1985, 85/374/CEE, relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri in materia di responsabilità per danno da prodotti difettosi, deve essere interpretato nel senso che i diritti attribuiti ai danneggiati a causa di un prodotto difettoso dalla normativa di uno Stato membro, in forza di un regime generale di responsabilità basato sullo stesso fondamento della disciplina attuata dalla suddetta direttiva, possono essere limitati o ristretti in seguito al recepimento di quest'ultima nell'ordinamento giuridico interno del suddetto Stato». L'intento di armonizzazione globale tra le discipline degli Stati membri è stato ribadito a più riprese: si cfr., ad esempio, Corte di Giustizia (causa C-52/00, C-154/00 e C-183/00), in *curia.europa.eu*.

di responsabilità presunta che presenta prove liberatorie tassative, e, al tempo stesso, consentire agli Stati membri di applicare alla stessa tipologia di danno una responsabilità più severa e rigorosa.

È possibile dunque domandarsi quali siano i diritti che rimangono salvi: attenta dottrina sul punto ha notato che sono, ad esempio, quelli contrattuali[25] – con la conseguenza che rimane salva la responsabilità contrattuale di chi ha venduto il prodotto, al di là del produttore –; oppure, come già notato in precedenza, l'ordinaria responsabilità civile[26] ai sensi dell'art. 2043 c.c.: fino a che non si accerta l'insicurezza del bene è possibile infatti far valere il rischio da sviluppo, mentre, successivamente, pur potendo non essere ritenuti responsabili secondo la disciplina consumeristica perché liberati, sorge l'obbligo di ritiro del prodotto viziato, sanzionabile in base all'art. 2043 c.c.

2. *La disciplina europea sulla sicurezza dei prodotti alimentari*

La centralità della disciplina emerge allora dal suo carattere trasversale, essendo applicabile ad ogni prodotto difettoso; non si ricava dall'analisi, infatti, una distinzione di categoria. Tuttavia, per quanto concerne il prodotto alimentare[27],

---

[25] Per un esame in chiave critica vd. N. Chiricallo, *Il "richiamo" dei prodotti pericolosi e i nuovi rimedi civilistici esperibili dall'acquirente-consumatore. L'art. 37 del Regolamento UE 2023/988 sulla sicurezza generale dei prodotti*, in *Nuove l. civ. comm.*, 3, 2024, p. 669 ss.

[26] Sul ricorso alle regole di diritto comune cfr. A. Fusaro, *Effetto avverso del farmaco: obblighi informativi e responsabilità*, in *Nuova giur. civ. comm.*, 5, 2021, p. 1145.

[27] Vd., senza pretesa di esaustività, E. Al Mureden, *La conformità*, cit.; P. Borghi, *Il rischio alimentare e il principio di precauzione*, in L. Costato, A. Germanò ed E. Rook Basile (a cura di), *Trattato di diritto agrario*, Milano, 2011, vol. III, , p. 53–73; F. Capelli, V. Silano e B. Klaus, *Nuova disciplina del settore alimentare e autorità europea per la sicurezza alimentare*, Milano, 2006; S. Carmignani, *Il ruolo del consumatore e le azioni di tutela*, in P. Borghi, I. Canfora, A. Di Lauro e L. Russo (a cura di), *Trattato di diritto alimentare italiano e dell'Unione Europea*, Milano, 2024, 2ª ed., p. 382 ss.; S. Carmignani, *Produzione e mercati degli alimenti nel diritto nazionale*, in *o.u.c.*, p. 121 ss.; A. D'Alessio, *La responsabilità del produttore di alimenti tra difetto e sicurezza del prodotto*, in *Resp. civ. prev.*, 6, 2018, p. 2016 ss.; M. Ferrari, *Digitalizzazione e strutture agricole*, in *Quad. riv. dir. al.*, fasc. XVII, 1, 2023, p. 46; A. Germanò - E. Rook Basile, *La sicurezza alimentare*, in *Il diritto alimentare tra comunicazione e sicurezza dei prodotti*, Torino, 2005, p. 275–312; G. Germanò, M.P. Ragionieri ed E. Rook Basile., *Diritto agroalimentare*, cit.; G. Vaccaro, *Il principio di precauzione e la responsabilità delle imprese nella filiera alimentare*, in *Riv. dir. al.*, fasc. IX, 4, 2015, p. 50 ss.

stanti le diverse caratteristiche peculiari insite, occorre verificarne la compatibilità al fine pure di evidenziarne eventuali rilievi critici[28]. Tra le circostanze di cui occorre anzitutto tener conto per valutare la sicurezza v'è quella attinente al periodo di tempo coincidente con l'immissione sul mercato ed il deterioramento derivante dall'uso prolungato. Questo a ben vedere mal si concilia con un prodotto destinato all'alimentazione, che anzitutto non è suscettibile di un uso prolungato, in quanto è proprio con l'uso che si consuma e, inoltre, se consumato entro la data consigliata, non pare lambito dal lasso di tempo intercorrente tra l'immissione e il deterioramento[29].

La destinazione al nutrimento del prodotto comporta anche un'ulteriore conseguenza. Nell'ipotesi in cui l'evento dannoso si verifichi a seguito del consumo di un prodotto alimentare difettoso, grava infatti sul danneggiato l'onere di dimostrare il difetto. Considerato che per la giurisprudenza italiana la prova del difetto è raggiunta laddove l'attore dimostri di aver subito il danno in occasione dell'utilizzazione normale del prodotto, è ragionevole dedurre che per il prodotto alimentare, cui il consumo ne determina irrimediabilmente la scomparsa, prova siffatta potrebbe risultare maggiormente complessa, potendosi opinare, in tal senso, un giudizio giurisprudenziale fondato unicamente su presunzioni[30].

Vi è poi l'ipotesi di esclusione della responsabilità del produttore che assume una particolare rilevanza per la produzione e circolazione dei prodotti alimentari[31]: la disciplina di matrice comunitaria non solo quasi si disinteressa della condotta «post commercializzazione» del produttore ma, come visto, per mezzo del rischio da sviluppo, sembra in molti casi alterare ogni possibile funzione deterrente della responsabilità, disincentivando, in particolare, gli investimenti relativi alla ricerca da parte produttore[32]. Concepire coordinate così congegnate

---

[28] Così A. D'Alessio, *La responsabilità*, cit., p. 217.

[29] A. Germanò, *Prodotti*, cit., p. 535.

[30] A. Germanò, *o.u.c.*, p. 536.

[31] Cfr. M. Mazzo, *Il codice del consumo e la questione delle definizioni generali e speciali di produttore*, in *Riv. dir. agr.*, 1, 2007, p. 65–74.

[32] È evidente che la regola di responsabilità si prefigge di svolgere una funzione preventiva e di garantire la sicurezza dei prodotti, nella misura in cui la previsione dell'obbligo di risarcire l'eventuale danno cagionato dall'uso di un prodotto difettoso dovrebbe indurre il soggetto responsabile a adottare misure idonee per evitare l'immissione sul mercato di prodotti non sicuri, ossia pericolosi. Vi sono peraltro delle situazioni, osserva A. Albanese, *La sicurezza*, cit., p. 980 ss., in cui la norma sulla responsabilità non riesce a svolgere questa funzione in modo efficiente. Può difatti accadere che il produttore ritenga più conveniente accettare il rischio di dover risarcire i danni eventualmente provocati piuttosto che sopportare i costi funzionali a rendere sicuri i prodotti. Per eliminare o attenuare il rischio il produttore dovrebbe comunque

permette di ipotizzare come il produttore, rassicurato dallo scudo dell'esimente, possa non considerarsi stimolato a migliorare il livello complessivo delle conoscenze scientifiche relative al proprio prodotto, così da aumentare la sicurezza e minimizzare i rischi per i consumatori. La direttiva in questo modo si dimostra parzialmente incapace di assicurare una reale protezione dei consumatori anche nel caso in cui il danno non fosse noto o prevedibile al momento dell'immissione in commercio del prodotto[33].

---

effettuare controlli o adottare misure per evitare difetti che possono rendere il prodotto pericoloso. Lo sforzo che il produttore deve compiere in tal senso viene determinato in base ad un calcolo economico di opportunità. In questa analisi il produttore può anche valutare la convenienza di una polizza assicurativa per la responsabilità civile, in modo tale che il premio pagato alla compagnia assicurativa tramuti il rischio del risarcimento in un costo certo. In caso di assicurazione risulterebbe quindi soddisfatto l'interesse patrimoniale del consumatore ad ottenere il risarcimento del danno, ma non adeguatamente tutelato l'interesse primario a non subire il danno, in quanto l'obbligo di risarcimento posto a carico del produttore potrebbe non rappresentare un deterrente sufficiente per indurlo a rendere più sicuri i prodotti.emanato in attuazione della direttiva 95/2001, ha introdotto nel nostro ordinamento una normativa alla sicurezza generale dei prodotti.

[33] A. Germanò, *Prodotti*, cit., p. 536; A. Cioni, *L'influenza indiretta del diritto europeo: il caso dei danni cagionati dai prodotti pericolosi. Spunti per una riscoperta dell'articolo 2050 c.c.*, in *Riv. dir. civ.*, n. 5, 2023, p. 956 ss. Secondo R. Montinaro, *Responsabilità del produttore di farmaci, art. 2050 c.c. e gestione precauzionale del rischio*, in *Resp. civ. prev.*, 5, 2019, p. 1587–1608, il legislatore, nella disciplina speciale del danno da prodotto ha inteso distinguere la responsabilità del produttore da forme di responsabilità da rischio d'impresa, basate unicamente sul nesso di causalità tra prodotto e danno. La valutazione sul carattere difettoso del prodotto, infatti, deve operarsi in base ad una prospettiva *ex ante*, per cui si richiede al produttore solamente di avere riguardo allo sviluppo tecnico-scientifico in essere al tempo della commercializzazione, ma non anche dei successivi incrementi delle conoscenze e delle capacità tecniche. La libertà concessa dalla Direttiva 374/1985/CEE agli Stati membri di scegliere se inserire o meno l'esimente è stata originariamente mossa dal timore che far ricadere sul produttore il rischio da sviluppo potesse scoraggiare, da un lato, la ricerca sui rischi di danno, e, dall'altro, l'introduzione di beni utili, ma implicanti un certo grado di pericolo di effetti collaterali (si pensi ai farmaci). L'A. nota come sorgano perplessità nella misura in cui, anzitutto, dalla disciplina derivino delle difficoltà interpretative legate all'applicazione dell'esimente. È poi apparso evidente il disallineamento tra la previsione, che assume come punto temporale di riferimento l'immissione del prodotto in commercio, e le discipline speciali sulla sicurezza dei prodotti, che dispongono anche per la fase successiva doveri di monitoraggio, vigilanza e controllo, funzionali alla acquisizione di conoscenze ulteriori sui rischi collegati all'uso del prodotto ed alla loro gestione. L'esimente in questione può quindi tradursi in un disincentivo per i produttori a adoperarsi al fine di innalzare il grado di sicurezza del prodotto, rassicurati dall'*escamotage* garantita dalla disposizione,

Sebbene poi la prima formulazione della direttiva lasciasse liberi gli Stati membri di estenderla, questa in origine lasciava fuori dal suo ambito di applicazione «i prodotti agricoli naturali», ossia i prodotti dell'agricoltura, della caccia e della pesca che non avessero subito una trasformazione. Ciò in ragione di una ritenuta intrinseca sicurezza del prodotto agricolo[34], che venne successivamente superata dall'avvento di crisi alimentari[35], che indussero il legislatore europeo ad intervenire estendendo la disciplina anche al prodotto agricolo per mezzo della Direttiva 99/34/CEE[36]. L'estensione pedissequa ad un'entità così peculiare dovrebbe suggerire l'analisi della sicurezza relativa al prodotto alimentare naturale, che potrebbe essere reputato difettoso a seguito delle implementazioni tecnologiche o biotecnologiche: l'esimente del rischio da sviluppo[37], in questo caso, potrebbe trovare più ampi margini di applicazione per i danni da prodotti alimentari dell'agricoltura, per i quali i rischi da sviluppo costituiscono la principale causa di difetto.

Il regime di decadenza prevede inoltre un termine di dieci anni dalla messa in circolazione del prodotto, che irrimediabilmente ha l'effetto di escludere la risarcibilità dei danni a lungo termine[38]. Un modello simile di responsabilità rischia

---

con la conseguenza paradossale di lasciare i danneggiati sguarniti di adeguata tutela in un ambito in cui questa appare necessaria, per via dell'intensità dei rischi che il prodotto pone rispetto ad un bene giuridico di rilevanza primaria, quale la salute.

[34] A. Germanò, *Prodotti*, cit., p. 536.

[35] A. D'Alessio, *La responsabilità*, cit., p. 2030; D. Romano, *La coltivazione*, cit.

[36] Per una analisi vd. G. Alpa, *La Comunicazione N. 398/2001/CE sulla armonizzazione del diritto privato. Una premessa al dibattito*, in *Nuova giur. civ. comm.*, 5, 2001, p. 425 ss.

[37] Vd. l'art. 7 della Direttiva 85/374/CEE, secondo cui «il produttore non è responsabile ai sensi della presente direttiva se prova: a) che non ha messo il prodotto in circolazione; b) che, tenuto conto delle circostanze, è lecito ritenere che il difetto che ha causato il danno non esistesse quando l'aveva messo in circolazione o sia sorto successivamente; c) che non ha fabbricato il prodotto per la vendita o qualsiasi altra forma di distribuzione a scopo economico, né l'ha fabbricato o distribuito nel quadro della sua attività professionale; d) che il difetto è dovuto alla conformità del prodotto a regole imperative emanate dai poteri pubblici; e) che lo stato delle conoscenze scientifiche e tecniche al momento in cui ha messo in circolazione il prodotto non permetteva di scoprire l'esistenza del difetto; f) nel caso del produttore di una parte componente, che il difetto è dovuto alla concezione del prodotto in cui è stata incorporata la parte o alle istruzione date dal produttore del prodotto».

[38] L'art. 11 della Direttiva 85/374/CEE prevede infatti che «i diritti conferiti al danneggiato in applicazione della presente […] si estinguono alla scadenza di dieci anni dalla data in cui il produttore ha messo in circolazione il prodotto che ha causato il danno, a meno che il danneggiato non abbia avviato, durante tale periodo, un procedimento

dunque di risultare limitatamente efficace per le ipotesi di danno da prodotto alimentare immediato, quali intossicazioni o avvelenamenti, mentre, invece, per le ipotesi più gravi dei danni a lungo termine, determinati dall'eventuale bioaccumulo di sostanze non immediatamente nocive, non troverebbe applicazione.

Nondimeno, una maggiore sensibilità da parte del legislatore europeo nei confronti della posizione dei consumatori si è avuta con l'adozione del Regolamento (CE) del Parlamento europeo e del Consiglio n. 178/2002[39], del 28 gennaio 2002, in cui emergono dati rilevanti con riguardo alla definizione di prodotto non sicuro, al novero dei doveri in capo ai privati e alla menzione espressa del principio di precauzione[40]. Analizzandone il profilo funzionale, appare come

giudiziario contro il produttore».

[39] Il regolamento, nonostante sia testualmente relativo alla cd. *food safety*, è concepito come una sorta di "legislazione alimentare generale" (così è rubricato il Capo II) e quindi come una legge quadro del diritto alimentare, cui conformarsi in vista dell'adozione di norme successive da parte dell'Unione europea e dei singoli Stati membri (art. 4). Questo si prefigge molteplici finalità, tra cui la garanzia di "un livello elevato di tutela della salute umana e degli interessi dei consumatori in relazione agli alimenti, tenendo conto in particolare della diversità dell'offerta di alimenti, compresi i prodotti tradizionali, garantendo al contempo l'efficace funzionamento del mercato interno" (art. 1, parr. 1-2). Vd. M. Ramajoli, *La giuridificazione del settore alimentare*, in *Dir. amm.*, 4, 2018, p. 657.

[40] Tuttavia, secondo P. Borghi, *Il rischio*, cit., p. 53 ss., l'impostazione del legislatore appare poco precauzionale. Dalla lettura dell'art. 7 paiono derivano mere facoltà per gli Stati membri e per le Istituzioni comunitarie, le quali «*possono* essere adottate le misure *provvisorie* di gestione del rischio necessarie *in attesa* di ulteriori informazioni scientifiche per una valutazione più esauriente del rischio». La norma manifesta cautela e stride con un contesto caratterizzato da norme stringenti (si pensi al divieto di immissione sul mercato di prodotti che non rientrano nei requisiti di sicurezza delineati dagli artt. 14 e 15, agli obblighi di ritiro del prodotto dal mercato, di creazione di un sistema di tracciabilità, alla presunzione di pericolosità dell'intero lotto). La fisionomia che il principio di precauzione assume nel regolamento è allora tale da condurre verso un certo affievolimento della tutela, in presenza dell'incertezza scientifica del rischio alimentare. Infatti, in presenza di rischio, il regolamento, sebbene dica di non ignorare l'esistenza dell'incertezza, non dice nulla sulle caratteristiche che tali dubbi devono avere per assumere rilievo giuridico. Se ne trae allora la conseguenza che Stati e Istituzioni possono adottare misure proporzionate ma limitate e transeunti. La conseguenza della scarsa delineazione del principio emerge peraltro dall'analisi della giurisprudenza della Corte di Giustizia: dall'approccio del giudice comunitario pare derivare che una misura preventiva può essere adottata esclusivamente qualora il rischio, senza che la sua esistenza e la sua portata siano dimostrate pienamente da dati scientifici concludenti, appaia nondimeno sufficientemente documentato sulla base di dati scientifici al momento della adozione di tale misura. Vd. pure A. D'Alessio, *La*

questa possa porsi in coordinamento con la già citata Direttiva 85/374/CE. Tuttavia, mentre il regolamento, intervenendo prima che si produca il danno, tende ad individuare una serie di doveri che investono tanto i soggetti pubblici quanto i soggetti privati, la disciplina della responsabilità per danno da prodotto difettoso resta deputata ad operare successivamente, stabilendo le condizioni attraverso le quali attivare lo strumento risarcitorio, con tutti i limiti che, poc'anzi evidenziati, restano tali.

La recente direttiva prevede peraltro ulteriori novità. Sul piano probatorio, l'art. 10 della Direttiva (UE) 2024/2853 dispone che qualora l'attore incontri «difficoltà eccessive, […] a causa della complessità tecnica o scientifica, nel provare il carattere difettoso del prodotto o il nesso di causalità tra il carattere difettoso e il danno o entrambi» l'organo giurisdizionale possa presumere «il carattere difettoso del prodotto o il nesso di causalità tra il carattere difettoso e il danno». Il termine di decadenza poi, innovato nell'ottica di assicurare un maggiore *favor* verso l'utilizzatore, è aumentato, in deroga a quello ordinario di dieci anni, a venticinque anni per il danno lungolatente[41].

Alla luce comunque delle osservazioni svolte sul piano del danno, emerge come attualmente, con riferimento ai difetti ignoti al tempo della commercializzazione, al regime decadenziale, alle peculiarità presenti nel prodotto alimentare, la normativa europea presenti talune ipotesi da cui ravvisare la totale irresponsabilità del produttore, che sono da considerare quantomeno in parte irragionevoli. La normativa al momento in vigore pare sacrificare la garanzia ad una reale protezione dei consumatori sull'altare della massimizzazione dei traffici, presentando un bilanciamento che non tiene in considerazione valori fondamentali di cui l'intero impianto consumeristico si fonda, quali la tutela del contraente debole, che trova addentellato costituzionale nel principio solidaristico e di uguaglianza sostanziale di cui agli artt. 2 e 3, c. 2, Cost.

3. *Il ricorso a tecnologie avanzate*

L'esimente del rischio da sviluppo esclude la responsabilità del produttore anche quando nella fabbricazione del prodotto questi si avvalga di strumenti di tecnologia innovativa, potendo dimostrare che il difetto del prodotto non era conoscibile al momento della sua messa in circolazione, anche applicando la migliore tecnologia disponibile, benché questa sia in grado di dotare il produttore

responsabilità, cit., p. 2027.

[41] Vd. il commento di M. Bujalski, *On Producers 'Obligation to Repair Defective Goods: Direct Producers' Liability vs. Self-Standing Obligation under R2R Directive*, in *Journal of European Consumer and Market Law*, 4, 2024, p. 178–184.

stesso di competenze rafforzate, funzionali alla previsione e catalogazione di quei rischi che, non ancora accertati scientificamente e solo sospetti, consentono però una prognosi più attendibile di pericolosità del prodotto.

La problematica non è nuova nel panorama giuridico nazionale. Il continuo stagliarsi nel sistema del danno da prodotto conforme e le conseguenti limitazioni della tutela del danneggiato, in ossequio all'interpretazione data alla disciplina di cui agli artt. 114 ss. cod. cons., hanno costituito il presupposto per valorizzare una lettura dell'art. 2050 c.c. funzionale a moderare l'eccessivo rigore dell'orientamento che oggi permette diverse «vie di fuga» al produttore. In questo senso erano stati considerati pericolosi e attratti entro la disciplina codicistica prodotti quali bombole a gas, derivanti del tabacco, fuochi d'artificio e farmaci[42]. Ciò aveva permesso di ricondurre nell'alveo della fattispecie profili attinenti ai rischi che non era possibile prendere in considerazione nel momento in cui la sicurezza del prodotto era stata valutata e dei profili di dannosità noti e inclusi nell'ambito dei rischi ragionevolmente correlati all'uso del prodotto.

È stato evidenziato, nondimeno, come la lettura dell'art. 2050 c.c., benché giustificata dalla necessità di individuare contesti nei quali le esigenze di protezione della persona debbano reputarsi meritevoli di un rafforzamento della tutela risarcitoria, trovi un limite nella misura in cui si ponga in contrasto con l'obiettivo di armonizzazione manifestato a più riprese dal diritto dell'Unione europea e consolidato dalle molteplici pronunce della Corte di Giustizia, che ha avuto modo di denunciare ogni tipo di disallineamento recante un *vulnus* al valore dell'armonizzazione[43].

D'altronde, l'assunto per cui una regola generale secondo la quale la conformità agli standard legislativi sovranazionali rappresenta un limite alla statuizione della responsabilità del produttore entro i regimi della responsabilità oggettiva codicistica è tenuto in considerazione dalla Corte di Cassazione, consapevole, da una parte, che vi siano esigenze condivisibili[44], e, dall'altra, che sia oggetto di

---

[42] E. Al Mureden, *La conformità*, cit., p. 902.

[43] Al Mureden, *o.u.c.*, p. 903. In senso critico vedi il commento a Corte di Giustizia, 25/04/2002, nn. 52 e 154 effettuato da A. Palmieri - R. Pardolesi, *Difetti del prodotto e del diritto privato europeo*, in *Foro it.*, IV, 2002, p. 300, i quali rilevano le contraddizioni derivanti dalle pronunce della giurisprudenza europea, che da un lato ammette che lo Stato membro intervenga al fine di diminuire il livello di tutela del consumatore, mentre dall'altro impedisce l'estensione del regime di responsabilità ad aree prive di copertura.

[44] Che tuttavia vengono ad affiancarsi e non si sostituiscono alla disciplina dettata dall'ordinamento interno (vd. Cass., 1/6/2010, n. 13432; Cass., 29/4/2005, n. 8981; Cass., 7/11/2019; n. 28626; Cass., 7/3/2019, n. 6587, in *Onelegale*), non rimanendo pertanto da quella del codice del consumo esclusa, stante la diversità di *ratio* e ambito

più ampio respiro per mezzo dell'armonizzazione da parte del diritto dell'Unione europea, che riconduce il regime di responsabilità ad una fattispecie comune a tutti gli Stati membri[45].

Sarebbe opportuno, a ben vedere, che, stanti le peculiarità insite in ogni categoria di prodotti considerata, si promuovesse un diverso e nuovo approccio che introduca un regime di responsabilità oggettiva, diretta a porre sul produttore il costo del danno provocato dall'utilizzo del prodotto difettoso, con una delimitazione ad alcuni settori, come quello alimentare, oppure all'utilizzo di tecnologie avanzate idonee a fornire attendibili previsioni di rischio. Sul punto, peraltro, si ravvisa una sempre più accentrata sensibilità in ordine alla specificazione normativa del prodotto sotto il profilo merceologico; ricondurre ciascuno di questi beni all'interno di una specifica disciplina che ne governa la sicurezza risulta pregnante, in particolare, nei settori in cui si ravvisa la presenza di prodotti cosiddetti *borderline*[46].

3.1 *L'IA nel settore alimentare: prospettive future*

L'intelligenza artificiale viene sempre più adoperata nel settore alimentare per migliorare i processi produttivi, ottimizzare le risorse e sviluppare i prodotti evolutivi[47]; ne sono un esempio la carne coltivata in laboratorio – in cui l'intelligenza artificiale viene adoperata per analizzare e ottimizzare la crescita delle cellule –, gli alimenti a base vegetale alternativi alla carne – ove viene impiegata per analizzare le proteine vegetali, i grassi e altri ingredienti, combinandoli in modo da ottenere il gusto e la consistenza della carne – o, ancora, il vino e le bevande fermentate – per i quali gli algoritmi monitorano i parametri di fermentazione, come temperatura, pH e tempo, per assicurare che il sapore sia ottimale. Queste

applicativo, l'operatività (anche) della norma di cui all'art. 2050 c.c.

[45] E. Al Mureden, *La conformità*, cit., p. 903.

[46] Sono quei prodotti che, per loro natura, non sono immediatamente riconducibili ad un determinato settore, per cui quindi è difficile definire quale sia la normativa di riferimento da applicare. La rilevanza assunta da una corretta qualificazione è stata recentemente ribadita dal Reg. 2017/745/UE che, nel disciplinare i dispositivi medici, sottolinea le rilevanti peculiarità che caratterizzano questa tipologia di prodotti ed impediscono di estendere l'applicazione della disciplina ad essi dedicata agli alimenti (Reg. 2002/178/CE) ed ai cosmetici (Reg. 2009/1223/ CE). E. Al Mureden, *La conformità*, cit., p. 903.

[47] Per un approfondimento su tali tecniche vd. N.J. Watson, A.L. Bowler, A. Rady, O.J. Fisher, A. Simeone, J. Escrig, E. Woolley, A.A. Adedeji, *Intelligent Sensors for Sustainable Food and Drink Manufacturing*, in *Front. Sustain. Food Syst.*, 5, 2021.

sono solo alcune ipotesi che mostrano come l'intelligenza artificiale stia non solo rivoluzionando i metodi di produzione, ma anche influenzando le proprietà, il gusto e la qualità degli alimenti, portando alla creazione di prodotti innovativi che cercano di rispondere a nuove esigenze etiche, ambientali e di consumo. Nel caso dunque di prodotti alimentari realizzati ricorrendo a simili procedure, la esaminata disciplina rischia di diventare effettivamente troppo favorevole per il produttore[48].

Nello specifico, le tecnologie basate sull'intelligenza artificiale sono in continua evoluzione e presentano dei profili di complessità in grado di generare errori o difetti nascosti, difficili da individuare; allo stesso tempo, inoltre, la natura dell'alimento richiederebbe *ex se* uno standard di tutela particolarmente elevato per le evidenti ricadute dalla destinazione d'uso sulla salute dei consumatori. Consentire, in questa direzione, al produttore di alimenti di non rispondere in caso di danni derivanti dal rischio da sviluppo rischierebbe di ridurre eccessivamente il livello di tutela dei consumatori in un campo dove invece la sicurezza è fondamentale. Sicché, l'eventuale riconduzione della casistica nell'alveo della fattispecie di cui all'art. 2050 c.c. potrebbe aumentare lo standard di tutela dei consumatori e valorizzare il contenuto del Regolamento CE n. 178/2002 in cui si fa espresso riferimento al principio di precauzione[49]. Questo, che impone agli

[48] Per G. Votano, *Intelligenza artificiale in ambito sanitario: il problema della responsabilità civile*, in *Danno resp.*, 6, 2022, p. 677 ss., in particolare, «è legittimo dubitare che l'attuale quadro giuridico sia idoneo a coprire i danni causati dalla nuova generazione di dispositivi intelligenti, soprattutto alla luce della circostanza che detti sistemi sono dotati di capacità di auto-apprendimento che implicano un certo grado di imprevedibilità nel loro comportamento (essendo capaci di "imparare" in modo autonomo, in base alle specifiche esperienze e all'interazione con l'ambiente). E ciò rende particolarmente difficile (se non proprio impossibile) fornire la prova dell'esistenza di un difetto di funzionamento eziologicamente connesso al danno subito, con conseguente impossibilità di ottenere il risarcimento dei danni subiti».

[49] L'art 7 del Reg. 2002/178/CE, rubricato «Principio di precauzione», stabilisce che «qualora, in circostanze specifiche a seguito di una valutazione delle informazioni disponibili, venga individuata la possibilità di effetti dannosi per la salute ma permanga una situazione d'incertezza sul piano scientifico, possono essere adottate le misure provvisorie di gestione del rischio necessarie per garantire il livello elevato di tutela della salute che la Comunità persegue, in attesa di ulteriori informazioni scientifiche per una valutazione più esauriente del rischio. Le misure adottate sulla base del paragrafo 1 sono proporzionate e prevedono le sole restrizioni al commercio che siano necessarie per raggiungere il livello elevato di tutela della salute perseguito nella Comunità, tenendo conto della realizzabilità tecnica ed economica e di altri aspetti, se pertinenti. Tali misure sono riesaminate entro un periodo di tempo ragionevole a seconda della natura del rischio per la vita o per la salute individuato e del tipo di informazioni scientifiche necessarie per

operatori del settore alimentare di prevenire rischi incerti per la salute pubblica, adottando misure rigorose e preventive in assenza di certezze scientifiche, ben si combinerebbe con un regime di responsabilità oggettiva[50] per chi esercita un'attività pericolosa; in particolare, responsabilità siffatta imporrebbe al produttore l'obbligo di rispondere dei danni causati dai propri prodotti, indipendentemente dalla prevedibilità del rischio o dall'esistenza di conoscenze tecniche al momento della immissione nel mercato. Non vi sarebbe dunque la possibilità per il produttore di liberarsi provando il rischio da sviluppo, il quale, ad uno sguardo attento, oltre a ad essere cosa diversa dal caso fortuito, in quanto non si tratta di un evento esterno e imprevedibile ma di un elemento intrinseco al prodotto, può altresì entrare in contrasto con l'ascritto principio di precauzione, poiché consente di evitare la responsabilità per rischi che non potevano essere previsti in base allo stato della scienza e della tecnica al momento della produzione. Tale esimente, quindi, impedisce di configurare in capo ai produttori un atteggiamento pienamente precauzionale, coerentemente con l'approccio del Regolamento CE n. 178/2002, che pone la salute dei consumatori come priorità assoluta e postula la recisione dei rischi per la sicurezza alimentare alla fonte.

La responsabilità oggettiva potrebbe poi incentivare una maggiore vigilanza, influenzando i produttori che si avvalgono di tecniche di intelligenza artificiale a adottare dei protocolli di monitoraggio e controllo più rigorosi, poiché non sarebbe possibile difendersi appellandosi alla mancanza di conoscenza del difetto; sarebbero così spinti a seguire attivamente gli sviluppi scientifici e tecnologici al fine di prevenire ogni tipo di rischio, anche potenziale[51].

---

risolvere la situazione di incertezza scientifica e per realizzare una valutazione del rischio più esauriente».

[50] Pertinenti sul punto si rivelano le osservazioni di G. D'Amico, *La responsabilità contrattuale: attualità del pensiero di Giuseppe Osti*, in *Riv. dir. civ.*, 1, 2019, p. 1 ss. Cfr. pure G. Osti, *Scritti*, cit., *passim*; Id., *Contratto*, in *Nov. dig. it.*, 1968, *passim*.

[51] Cfr. Risoluzione del Parlamento europeo del 16 febbraio 2017, in *eur-lex.europa.eu*, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL), in particolare par. 56 sui Principi generali riguardanti lo sviluppo della robotica e dell'intelligenza artificiale per uso civile, in cui si ritiene che, in linea di principio, «una volta individuati i soggetti responsabili in ultima istanza, la loro responsabilità dovrebbe essere proporzionale all'effettivo livello di istruzioni impartite al robot e al grado di autonomia di quest'ultimo, di modo che quanto maggiore è la capacità di apprendimento o l'autonomia di un robot e quanto maggiore è la durata della formazione di un robot, tanto maggiore dovrebbe essere la responsabilità del suo formatore; osserva in particolare che, nella determinazione della responsabilità reale per il danno causato, le competenze derivanti dalla "formazione" di un robot non dovrebbero essere confuse con le competenze che dipendono strettamente dalle sue abilità di autoapprendimento; osserva che, almeno nella fase attuale, la responsabilità

Si potrebbe osservare che già oggi il principio di precauzione introdotto dall'ordinamento eurounitario condurrebbe a concepirlo come innervante non solo la fase antecedente all'immissione, ma anche quella successiva. Benché riguardi in primo luogo le misure preventive che un produttore o distributore deve adottare per garantire che i prodotti siano sicuri prima che vengano immessi sul mercato, il principio di precauzione impone agli stessi di monitorare continuamente i rischi associati ai loro prodotti anche dopo la commercializzazione, per mezzo pure del ricorso a strumenti di ritiro o modifica laddove emergano rischi per la salute. È altresì vero, tuttavia, che la responsabilità presunta di cui al codice del consumo consente al produttore di liberarsene dimostrando il rischio da sviluppo, nonostante l'apparente rispetto del principio di precauzione e delle conoscenze scientifiche disponibili all'epoca. Pertanto, se un difetto emerge successivamente alla commercializzazione e il produttore riesce a dimostrare che quel difetto era impossibile da conoscere, non è ritenuto responsabile per i danni prodotti sino a quel momento.

Il rischio da sviluppo rappresenta quindi un canale di indebolimento del principio di precauzione, in quanto, concedendo ai produttori un margine di esonero per difetti imprevedibili, può creare una zona grigia di rischio; segnatamente, mentre il principio di precauzione richiede cautele e misure preventive stringenti anche in presenza di incertezze scientifiche, il rischio da sviluppo ammette una difesa basata sull'impossibilità tecnica di prevedere il difetto. Per tali ragioni, anche alla luce delle summenzionate intenzioni del legislatore europeo, per valorizzare massimamente il profilo di tutela del consumatore, in un ambito così delicato come quello del diritto alimentare, parrebbe opportuno configurare un regime di responsabilità più severo, in particolare per quei produttori che, avvalendosi di tecniche di intelligenza artificiale, si dotano di strumenti suscettibili di implementare le competenze in ordine ai rischi potenzialmente insiti al prodotto.

L'esimente può in definitiva diminuire il grado di tutela dei consumatori, specialmente nei casi in cui le conoscenze scientifiche e tecniche siano in continua evoluzione. Saper di poterla invocare può influire sull'incentivo per i produttori a investire in standard di sicurezza ulteriori a quelli richiesti dalla normativa corrente, sull'immissione nel mercato di un prodotto innovativo senza essere pienamente certi della sua sicurezza a lungo termine e, infine, sulla eventuale anticipazione di possibili rischi derivanti da tecnologie e sostanze non ancora studiate. Rappresentando, in tale ottica, una scappatoia legale per evitare la responsabilità in caso di danni futuri derivanti da innovazioni i cui rischi erano sconosciuti al momento della commercializzazione, costituisce in un certo senso un limite in ordine alla piena efficacia del principio di precauzione nel proteggere

---

deve essere imputata a un essere umano e non a un robot».

i consumatori, perché ammette l'esistenza di un margine di rischio accettabile per i prodotti immessi sul mercato.

Una soluzione simile potrebbe da ultimo configurarsi in seguito, complici le recenti normative unionali in tema di responsabilità per danno da prodotti difettosi. L'Unione europea è, come già accennato, intervenuta recentemente con la Direttiva (UE) 2024/2853, la quale, nell'ottica di abrogare la Direttiva 85/374/CEE, in relazione al rischio da sviluppo ammette che, a partire dalla considerazione secondo cui si tratti di «una limitazione indebita della protezione delle persone fisiche», uno Stato membro possa «derogare a tale possibilità introducendo nuove misure o modificando quelle esistenti, al fine di estendere la responsabilità in tali situazioni a specifici tipi di prodotti se ciò è ritenuto necessario, proporzionato e giustificato da obiettivi di interesse pubblico, come quelli enunciati nel trattato sul funzionamento dell'Unione europea[52]». In ordine poi agli ultimi interventi in tema di intelligenza artificiale – tra cui si segnala il Regolamento (UE) 2024/1689 (noto come AI Act[53]) – per la quale l'Unione europea stabilisce regole per l'uso di tali sistemi, classificando i rischi, e sulle cui basi si ricava la necessità configurare forme di responsabilità per coloro che si avvalgono di sistemi di intelligenza artificiale, è plausibile ipotizzare la realizzazione di una combinazione tra discipline che opti verso una graduale eliminazione dell'esimente in luogo di un regime di responsabilità oggettiva, laddove non si reputi più giustificabile il rischio da sviluppo in un contesto in cui l'uso di tecnologie avanzate permette al produttore di raccogliere, analizzare e monitorare in modo più efficace i dati per anticipare potenziali difetti o rischi, rendendo difficile sostenere l'imprevedibilità di un difetto.

---

[52] Così il *Considerando* n. 59 della Direttiva (UE) 2024/2853, che statuisce poi il ricorso alla deroga all'esonero da responsabilità basato sui rischi da sviluppo tramite notifica alla Commissione, che può emettere sulla questione «pareri non vincolanti sulle misure o modifiche proposte». Si noti il differente tenore della lettera rispetto alla precedente Direttiva 85/374/CEE, che ammetteva tale deroga solo a condizione che fosse subordinata «ad una procedura di statu quo comunitaria per aumentare, se possibile, in modo uniforme il grado di protezione della Comunità». Rilevante altresì il *Considerando* n. 51 della Direttiva (UE) 2024/2853, che stabilisce come sia «opportuno limitare la possibilità che gli operatori economici si sottraggano alla responsabilità provando che il difetto è sopravvenuto dopo il momento dell'immissione sul mercato o della messa in servizio del prodotto nel caso in cui il difetto di un prodotto consista nella mancanza di aggiornamenti o migliorie del software necessari per rimediare a vulnerabilità in materia di cibersicurezza e mantenere la sicurezza del prodotto».

[53] Cfr. A. Gentili, *Regole per l'intelligenza artificiale*, in *Contr. impr.* 4, 2024, p. 1043 ss.

Sezione IV

IA E CATEGORIE GENERALI DEL DIRITTO

Smart contract: auto-esecuzione delle prestazioni e rapporto obbligatorio

di **Giacomo Angelo Puggioni**

Sommario: 1. Limitazione del campo di indagine: cenni sui contratti cibernetici. – 2. Il problema definitorio. – 3. L'auto-esecuzione: quali legami con l'ordinamento giuridico?

1. *Limitazione del campo di indagine: cenni sui contratti cibernetici*

La tecnologia agevola l'operare umano, tendente a conformarsi al principio del minimo mezzo, in ragione del quale – a parità di risultati – i consociati sono orientati a eleggere il meccanismo che comporta minori costi, in termini di tempo, denaro ed energie. Gli studi sugli *smart contracts*, condividendone parzialmente le problematiche, si inseriscono nelle ricerche sugli automi nel diritto privato – quali strumenti aventi la «proprietà di sostituire e estendere l'attività umana»[1] – ma le peculiarità riconducibili ai c.d. contratti intelligenti, specie nel loro operare in sinergia con le tecnologie basate su registri distribuiti[2], vi riservano uno spazio d'autonomia concettuale e correlati specifici interrogativi di rilevanza giuridica. Prima di misurarci con questi ultimi, nondimeno, nell'ambito di una raccolta di contributi dal tema "*Intelligenza artificiale, dati e diritto*", è doveroso un preliminare lavoro di regolamento di confini. Infatti, i meccanismi

---

[1] A. Cicu, *Gli automi nel diritto privato*, in *Il Filangieri*, Milano, 1901, p. 561 ss., ove si rinviene ampia bibliografia relativa alla dottrina tedesca del XIX secolo sul tema. Nella letteratura giuridica italiana del primo '900 si segnala anche A. Scialoja, *L'offerta a persona indeterminata ed il contratto concluso mediante automatico*, Città di Castello, 1902, p. 151 ss.

[2] Non sarà possibile soffermarci estesamente sulle sopramenzionate tecnologie, le quali rappresentano il substrato, o, comunque, uno dei referenti materiali delle presenti indagini. Per la descrizione delle caratteristiche – effettive o auspicate – delle *blockchain*, la più nota tra le *Dlt,* e tecnica di organizzazione e conservazione dei dati (la non alterabilità, la condivisione, la crittografia, il ruolo dell'*oracle*, etc.), rimandiamo alla letteratura sullo *smart contract*, di seguito citata.

che governano lo *smart contract* nell'ambito delle *Dlt* divergono e, per certi aspetti, rispondono a logiche antitetiche rispetto a quanto può osservarsi nei contratti cibernetici[3], nome attribuito all'impiego dell'intelligenza artificiale, o, con altra espressione, degli agenti *software* autonomi nella contrattazione[4]. In questa ipotesi, infatti, il dato caratterizzante risiede nella circostanza per cui chi sceglie di avvalersi della "*famiglia di tecnologie*"[5] declinate sotto il sintagma "intelligenza artificiale", lo fa nella contezza di non poterne calcolare e controllare l'imprevedibile funzionamento. Gli agenti *software* sono tendenzialmente in grado di sottrarsi al dominio degli utilizzatori e terzi, specie laddove l'intelligenza artificiale considerata sia dotata della capacità di assumere decisioni in situazioni di incertezza[6].

---

[3] Peraltro, le avanzate piattaforme in esame presentano innovazioni tali da scandire uno iato anche con gli ormai "tradizionali" contratti telematici, ossia negozi concernenti beni o servizi venduti sui siti commerciali in *Internet* e nei quali – sotto il profilo della conclusione del contratto – il supporto informatico è utilizzato come mero strumento per la trasmissione di dichiarazioni o manifestazioni di volontà formatesi in capo ai soggetti che utilizzano la tecnologia. Per un inquadramento delle questioni sottese alla formazione dei contratti telematici cfr. G. Conte, *La formazione del contratto*, in *Il codice civile. Commentario* fondato da P. Schlesinger, diretto da F. D. Busnelli, Milano, 2018, p. 262 ss.; A. M. Gambino, *La contrattazione telematica*, Milano, 1997; L. Follieri, *Il contratto concluso in Internet*, Napoli, 2005; A. M. Benedetti, *Autonomia privata procedimentale*, *La formazione del contratto fra legge e volontà delle parti*, Torino, 2011, p. 74 ss.

[4] Una maggiore accuratezza impone di non trascurare che la natura contrattuale del c.d. contratto cibernetico non sia scontata: la soluzione del problema, che si pone sul solco di una nota *querelle* in materia di contratti di massa, dipende essenzialmente dalla concezione di accordo che si ritiene di accogliere. Esemplificando, l'assenza di dialogo – alla quale conseguirebbe il non perfezionarsi del contratto – è l'argomentazione fatta propria dalle opinioni non contrattualiste (celebre il contributo di N. Irti, *Scambi senza accordo*, in *Riv. trim. dir. proc. civ.,* Milano, 1998, p. 347 ss.), fronteggiate da quelle contrattualiste, le quali, tenendo conto del processo di oggettivazione dello scambio (cfr. G. Oppo, *Disumanizzazione del contratto?*, in *Riv. dir. civ.,* Milano, 1998, I, p. 525 ss.) e dell'affermarsi del fatto sociale, non escludono che un atto compiuto dall'intelligenza artificiale possa considerarsi un contratto: cfr. V. Caredda, *Intelligenze artificiali e contratti. Aspetti problematici*, in *Il lavoro attraverso piattaforme digitali tra rischi e opportunità* a cura di P. Loi, Napoli, 2021, p. 259 ss., spec. p. 273 ss. Sul tema, tra i tanti, cfr. U. Ruffolo, *Intelligenza Artificiale, machine learning e responsabilità da algoritmo,* in *Giurisprudenza italiana,* Torino*,* 2019, p. 7; ID. *La "personalità elettronica", in Intelligenza artificiale. Il diritto, i diritti, l'etica, a cura di ID.,* Milano, 2020; F. Bravo, *Contrattazione telematica e contrattazione cibernetica*, Milano, 2007.

[5] Considerando 4, Reg. UE 2024/1689.

[6] All'estensione dell'autonomia conseguono soluzioni giuridiche diverse. Secondo autorevole dottrina, il grado di autonomia che determina che l'intelligenza

A fronte di tale autonomia e imprevedibilità, nel progetto sotteso all'utilizzo – e allo sviluppo – dello *smart contract*, l'intento è quello di ottenere univoci risultati predefiniti: in via di prima approssimazione, la rigidità, gli automatismi, l'irreversibilità e l'immodificabilità di quanto analiticamente programmato sono le peculiarità riscontrate e – per alcune posizioni – gli incentivi ad avvalersi dello strumento.

2. *Il problema definitorio*

Superata la (sommaria) fase di delimitazione dell'angolo prospettico, resta, in positivo, da tracciare la fisionomia dello *smart contract*. Le definizioni elaborate dalla dottrina e quella accolta dalla normativa[7], lungi dal convergere verso un risultato monosemico, sono espressione dell'ambiguità semantica che aleggia attorno alla locuzione *smart contract*[8], il cui impiego è tanto elastico da opacizzarne il significato, acquisendo il lemma in questione il ruolo di "contenitore"

---

artificiale non sia più una mera macchina – e il riconoscimento di una sua soggettività giuridica parziale – risiede nella capacità di assumere decisioni con un elevato grado di imprevedibilità. Se l'agente *software* dispone di questo livello di autonomia, allora le dichiarazioni/manifestazioni di volontà che emette sarebbero a esso imputabili ed è a esso riferibile anche la responsabilità: si veda G. Teubner, *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, a cura di P. Femia, Napoli, 2019, p. 55 ss. Sul problema della soggettività giuridica legato alle c.d. RAI (*Robotics and AI-based applications*) cfr. A. Bertolini, F. Episcopo, *Robots and AI as Legal Subjects? Disentangling the Ontological and Functional Perspective*, 2022, https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.iris.sssup.it/retrieve/e9a36b3a-43b5-470e-9515-6aafc4e1f940/the-expert-groups-report-on-liability-for-artificial-intelligence-and-other-emerging-digital-technologies-a-criticalassessment.pdf&ved=2ahUKEwjL4o3x2p2LAxVxhP0HHTvdH AQFnoECBcQAQ&usg=AOvVaw0s2DE30dK6kXK5LeSiaocI; ID., *Intelligenza artificiale e responsabilità civile. Problema, sistema, funzioni*, Bologna, 2024, spec. p. 118 ss.

[7] Art. 8*ter*, comma 2, d. l. n. 135 del 2018, convertito con modificazioni da l. n. 12 del 2019. La definizione normativa succede alle definizioni descrittive fornite dagli interpreti, collocandosi – almeno in parte – lungo l'impostazione per cui lo *smart contract*, propriamente inteso, sia rappresentato dal programma per elaboratore, dal *software* che consente di concludere e gestire il contratto; vedi nota 9.

[8] Secondo l'informatico che ha coniato il sintagma, lo *smart contract* è «*a computerized transaction protocol that executes the terms of a contract*» N. Szabo, *Smart contracts*, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html; cfr. anche ID., *Formalizing and Securing Relationships on Public Networks*, *https://firstmonday.org/ojs/index.php/fm/article/view/548* e ID. *Secure Property Titles with Owner Authority,* https://nakamotoinstitute.org/library/secure-property-titles/.

di meccanismi tecnologici difformi. L'esame delle eterogenee definizioni esula dall'economia del presente lavoro[9], ma un cursorio esercizio di sintesi delle stesse è necessario, perché, da un lato, agevola l'intelligenza della nozione di *smart contract* fornitaci dalla normativa domestica e, dall'altro, consente di rintracciare i due tratti fondamentali che lo caratterizzano: lo schema causale *if this*, *then that*[10] e la interrelata "esecuzione automatica delle prestazioni" o "auto-esecuzione". Tali tratti costituiscono, al contempo, la fonte principale dell'entusiasmo e delle perplessità che circondano il fenomeno. Più nel dettaglio, nei sistemi in questione viene immesso un numero indefinito di informazioni e di istruzioni e, al verificarsi delle condizioni prestabilite (*if this*), si producono conseguenze determinate (*then that*)[11]. Si ottengono così risultati ai quali non è possibile sottrarsi:

---

[9] Si segnala che, per un certo indirizzo, si tratterebbe di «Uno speciale protocollo volto a offrire, accertare o implementare la negoziazione o l'esecuzione del contratto in maniera tracciabile e irreversibile, senza l'ausilio di terzi»: A.U. Janssen - F. P. Patti, *Demistificare gli smart contracts*, in *Osservatorio del diritto civile e commerciale*, Bologna, 1, 2020, p. 32. Su questa linea anche M. Maugeri, *Smart contracts e disciplina dei contratti*, *cit.*, p. 28 e P. Cuccuru, *Blockchain e automazione contrattuale. Riflessioni sugli smart contract*, in *La nuova giurisprudenza civile commentata*, Milano, 1, 2017, p. 107 ss., 111. Di diverso avviso coloro che lo riconducono a un contratto (cfr. D. Di Sabato, *Gli smart contracts: robot che gestiscono il rischio contrattuale*, in *Contratto e impresa*, Milano, 2, 2017, p. 386; L. Parola, P. Meratti e G. Gavotti, *Blockchain e smart contract: questioni giuridiche aperte*, in *I contratti*, Milano, 6, 2018, p. 684: contratti digitali, le cui «clausole contrattuali sono incorporate nel software sotto forma di codice») e altri studiosi, per i quali lo *smart contract* consisterebbe soltanto nella trasposizione nel sistema di «una o più fasi esecutive di un precedente contratto, spesso congegnato come contratto quadro o come contratto per adesione» (F. Di Ciommo, *Smart contract e (non-) diritto. Il caso dei mercati finanziari*, in *Nuovo diritto civile,* Roma, 4, 2019, p. 257 ss., spec. p. 259).

[10] Tale aspetto è al centro di diversi contributi sul tema: oltre agli studi già indicati, si segnala anche E. Bivona, *Smart contracts, diritto nazionale e discipline eurounitarie*, in *Smart. La persona e l'infosfera*, a cura di U. Salanitro, Pisa, 2022, p. 325 ss. e C. Pernice, *Distributed ledger technology, blockchain e smart contracts: prime regolazioni*, in *Tecnologie e diritti*, Napoli, 2, 2020, p. 495 ss. Sulle interazioni tra questo meccanismo e la condizione cfr. G. Marchetti, *Lineamenti evolutivi della potestatività condizionale: dal contratto allo smart contract*, in *Riv. dir. civ.*, Milano, 1, 2022, 96 ss., spec. 121 ss.

[11] L'impianto di tale sistema potrebbe accostarsi a talune concezioni antimperativiste della norma giuridica, per le quali essa si pone come giudizio ipotetico, secondo lo schema se A *deve essere* B: la legge esprime un rapporto di causalità giuridica, nella quale, al verificarsi di un fenomeno, consegue un dover-essere (*Sollen*) ideale (cfr. H. Kelsen, *La dottrina pura del diritto* a cura di M. G. Losano, Torino, 2021, p. 341 ss. Sulla differenza tra il rapporto di causalità, proprio delle leggi naturali, e il c.d. rapporto di imputazione facente capo alla norma giuridica spec. p. 377 ss.) o un'esigenza della

avviato il procedimento, l'ingerenza nel funzionamento dei programmi in esame è preclusa a utenti e terzi, impossibilitati a modificare quanto in precedenza pattuito. Questo meccanismo è descritto da alcuni studiosi, perlomeno con riguardo ai sistemi connotati da una maggiore rigidità[12], come «esecuzione automatica e irreversibile»[13] o, con altre formulazioni, si parla di contratto che viene «automaticamente eseguito»[14], o, ancora, di puntuale applicazione di quanto previsto da parte del programma[15].

La c.d. auto-esecuzione viene messa in risalto anche dal diritto positivo, nel quale si allude ad una esecuzione – letteralmente del *software*, del "*programma per elaboratore*" – che "*vincola automaticamente le parti sulla base di effetti predefiniti dalle stesse*". Affiorano, nondimeno, gli interrogativi: viene fotografata, in termini equivoci, una realtà che vive fuori dagli schemi giuridici[16] e la si pone in

---

vita umana (effetto giuridico come valore reale, cfr. A. Falzea, (voce) *Efficacia giuridica*, oggi in *Ricerche di teoria generale del diritto e di dogmatica giuridica*. II – *dogmatica giuridica*, Milano, 1997, p. 3 ss. spec. p. 27 ss., 68) Sulla nozione di norma come giudizio ipotetico cfr. anche N. Irti, *Rilevanza giuridica*, in *Jus*, 1-2, Milano, 1967, p. 55 ss., spec. p. 68 ss. e M. Orlandi, *Introduzione alla logica giuridica*, Bologna, 2021, p. 21 ss. Uno scrutinio di tali diverse concezioni della norma giuridica si registra in V. Caredda, *La questione dell'onere*, Torino, 2024, p. 13 ss. e EAD., *L'onere e la norma: prove di accesso al diritto*, in *Giustizia civile,*1, Milano, 2019, p. 51 ss.

[12] Una distinzione tra le tecnologie in esame, relativa al grado di "flessibilità" delle stesse e al correlato ampliarsi dello spazio di intervento degli utenti, è illustrata da F. Bassan, M. Rabitti, *Recenti evoluzioni dei contratti sulla blockchain*. *Dagli smart legal contracts ai contracts on chain*, in *Rivista di diritto bancario*, luglio/settembre 2023, https://rivista.dirittobancario.it/, p. 561 ss.

[13] E. Bivona, *Smart contracts*, *cit.*, p. 325 ss.

[14] G. Finocchiaro, *Il contratto nell'era dell'intelligenza artificiale*, *cit.*, p. 458 ss. Sul tema cfr. anche C. Attanasio, *Inadempimento dello smart contract, sistema rimediale e tutela effettiva*, in *Riv. dir. civ.*, Milano, 4, 2024, 719 ss.

[15] D. Di Sabato, *Gli smart contracts: robot che gestiscono il rischio contrattuale*, *cit.*, p. 386 ss. Un margine di incertezza può essere dettato dal fatto che l'impulso che determina l'esecuzione delle istruzioni non dipenda da elementi interni al sistema (come lo spirare di un termine), ma da un fattore esterno alla *blockchain*: il collegamento tra la catena di blocchi e il mondo reale avviene mediante l'impiego dei c.d. oracoli, i quali consentono la verifica del soddisfacimento delle condizioni programmate (cfr. L. Parola, P. Meratti e G. Gavotti, *Blockchain e smart contract*, *cit.*, p. 674).

[16] Nulla di eccentrico, la realtà giuridica si articola in diverse specie: «Il diritto crea delle vere e proprie realtà che senza di esso non esisterebbero, delle realtà, quindi, che il diritto non prende da un mondo diverso dal suo per appropriarsele con o senza modificazioni, ma che sono esclusivamente e originariamente sue», ma può anche assumerle «da un diverso ordine di conoscenze», esse «si dicono giuridiche, […] solo

relazione con un atto di autonomia privata, ma non è chiaro se sia l'esecuzione del programma a rappresentare la "fonte" del vincolo, né quale accezione sia da attribuire al verbo "*vincola*"[17], peraltro nell'ambito di una locuzione a cui gli si affianca l'avverbio "*automaticamente*". A quale istituti giuridici e discipline dobbiamo rivolgerci?

A dire il vero, neppure la sussunzione nelle maglie dell'ordinamento sembrerebbe scelta obbligata per alcuni: essa è deliberatamente osteggiata dalle inaccettabili posizioni di coloro che vedono nello *smart contract* un'entità che si pone al di fuori del circuito giuridico, autonoma e autoreferenziale («*code is law*»[18], «*outside entities or jurisdictions*») e, dunque – così si afferma –, più solida e efficiente[19], poiché alla libertà di azione umana si sostituisce l'esecuzione automatica e perché, sul versante delle tutele, si precluderebbe – questo sarebbe il proposito – la sindacabilità da parte del giudice. Accantonerei rapidamente tali impostazioni, che al più presentano un interesse culturale e che risultano declinazioni di un noto orientamento – da esse esasperato – ai sensi del quale i privati, nella diffusa sfiducia verso la tutela giurisdizionale dei diritti, cercano di ridurre all'osso le imprevedibili decisioni dell'autorità giudiziaria[20]. Le considerazioni avanzate dai

---

perché il diritto le prende in considerazione, le qualifica, ne la dipendere conseguenze svariatissime»: S. Romano, (voce) *Realtà giuridica*, in *Frammenti di dizionario giuridico*, Milano, 1947, p. 204 ss., spec. p. 211. *Infra* nota 17.

[17] L'utilizzo del verbo "*vincola*" non è di certo eloquente in ordine al proprio significato: solo nel IV libro del codice civile, tale verbo o l'aggettivo "vincolato/i" assumono differenti significati: a titolo esemplificativo, all'art. 1331 c.c. si indica la soggezione del concedente al potere dell'opzionario; all'art. 1420 c.c. il riferimento sembra rivolto alla vincolatività del contratto e, all'art. 1305 c.c., il "*vincolo*" richiamato parrebbe quello relativo al rapporto obbligatorio. Come evidenzia anche V. Roppo, *Il contratto*, in *Trattato di diritto privato* a cura di G. Iudica e P. Zatti, Milano, 2011, p. 480 ss., la '"vincolatività" o "impegnatività" del contratto è un concetto che insiste su un piano diverso da quello dell'efficacia – in questo caso gli effetti obbligatori – ed essi non vanno sempre di pari passo: ai sensi dell'indirizzo oggi dominante in dottrina, la giuridicità del fatto dipende esclusivamente dalla presa in considerazione del fatto medesimo da parte della norma giuridica – dalla sua conformità al tipo normativo (N. Irti, *Rilevanza giuridica*, *cit.,* p. 66 ss.).

[18] L. Lessig, *Code and Other Laws of Cyberspace*, New York, 1999, p. 24.

[19] A. Savelyev, *Contract law 2.0: «smart» contracts as the beginning of the end of classic contract law*, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241*, p. 18, 21.

[20] Tale pretesa di autosufficienza non rappresenta un dato isolato: ravvisiamo in essa un'esaltazione del mutato paradigma in ordine al rapporto tra contratto e rimedio. A fronte dell'impostazione tradizionale («una scansione diacronica della sequenza regolativa, per cui vi sarebbe un "prima" (il contratto) cui farebbe seguito un "dopo"

fautori di queste impostazioni possono, però, forse, fornire qualche spunto per l'interprete, ad esempio laddove si legge «*smart contract does not create obligations in its legal meaning*»[21]. Tale affermazione, con una certa cautela, potrebbe rivelarsi non del tutto inappropriata, ma non perché si tratti di effetti estranei al diritto, semmai poiché essi potrebbero rispondere a principi giuridici e regole diverse da quelle proprie del rapporto obbligatorio[22].

3. *L'auto-esecuzione: quali legami con l'ordinamento giuridico?*

L'inaccettabile corrente di pensiero ora citata propugna una visione sconfinata dell'autonomia privata[23]: muoversi nell'ordito di un sistema effettivamente informato dal principio della libertà individuale e della liceità dei comportamenti non espressamente vietati può condurre al superamento di certe restrizioni dell'autonomia privata tradizionalmente sostenute[24], ma non equivale di certo a con-

---

(il rimedio)», parrebbe registrarsi, almeno in certi orientamenti e in certi settori, un superamento di questa scansione e «il rimedio, appunto, attraverso la previsione legale viene incistato nel contratto, andando ad arricchirne il ciclo degli effetti […] là dove esso viene strutturato dal legislatore alla stregua di un dispositivo capace di autocorreggersi e di neutralizzare, per così dire, in anticipo i suoi stessi possibili fallimenti»: L. Nivarra, *Il diritto privato e il passaggio dai rimedi contrattuali al contratto/rimedio: primi spunti di riflessione**, in *Rivista critica di diritto privato*, 1-2, 2023, 61 ss., spec. 62-63. Inoltre, anche la diffidenza nei confronti della incertezza ermeneutica non è di certo un fenomeno sconosciuto: il ricorso ai patti di inversione e modifica dell'onere della prova è riconducibile a tale processo culturale. Qui, tuttavia, i limiti dell'autonomia privata sono chiaramente enunciati (anche) dalla norma stessa: sui rapporti tra l'autonomia negoziale e l'art. 2698 c.c., si veda V. Caredda, *La questione dell'onere*, *cit.*, p. 207 ss.; cfr. anche S. Patti, *Le prove*, in *Trattato di diritto privato* a cura di G. Iudica e P. Zatti, Milano, 2021, spec. p. 343 ss. e 358 ss.

[21] A. Savelyev, *Contract law 2.0: «smart» contracts as the beginning of the end of classic contract law*, *cit.*, p. 17.

[22] *Infra* par. 3.

[23] Rammentiamo che il concetto di «autonomia», anche dal punto di vista terminologico (S. Pugliatti, (voce) *Autonomia privata*, in *Enc. dir.*, IV, Milano, 1959, p. 367 ss.), richiama immediatamente quello di «eteronomia» e il concetto di «libertà» quello di «autorità».

[24] Com'è noto, l'autonomia privata è stata fino a non troppo tempo fa sostanzialmente circoscritta all'area del contratto – fondata esclusivamente sull'art. 1322 c.c. – e, anche in questo settore, si consideravano inaccessibili ad essa tanto la fase di formazione del contratto (cfr. R. Sacco, (voce) *Autonomia nel diritto privato*, in *Dig. disc. priv.*, Torino, 1987, p. 517 ss., spec. p. 518, «L'autonomia incomincia là dove l'ordinamento mette a disposizione del consociato uno o più procedimenti […]

templare un'idea di onnipotenza della stessa. Al più, a nostro avviso, l'adesione a impostazioni che attribuiscono un'ampia (ma controllata) operatività dell'autonomia privata può agevolare il procedimento di costruzione del senso razionale degli strumenti in esame e fornire agli stessi un adeguato quadro di disciplina[25].

Riconsiderando l'opaco tenore del menzionato dato normativo[26], parrebbe, a primo impatto, che la fonte di detto vincolo risieda nell'esecuzione del codice informatico sul registro decentralizzato. Com'è noto, la presenza di un atto normalmente[27] esecutivo non è estranea alla conclusione del contratto: ci si riferisce

---

adottando i quali il consociato riesce a creare la regola giuridica»; G. Benedetti, *Dal contratto al negozio unilaterale*, Milano, 1969, p. 36), quanto l'area dei suoi effetti (E. Betti, *Teoria generale del negozio giuridico*, Rist. Napoli, 2002, p. 86).

[25] Si usa indicare gli *Smart contracts* che consentono sia la conclusione che l'esecuzione della transazione con l'espressione "*Smart legal contracts*" e quelli nei quali la sola esecuzione avviene sulle *Dlt* come "*Smart code contracts*": cfr. M. Maugeri, *Smart contracts e disciplina dei contratti*, *cit.*, p. 33. Com'è agevole immaginare, è la prima ipotesi contemplata a sollevare i maggiori quesiti in ordine al procedimento di formazione e perfezionamento dell'accordo, sempre ammesso che di accordo possa discorrersi. Autorevole dottrina, fautrice dell'autonomia privata procedimentale, accosta la locuzione "*effetti predefiniti dalle parti*" al negozio di configurazione: A. M. Benedetti, *Contratto, algoritmi e diritto civile transnazionale: cinque questioni e due scenari*, in *Rivista di diritto civile*, Milano, 2021, p. 69 ss., spec. p. 74. Sul negozio configurativo, per il medesimo autore – ove ampia bibliografia sul tema – ci permettiamo di rimandare a ID., *Autonomia privata procedimentale*, *cit.*, p. 237 ss. e p. 425 ss.; cfr. anche G. Palermo, *L'autonomia negoziale*, Torino, 2015, p. 26 ss. Per quanto concerne, invece, l'atteggiarsi dell'autonomia privata nei procedimenti di formazione del contratto cibernetico cfr. V. Caredda, *Intelligenze artificiali e contratti*, *cit.*, p. 273 ss.

[26] Si veda nota 7.

[27] Il concetto di esecuzione richiama una relazione e, tendenzialmente, si riconduce all'effetto (eventualmente prodotto da un contratto già concluso) – di cui rappresenta il *posterius*, almeno dal punto di vista logico – e si risolve in un insieme di fenomeni, qualitativamente eterogenei, che costituiscono «realizzazione di uno stato di fatto corrispondente o conforme a quello stato (di fatto) che nell'effetto si *auspica o si comanda* che accada»: A. Di Majo Giaquinto, *L'esecuzione del contratto*, Milano, 1967, p. 18. Cfr. anche L. Nivarra, (voce) *Esecuzione del contratto*, in *Enc. del dir. I tematici*, diretto da G. D'Amico, Milano, p. 529 ss., 535. È in virtù dell'atto di autonomia privata che il contegno conforme – esecutivo – dell'agente assume significato per il diritto: cfr. G. Amadio, *Controllo sull'esecuzione ed efficacia negoziale (note intorno al concetto di onere)*, in *Letture sull'autonomia dei privati*, Padova, 2005, spec. p. 225 ss., spec. p. 229. Peraltro, quanto da ultimo richiamato, all'evidenza, richiede una certa cautela, coinvolgendo l'insoluta – e irrisolvibile? – questione dell'ambivalenza in ordine al rapporto tra il negozio e i suoi effetti, tra il negozio giuridico quale fatto giuridico o valore, presupposto materiale dell'efficacia o criterio di valutazione e qualificazione dei

tipicamente alla consegna – qui non ancillare a un diritto già trasferito/costituito – che il privato ha l'onere di porre in essere per perfezionare un contratto reale[28], oppure all'inizio di esecuzione della prestazione da parte dell'oblato[29]. Tuttavia, non siamo affatto certi che la norma *de quo* orienti univocamente verso un determinato procedimento di formazione del contratto[30] – né gli argomenti letterali, di per sé, possono considerarsi dirimenti a conferma di un tale indirizzo ermeneutico – e, semmai, della stessa disposizione saremmo propensi a fornire una lettura correttiva che, come suggerito da alcuni studiosi[31], potrebbe avere un simile tenore: "*accordi mediante cui le parti si vincolano all'auto-esecuzione*": ad emergere sarebbe allora non un problema legato al procedimento formativo, bensì agli effetti del contratto[32]. Nello specifico, come anticipato, si registrerebbe

---

fatti: cfr. per tutti B. De Giovanni, *Fatto e valutazione nella teoria del negozio giuridico*, Rist. Napoli, 2016.

[28] Ciò a differenza dei contratti consensuali, ove la consegna medesima consegna è considerata, in modo pacifico, come atto esecutivo di un contratto già concluso: A. M. Benedetti, *Autonomia privata procedimentale*, *cit.*, p. 254. Sulla *traditio* quale ultima tappa della sequenza formativa del contratto reale cfr. anche G. Benedetti, *Dal contratto al negozio unilaterale*, *cit.*, p. 75 e 82 ss.; sui rapporti tra realità e esecuzione del contratto cfr. anche L. Nivarra, (voce) *Esecuzione del contratto*, *cit.*, p. 536.

[29] Il procedimento di cui all'art. 1327 c.c. presenta, nell'esame dello *smart contract*, particolare rilevanza se si tiene conto del fatto che proprio l'informatico Szabo considerava quali antesignane allo *smart contract* (*Formalizing and Securing Relationships*, *cit.*) le c.d. vendite per automatico, *id est* quegli scambi che si realizzano con una persona che interagisce con un distributore automatico di merce di qualunque genere. Il procedimento di conclusione di tali negozi, secondo certe impostazioni, sarebbe costituito dall'art. 1327 c.c. e la condotta esecutiva dell'accettante sarebbe il c.d. *iactus pecuniae*, ossia l'inserimento della moneta nell'apparecchio: cfr. G. Conte, *La formazione del contratto*, *cit.*, p. 232 ss.; per una più ampia riflessione sullo *iactus pecuniae* si veda sempre A. Cicu, *Gli automi nel diritto privato*, *cit.*, p. 577 ss. Con specifico riguardo allo *smart contract*, un accostamento dei relativi meccanismi all'art. 1327 c.c., o, alternativamente, allo schema dell'art. 1341 c.c. è proposto da M. Franzoni, *Il digitale, la rete, l'IA e la responsabilità civile*, in *Jus civile,* 2, Milano, 2024, p. 208 ss., spec. p. 217. Sulla distanza tra *smart contract* e contratti conclusi tramite distributori automatici cfr. anche B. Sirgiovanni, *Lo 'smart contract' e la tutela del consumatore: la traduzione del linguaggio naturale in linguaggio informatico attraverso il legal design*, in *Le nuove leggi civili commentate*, Milano, 1, 2023, 214 ss., spec. 223.

[30] Anche le variabili menzionate – *smart legal contracts* o *smart code contract* (cfr. nota 20) – potrebbero suggerire che la valutazione sul procedimento formativo applicabile possa mutare a seconda del caso di volta in volta considerato.

[31] T. Pellegrini, *Prestazioni auto-esecutive*, *cit.*, p. 847 (in nota).

[32] Ad ogni modo, il proseguo dell'indagine qui presentata avrà proprio riguardo a un problema che si assesta sulla dimensione effettuale, la quale si colloca successivamente

un'allusione ai menzionati sistemi auto-esecutivi, ai c.d. vincoli automatici, sui quali sembra doveroso interrogarsi.

La dottrina, imperniando il proprio ragionamento sulla descritta rigidità e sulla correlata insensibilità all'intervento umano, colloca comunque il fenomeno nelle maglie del rapporto obbligatorio[33]: si discorre di eliminazione di ogni spazio per il volontario inadempimento delle parti[34], del venir meno della «possibilità materiale di non adempiere al contratto stesso»; il risultato è un'ineluttabile proiezione verso la fisiologica estinzione del rapporto obbligatorio, rappresentata dall'adempimento[35]. A ciò seguono osservazioni di secondo livello, costituite ad es. dalla irrilevanza dell'*animus solvendi* del debitore e, pertanto, dall'incompatibilità con la teoria negoziale dell'adempimento[36], dall'accostamento dello *smart*

---

al compiersi del procedimento formativo della fattispecie.

[33] Del resto, come evidenziato da L. Nivarra, (voce) *Esecuzione del contratto*, *cit.*, il problema del dare esecuzione (a un effetto giuridico) rinvia tendenzialmente al modello dell'obbligazione, nonostante il concetto di esecuzione del contratto, opportunatamente messo a fuoco, sia più esteso. Inoltre, praticamente tutti i contratti, all'interno del nostro ordinamento, sono (anche) fonte di effetti obbligatori: l'asimmetria, rispetto ai contratti a effetti reali, è ben delineata da V. Roppo, *Il contratto*, *cit.*, p. 481 ss.

[34] P. Cuccuru, *Blockchain e automazione contrattuale. Riflessioni sugli smart contract*, *cit.*, p. 111; G. Finocchiaro, *Il contratto nell'era dell'intelligenza artificiale*, *cit.*, p. 458.

[35] Gli scambi di valori ricalcherebbero, strutturalmente, un trasferimento di ricchezza/denaro attuato mediante l'aggiornamento – senza intermediazione di una banca – di due poste di conto. Ad esempio, nel settore assicurativo, si rinvengono casi di sperimentazione di servizi e prodotti basati sulla *blockchain*: registrato, tramite l'impiego degli oracoli, il verificarsi dei presupposti che attivano la copertura assicurativa, l'assicurato riceverebbe automaticamente sul proprio conto l'indennità dovutagli (C. Pernice, *Distributed ledger technology, blockchain e smart contracts*, *cit.*, p. 502). Quanto detto e, soprattutto, quanto si affermerà in ordine ai rapporti obbligatori, vale anche per il rapporto tra assicuratore e assicurato, a patto che si accetti l'appartenenza di quest'ultimo al medesimo settore: il tema è affrontato diffusamente in P. Corrias, *Garanzia pura e contratti di rischio*, in *Il diritto della banca e della borsa*, Milano, 2006, spec. nei primi capitoli. Diverse ipotesi applicative della tecnologia *smart contract* sono illustrate da E. Battelli, *Le nuove frontiere dell'automazione contrattuale tra codici algoritmici e big data: gli smart contracts in ambito assicurativo, bancario e finanziario*, in *Giustizia civile*, Milano, 2020, p. 681 ss.).

[36] Peraltro tale profilo non sarebbe foriero di particolari perplessità in ragione del "superamento" di tale impostazione – per la quale la validità e l'efficacia dell'adempimento è subordinata alla sussistenza di un specifico intento negoziale diretto all'estinzione dell'obbligazione o, secondo alcuni, a un vero e proprio accordo tra debitore e creditore che deve accompagnare l'esecuzione – dominante nel XIX secolo, ma che ha ceduto il passo principalmente alle teorie che ascrivono all'adempimento natura di fatto giuridico

contract a un'eccezione di inadempimento[37] o a una clausola *solve et repete*[38].

A nostra sommessa opinione, nondimeno, è l'accoglimento disinvolto della premessa – la circostanza per cui tali automatismi sarebbero sovrapponibili al rapporto obbligatorio – a sollevare alcune perplessità: ai vantaggi connessi all'autoesecuzione dello *smart contract* (rappresentati essenzialmente dalla maggiore certezza del buon esito degli scambi[39] e, ulteriormente, dalla diminuzione dei rischi che originano dal commercio elettronico e dalla conseguente deflazione del contenzioso) potrebbero forse far da contraltare problemi (anche) d'ordine dogmatico, con evidenti ricadute pratico-applicative.

Si consideri il lato passivo del rapporto obbligatorio, l'obbligazione che investe il debitore: essa, secondo un'impostazione condivisa, viene ricondotta – quale sua *species* – alla categoria del dovere giuridico[40] e, segnatamente, a un dovere giuridico specifico di carattere patrimoniale (art. 1174 c.c.)[41]. L'intelligenza della

---

in senso stretto (C. M. Bianca, *L'obbligazione*, 4, Milano, 2019, p. 263 ss.) o alla concezione reale dell'adempimento, espressa nella formula dell'atto dovuto (facente capo, tra gli altri, a R. Nicolò, (voce) *Adempimento*, in *Enc. del dir.*, Milano, 1958, p. 554 ss., spec. p. 556 ss. e P. Perlingieri, *Dei modi di estinzione delle obbligazioni diversi dall'adempimento*, in *Commentario del codice civile* a cura di A. Scialoja e G. Branca, 1975, p. 173 ss.). Per una disamina delle diverse impostazioni sul tema – comprese quelle definibili eclettiche – cfr. A. Di Majo, *L'adempimento dell'obbligazione*, Bologna, 1993, p. 12 ss. e U. Breccia, *Le obbligazioni*, in *Trattato di diritto privato* a cura di G. Iudica e P. Zatti, Milano, 1991, p. 447 ss.

[37] M. Franzoni, *Il digitale, la rete, l'IA e la responsabilità civile*, *cit.*, p. 217: «un'attività del creditore riconducibile all'eccezione di inadempimento, valutabile secondo l'art. 1460 c.c.».

[38] T. Pellegrini, *Prestazioni auto-esecutive*, *cit.*, p. 862 ss.

[39] Il che rifluisce nel modo di confezionamento del contratto, in quanto riduce l'esigenza di prevedere clausole che regolino l'insorgenza degli eventuali futuri conflitti, tanto frequenti nel commercio elettronico: sul contratto, qua osservato soprattutto come strumento di programmazione dell'attività economica, di allocazione del rischio, si realizza un importante risparmio in ordine ai costi transattivi. Sul tema cfr. F. Macario, *Le sopravvenienze*, in *Trattato del contratto* a cura di V. Roppo – *Rimedi* - 2, Milano, 2022, p. 759 ss., spec. p. 761 ss.

[40] Cfr. R. Guastini, (voce) *Dovere giuridico*, in *Enciclopedia giuridica*, Roma, p. 2; cfr. anche E. Betti, (voce) *Dovere giuridico (teoria generale)*, in *Enciclopedia del diritto*, XIV, Milano, p. 53 ss.; M. Giorgianni, (voce) *Obbligazione* (*diritto privato*), in *Novissimo Dig. it., XI,* Torino, 1965, spec. p. 581 ss., 583; L. Mengoni, *L'oggetto dell'obbligazione*, in *jus*, 1956, p. 156 ss., spec. p. 158 ss.

[41] C. M. Bianca, *L'obbligazione*, 4, Milano, 2019, p. 1: «L'obbligazione è lo specifico dovere giuridico in forza del quale un soggetto, detto debitore, è tenuto ad una determinata prestazione patrimoniale per soddisfare l'interesse di un altro soggetto,

categoria medesima, efficace termine di distinzione tra situazioni giuridiche soggettive attigue[42], presuppone il corretto intendimento della "giuridica necessità"[43] di cui essa è espressione. È vero che ogni qualifica di doverosità limita lo spazio della libertà giuridica, ma è altrettanto rilevante mettere in luce come questo ridimensionamento non equivalga ad una sua integrale elisione: la «situazione di necessità, che costituisce il contenuto del dovere giuridico […] non esclude, né mortifica la libertà umana […], in quanto il soggetto, che si trova nella situazione di dovere, ha sempre la possibilità di scegliere tra l'adempimento del dovere e la sua violazione»[44]; nell'ottica del rapporto obbligatorio[45], si tratta della facoltà di adempiere o di rendersi inadempienti[46]. La questione è messa in risalto dalla mi-

---

detto creditore».

[42] Metodologia accolta da M. Giorgianni, (voce) *Obbligazione*, *cit.*, p. 583.

[43] Si veda C. M. Bianca, *L'obbligazione*, *cit.*, p. 21. La posizione di «giuridica necessità» (imposta per il soddisfacimento di un interesse altrui) è il perno su cui ruota la riflessione da noi proposta.

[44] R. Niccolò, *Istituzioni di diritto privato*, Milano, 1962, p. 4; che aggiunge: «bisogna avvertire che non si tratta di una necessità d'ordine fisico o materiale […] ma di una necessità di ordine morale, deontologica, e quindi relativa». Così M. Giorgianni, (voce) *Obbligazione*, *cit.*, p. 583; cfr. anche V. Caredda, *La questione dell'onere*, *cit.*, p. 65 ss., spec. 89: «Se non c'è dovere, non c'è violazione». A. Di Majo Giaquinto, *L'esecuzione del contratto*, *cit.*, p. 180, precisa che l'esecuzione della prestazione – qui intesa tecnicamente come oggetto dell'obbligazione – risponde ai requisiti di «incertezza e collocazione nel tempo che individuano la condizione».

[45] Sulla compatibilità tra il rapporto obbligatorio e i meccanismi in esame, un tema di interesse è rappresentato dal contrasto sull'oggetto dell'obbligazione: il dibattito, com'è risaputo, vede contrapporsi, da una parte, le teorie personali, che ravvisano l'oggetto del diritto di credito (asimmetrico rispetto al debito – cfr. L. Mengoni, *L'oggetto dell'obbligazione*, *cit.*, p. 175, il quale sul punto richiama, in parte discostandosi, le riflessioni di R. Nicolò, *L'adempimento dell'obbligo altrui*, rist. Napoli, 1978, p. 51 ss.) nell'attività dovuta dal debitore, dall'altra, le teorie patrimoniali, le quali individuano nel bene dovuto, distinto dal comportamento, il termine oggettivo del diritto. Ad ogni modo, «*Piattaforma comune*» di entrambe le concezioni sembra essere rappresentata dal concetto di obbligazione come dovere giuridico (L. Mengoni, *L'oggetto dell'obbligazione*, *cit.*, p. 158).

[46] L'ontologica impossibilità di essere inadempienti (così G. Finocchiaro, *Il contratto nell'era dell'intelligenza artificiale*, *cit.*, p. 458), sempre che di inadempimento si possa discorrere, è un *Quid* che insiste su un diverso piano rispetto a quello su cui poggiano le riflessioni di M. Orlandi, *La categoria dell'obbligazione ridotta*, in *Giustizia civile*, 3, Milano, 2019, p. 447 ss., spec. p. 463 ss. e ID., *Riduzione. Diritto senza forza*, Torino, 2024, spec. p. 92 ss., 102 ss., nelle quali si mette in risalto come ricorrano fattispecie che denotano un'asimmetria tra adempimento e inadempimento o fattispecie insuscettibili di inadempimento (non sempre il titolo implica la possibilità *logica*

gliore dottrina, la quale evidenzia come sia erroneo far discendere dalla qualifica di "atto giuridicamente dovuto" la certezza (naturalistica, reale) dell'evento (ad es. l'adempimento)[47]; inteso il dovere in termini di necessità reale[48], infatti, non rimarrebbe alcuno spazio per la sua violazione[49] e ciò, nella ricostruzione accolta[50], non viene accettato.

Preso atto di questo nucleo minimo di libertà qualificante il dovere giuridico[51], come collima la situazione del soggetto tipicamente investito dal dovere medesimo con le dinamiche – gli automatismi – proprie della c.d. auto-esecuzione nel fenomeno *smart contract*? La limitazione della propria libertà, *id est* la scelta

---

dell'inadempimento). In altri termini, in presenza di fenomeni di "riduzione", anche di quelli che vedono a monte un atto di autonomia privata (ad es. il *pactum de non petendo*), l'inesecuzione della prestazione da parte del debitore acquista una particolare rilevanza giuridica, diversa da quella che riceverebbe in assenza della "riduzione" medesima. Ma una "condotta" non consistente nell'adempimento – un contegno difforme – può materialmente verificarsi, e a cambiare è solo il suo significato giuridico. Ciò a differenza di quanto avverrebbe – stando alla narrazione comune sul tema – con riguardo alla c.d. "auto-esecuzione" nel fenomeno *smart contract*. In quest'ultimo caso, lungi dal verificarsi un indebolimento del vincolo, sembrerebbe rinvenirsi una forma di tutela più intensa dell'a*ccipiens*.

[47] L'errore di fondo è rappresentato dall'equivalenza tra la doverosità del comportamento e l'oggettiva certezza del suo verificarsi: cfr. G. Amadio, *La condizione di inadempimento. Contributo alla teoria del negozio condizionato*, Padova, 1996, p. 82 ss., spec. 84.

[48] G. Amadio, *La condizione di inadempimento*, *cit.*, p. 85.

[49] La negazione di libertà, la *necessitas*, contribuisce a descrivere posizione passive differenti dal dovere giuridico: cfr. anche F. Carnelutti, *Teoria generale del diritto*, Rist. Napoli, 1998, p. 169. *Infra* nota 51.

[50] Si vedano A. Falzea, (voce) *Efficacia giuridica*, *cit.*, p. 16 ss. e N. Irti, *Due saggi sul dovere giuridico* (*obbligo-onere*), Napoli, 1973, p. 22: «l'azione dovuta […] rappresenta qualcosa che potrà essere o non essere».

[51] Coinvolgendo nella trattazione altre situazioni giuridiche soggettive, non possiamo fare a meno di rammentare che di questo nucleo di libertà minima, com'è noto, non vi è traccia nell'ipotesi della soggezione, la quale comporta la mera esposizione – nonché impossibilità, in termini giuridici, di opporvisi – alle modifiche della propria sfera giuridica, provocate unilateralmente da chi è titolare del correlato diritto potestativo: C. M. Bianca, *La proprietà*, 6, Milano, 2017, p. 25 ss.; P. Perlingieri, *Manuale di diritto civile*, VIII, Napoli, 2017, (con P. Femia) p. 86. Il bene giuridico viene conseguito direttamente dal titolare del diritto potestativo, prescindendo da «qualsiasi correlativa attività dovuta dal soggetto passivo»: A. Falzea, *La separazione personale*, Milano, 1943, p. 130. Si discorre del diritto potestativo proprio quale diritto non suscettibile di violazione, in B. Carpino, (voce) *Diritti potestativi*, in *Enc. Giur. Treccani*, vol. XI, Roma, 1989, spec. p. 1.

di sacrificare la propria possibilità di non adempiere è compatibile con il dovere medesimo? Anche se si rinvenisse la sussistenza di suddetta compatibilità, sembrerebbe, tuttavia, che i privati, vincolandosi alla predetta esecuzione automatica, abbiano alterato la fisionomia del dovere giuridico, della relativa "necessità ideale" o giuridica. Ma ciò risulta consentito all'autonomia privata? Un percorso logico che conduca a una risposta di segno positivo potrebbe essere forse agevolato dall'accoglimento di opinioni che estendono l'autonomia negoziale agli effetti del contratto, alla possibilità di produrre effetti diversi da quelli «tipizzati o tipizzabili in via normativa»[52].

Le riflessioni condotte nell'embrionale ipotesi di lavoro formulata in questo contributo conducono alla condivisione degli interrogativi qui proposti, quesiti che sembrerebbero di grande rilevanza per più densi approfondimenti in ordine alla controversa figura dello *smart contract* e dei meccanismi che lo caratterizzano.

[52] Così G. Palermo, *L'autonomia negoziale*, *cit*., p. 82; si veda anche V. Roppo, *Il contratto*, *cit.,* p. 480, il quale reputa un'indebita riduzione dell'autonomia privata l'idea per cui la competenza a determinare gli effetti del contratto sia riservata in esclusiva alla legge.

Verso 'tre piani' di *accountability* per l'automobile intelligente

di **Giulia Bazzoni**

1. *L'avvento di Waymo, il robot taxi*

Ipotizzando uno scenario futuro, nei prossimi anni Waymo – il robot taxi creato da Google Alphabet e già collaudato negli Stati Uniti – potrebbe approdare nelle città europee, le quali, con la loro architettura antica, strade strette, denso traffico e variegata mobilità pedonale, costituiranno un test cruciale per la tecnologia di guida autonoma[1].

Waymo viene descritto oggi come il primo taxi a livello cinque di automazione, già attivo in numerose città americane[2]. Si tratta di un servizio di trasporto

[1] Per quanto riguarda l'implementazione di queste tecnologie nelle città europee, è fondamentale tenere a mente la differenza di approccio rispetto a questi strumenti e, in particolare, rispetto all'intelligenza artificiale tra Stati Uniti ed Europa. In specie, se gli Stati Uniti tendono a confidare nell'autoregolamentazione del mercato, l'Europa considera la regolamentazione come uno strumento essenziale per garantire la democrazia costituzionale e i diritti fondamentali. Questa distinzione è analizzata nel recente saggio di C. Pinelli, *L'AI Act: gestione del rischio e tutela dei diritti*, in *Giur. it.*, 2025, p. 452 ss. così anche A. Bradford, *Digital Empires: The Global Battle to Regulate Technology*, Oxford, 2023.

[2] Per maggiori dettagli relativamente alle caratteristiche di Waymo, si rimanda al sito ufficiale waymo.com/. Cfr. C. Knoll, *When Nobody is behind the wheel in car-obsessed Los Angeles*, in *New York Times*, 20 march 2024, www.nytimes.com/2024/03/20/us/los-angeles-waymo-driver.html. In proposito, nel settembre 2016, il Dipartimento dei Trasporti americano e la *National Highway Traffic Safety Administration* hanno definito

a guida totalmente autonoma che opera 24 ore su 24, sette giorni su sette, *fully electric*. I tre aggettivi che meglio descrivono questa autovettura sono: *convenient*, *consistent* e *safe*[3].

Questo robot taxi è stato addestrato per essere il miglior conducente possibile e significativamente più sicuro rispetto ad un uomo[4]. Sul sito ad esso dedicato si può leggere che il 94% degli incidenti negli Stati Uniti sono causati da un errore umano.

Waymo è dotato di un sistema integrato di sensori complementari e *radar* con microelettronica di ultima generazione e video-camere ad alta definizione di tipo termico che gli permettono di poter vedere ad una distanza di tre campi da calcio in tutte le direzioni, giorno e notte[5].

---

5 livelli di automazione per i veicoli: livello 0: Nessuna automazione. Il conducente ha il pieno controllo del veicolo; livello 1-3: Automazione parziale. Il sistema assiste in specifiche operazioni (frenata, gestione velocità), ma il controllo finale resta al conducente; livello 4: Automazione elevata. Il veicolo può operare autonomamente in condizioni predefinite, permettendo al conducente di distogliere completamente l'attenzione dalla guida; livello 5: Automazione completa. Il sistema gestisce tutte le funzioni di guida in qualsiasi condizione, indipendentemente dall'intervento umano. Questa classificazione intende offrire un quadro normativo per lo sviluppo e l'implementazione delle auto a guida autonoma, definendo gradi progressivi di tecnologia e responsabilità. In proposito, si rimanda al documento, in *open access* intitolato *Preliminary Statement of Policy Concerning Automated Vehicles*, www.nhtsa.gov/sites/nhtsa.gov/files/documents/automated_vehicles_policy.pdf. Per un commento, cfr. D.A. Riehl, *Car Minus Driver. Autonomous Vehicle Regulation, Liability and Policy*, in *The Computer & Internet Lawyer*, 2018, p. 1 ss.

[3] Si rimanda al *Paper* pubblicato sul sito il 20 dicembre 2023, intitolato *Waymo significantly outperforms comparable human benchmarks over 7+ million miles of rider-only driving*, waymo.com/blog/2023/12/waymo-significantly-outperforms-comparable-human-benchmarks-over-7-million/.

[4] Prima di essere messo in strada, Waymo ha percorso oltre 20 milioni di miglia su strade pubbliche e circa 10 miliardi di miglia in simulazione digitale. In merito, A.J. Hawkins, *Waymo has 7.1 million driverless miles – how does its driving compare to humans?*, in *The Verge*, 20 December 2023, www.theverge.com/2023/12/20/24006712/waymo-driverless-million-mile-safety-compare-human.

[5] Le sperimentazioni di Waymo sono state compiute perlopiù nella San Francisco *Bay area* con una flotta completamente elettrica. Waymo utilizza un sensore altamente tecnologico di nome Lidar che crea un'immagine tridimensionale a partire da ciò che si trova intorno al veicolo. Il sensore misura le dimensioni e la distanza degli oggetti intorno al veicolo e ne costruisce una rappresentazione tridimensionale. Per quanto riguarda le telecamere, invece, si tratta di soluzioni di tipo termico che lavorano congiuntamente ai sensori per garantire il campo visivo più ampio possibile, per catturare più dettagli e fornire immagini nitide negli ambienti di guida complessi. Le

Tale veicolo è connesso poi a un computer che calcola e analizza istantaneamente tutti i dati rilevati dai sensori, permettendogli di percepire dettagliatamente ciò che lo circonda. In particolare, l'automobile può determinare con precisione la propria posizione nel reticolo stradale e la propria velocità. Essa è in grado, altresì, di conoscere la situazione del traffico, di calcolare la rotta più efficiente ottimizzando percorso, soste e tempi di utilizzo, come pure di decifrare ogni entità circostante (pedoni, ciclisti, animali etc.); infine, la macchina sa leggere e comprendere tutti i segnali stradali[6]. In sostanza, Waymo può compiere lunghi tragitti senza l'intervento del conducente, mantenendosi sempre in contatto con gli altri autoveicoli della flotta[7].

Per quanto attiene al rapporto con i trasportati, anzitutto, Waymo è dotato di un sistema vocale bidirezionale che gli permette di dialogare con il cliente e di rispondere alle specifiche richieste[8]. Da ultimo, il robot-taxi monitora i parametri

---

videocamere di ultima generazione a lungo raggio e il sistema di visione a 360° possono individuare un pedone che attraversa la strada a 500 metri di distanza. Le telecamere perimetrali, inoltre, lavorando congiuntamente ai Lidar perimetrali, forniscono agli algoritmi di apprendimento automatico ulteriori dettagli per identificare gli oggetti in modo affidabile. Il Radar fornisce un ulteriore strato di informazioni rispetto a Lidar e telecamere con la sua capacità di vedere e misurare istantaneamente la velocità di un oggetto anche in condizioni meteorologiche difficili. Risulta migliorata anche la rilevazione degli oggetti sulle lunghe distanze, il che è molto importante per garantire al veicolo un tempo di reazione più lungo e avere la certezza di evitare gli ostacoli. Per maggiori dettagli, si rimanda al sito ufficiale di Waymo, waymo.com.

[6] In specie, la tecnologia di *autonomous driving* è basata sul pilota automatico. Si tratta di un sistema che è in grado di comunicare con le altre vetture e l'infrastruttura stradale. Di fatto, l'autopilota è un *software* che controlla l'auto attraverso una serie di sensori altamente tecnologici. In via generale, sulle *driverless cars* e le questioni attinenti alla rivoluzione che apporteranno nella mobilità si rimanda a E. Al Mureden, '*Event data recorder' e 'advanced driver assistance systems': la 'spinta gentile' verso la mobilità del futuro*, in *Contr. impr.*, 2022, p. 390 ss.; M.A. Geistfeld, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, in *California L. Rev.*, 2017, p. 1161 ss.

[7] In via generale, sul tema delle *driverless cars* si rimanda al recentissimo volume di E. Al Mureden, *Diritto dell'"automotive'. Dalla fabbrica alla strada: tra regole, mercato, tecnologia e società*, Bologna, 2024; nonché G. Calabresi, E. Al Mureden, '*Driverless cars'. Intelligenza artificiale e future della mobilit*à, Bologna, 2021. Si osservi, inoltre, M. Tampieri, *L'intelligenza artificiale: una nuova sfida anche per le automobili*, in *Contr. impr.*, 2020, p. 732 ss.; F.P. Patti, *The European road to authonomous vehicles*, in *Fordham International L. Jour.*, 2019, p. 125 ss.; in via critica, G.F. Simonini, *Dialogo tra un veicolo con sistemi elettronici intelligenti ed il conducente: riescono davvero a comprendersi o 'fingono' di farlo?*, in *Danno resp.*, 2024, p. 431 ss.

[8] A.J. Hawkins, *How will driverless cars 'talk' to pedestrians? Waymo has a few*

vitali dei trasportati nell'abitacolo e, in caso di emergenza, è programmato per intervenire[9].

Poste le premesse circa le indiscutibili potenzialità di Waymo, si constata come siffatte *driverless cars* siano l'emblema di una rivoluzione *disruptive* della mobilità[10]. Esse rappresentano il precipitato di una molteplicità di progressi tecnologici che stanno trasformando in modo strutturale il sistema dei trasporti, il quale si caratterizza sempre più per l'automazione della guida e la connessione tra autoveicolo e infrastrutture[11].

Il repentino incedere di tale livello di automazione richiederà, tuttavia, una nuova stagione di (complessa) uniformazione normativa. In proposito, l'Unione europea ha approvato recentemente diversi atti regolativi dedicati – in senso ampio – alla tecnologia, nel tentativo di instaurare un rapporto di maggiore complementarità tra diritto e tecnica.

È ragionevole pensare, pertanto, che i diversi regolamenti andranno a incidere ad ampio spettro sul mondo dell'automazione della guida e, concordemente,

---

ideas, *The Verge*, 13 October 2023, www.theverge.com/2023/10/13/23913251/waymo-roof-dome-communicate-intent-pedestrian-driver.

[9] Sul punto, è divenuto recentemente un caso mediatico quello dell'auto Tesla con guida autonoma che ha condotto in ospedale un uomo colpito da crisi iperglicemica e infarto. Sul punto si rimanda all'articolo online pubblicato sul Corriere della sera di P. Ottolina, *Una Tesla con guida autonoma ha portato in ospedale un uomo colpito da crisi iperglicemica e infarto*, in *Corriere della sera*, 14 aprile 2024, disponibile online su www.corriere.it/tecnologia/24_aprile_14/una-tesla-con-la-guida-autonoma-ha-portato-in-ospedale-un-uomo-colpito-da-crisi-iperglicemica-e-infarto-ba339b52-f6eb-4777-8015-52dd6a94bxlk.shtml.

[10] Per *disruptive innovation* si intende «an innovation that creates a new market and value network, which eventually disrupts an existing market and value network, typically displacing established market leading firms» cfr. in proposito, M.C. Grath, *Autonomous Vehicles, Opportunities, Strategies and Disruptions*, Poland, 2018, p. 141. Di conseguenza, secondo l'Autore, «autonomous vehicles will create an extreme degree of disruptions» perché questa evoluzione «will displace a huge existing industry, transportation, along with all its supporting industries». Si sofferma sull'argomento anche M. Cameron, Realising the potential of Driverless Vehicles, Wellington, 2018 e A. Herrmann, W. Brenner, R. Stadler, *Autonomous Driving, How the Driverless Revolution Will Change the World*, Bingley, 2018, p. 31 ss. In proposito, è d'obbligo richiamare poi E. Al Mureden, *'Autonomous cars' e responsabilità civile tra disciplina vigente e prospettive 'de jure condendo'*, in. *Contr. impr.*, 2019, p. 895 ss., spec. p. 901, in cui viene evidenziato compiutamente il carattere *disruptive* di tale innovazione.

[11] Si rimanda sul tema a G. Calabresi, E. Al Mureden, *Driverless cars*, cit., p. 95 ss.

anche su servizi come Waymo[12]. Pertanto, è utile sezionare, come in una tomografia, le aree tecniche che compongono il robot-taxi per provare a comprendere a quali discipline Waymo sarà tenuto a conformarsi una volta che le sue flotte approderanno in Europa.

2. *Le sezioni di Waymo 'driver' e i regolamenti europei*

Dall'esame delle componenti tecniche di Waymo, è possibile individuare una sequenza complessa di dati (personali e non), algoritmi e piattaforme[13]. In specie, i dati fungono, in primo luogo, da risorsa fondamentale per l'addestramento del robot taxi. Terminata questa prima fase di test – tendenzialmente compiuta in simulazione virtuale – la macchina, una volta su strada, continua comunque a raccogliere dati per mezzo dei propri sensori e li elabora in tempo reale, mantenendo costantemente aggiornato il proprio *database*.

In secondo luogo, come detto, ogni autovettura è connessa con le altre appartenenti alla flotta, al fine di scambiarsi vicendevolmente informazioni, sotto forma – appunto – di dati. Gli algoritmi rappresentano, invece, gli strumenti per mezzo dei quali estrarre valore dai dati: essi sono il centro di controllo della macchina, meglio ancora la 'mente' che va a definire i comportamenti dell'automobile. Infine, per utilizzare Waymo sarà necessario scaricare una applicazione che rimanderà ad una piattaforma tramite cui si potrà prenotare una corsa, acquistare abbonamenti, indicare la propria destinazione, osservare la rotta presa dal *driver robot* durante la corsa, lasciare recensioni e, infine, chattare con l'autovettura[14].

Ebbene, su ciascuno di questi tre elementi che caratterizzano il servizio di Waymo *driver* è possibile appuntare specifici segmenti di regolazione europea: il GDPR per la gestione dei dati (personali), l'AI Act per quanto riguarda la regolazione degli algoritmi di intelligenza artificiale e il *Digital Services Act* per quanto attiene i requisiti della piattaforma[15]. Ecco che il servizio di Waymo – una volta

---

[12] Il disegno strategico comprende, da una parte, la protezione dei dati personali ai sensi del Reg. 2016/679/UE; dall'altra, la nuova disciplina dei servizi digitali, *i.e.* il *Digital Services Act* ovverosia il Reg. 2022/2065/UE del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la Direttiva 2000/31/CE. Destinato ad integrarsi con tale impianto è poi il nuovo Regolamento sull'intelligenza artificiale, *i.e.* Reg. 2024/1689/UE.

[13] Rispetto a tale sequenza tra dati, algoritmi e piattaforme per i sistemi 'intelligenti', si rimanda a G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pub.*, 2022, p. 971 ss.

[14] Rispetto alla funzionalità della applicazione, si rimanda direttamente al sito di waymo.com/waymo-one/.

[15] In via generale, si interrogano sulla regolazione dei sistemi automatizzati

approdato in Europa – dovrebbe rientrare nell'ambito di applicazione di tutti i regolamenti indicati.

Si tratta, a ben vedere, di regolamenti fortemente complementari tra loro, in quanto rispondenti alla medesima *ratio*, ossia assicurare la costituzione di un mercato unico digitale europeo 'resiliente'[16]. In specie, i tre atti normativi presentano una comune struttura fondata sul cd. *risk based approach*, ossia un modello che – senza l'imposizione di limitazione eccessive – mira a trovare un corretto bilanciamento tra supporto all'innovazione tecnologica e gestione di ogni forma di rischio che possa compromettere la sicurezza[17]. Invero, esso intende stimare e mitigare i rischi relativi alla tecnica attraverso varie fasi di operative: l'iden-

---

'intelligenti' e sulle responsabilità attribuibili, A. Amidei, *Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo*, in *Giur. it*, 2021, p. 100 ss.; G. Di Rosa, *Quali regole per i sistemi automatizzati intelligenti?*, in *Riv. dir. civ.*, 2021, p. 823 ss.; A. Fusaro, *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso europeo*, in *Nuova giur. civ. comm*., 2020, II, p. 1344 ss.; U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, in *Riv. dir. civ*., 2020, p. 1246 ss.; si vedano poi i contributi di R. Cingolani, D. Andresciani, *Robots, macchine intelligenti e sistemi autonomi: analisi della situazione e prospettive*; F. Rodi, *Gli interventi dell'Unione Europea in materia di intelligenza artificiale e robotica: problemi e prospettive* e L. Ulissi, *I profili di responsabilità della macchina dell'apprendimento nell'interazione con l'utente*, tutti contenuti in *Diritto e intelligenza artificiale*, a cura di G. Alpa, Pisa, 2020, rispettivamente, pp. 23 ss.; 187 ss. e 435 ss.; P. Perlingieri, S. Giova, I. Prisco (a cura di), *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, Napoli, 2020; C. Trevisi, *La regolamentazione in materia di intelligenza artificiale, robot, automazione: a che punto siamo*, in *Riv. dir. media*, 2018, p. 447 ss.; E. Palmerini, *Robotica e diritto: suggestioni, intersezioni, sviluppi a margine di una ricerca europea*, in *Resp. civ. prev*., 2016, p. 1816 ss.; A. Zornoza, M. Laukyte, *Robotica e diritto: riflessioni critiche sull'ultima iniziativa di regolamentazione in Europa*, in *Contr. impr. eur.*, 2016, p. 808 ss.; U. Pagallo, *Even Angels Need the Rules: AI, Roboethics, and the Law*, in *IOS Press*, 2016, p. 214 ss.; C. Perlingieri, *L'incidenza dell'utilizzazione della tecnologia robotica nei rapporti civilistici*, in *Rass. dir. civ*., 2015, p. 1236 ss.; altresì A. Santosuosso, C. Boscarato, F. Caroleo, *Robot e diritto: una prima ricognizione*, in *Nuova giur. civ. comm*., 2012, II, p. 494 ss.

[16] Così, G. Finocchiaro, *Intelligenza artificiale e protezione dei dati personali*, in *Giur. it.*, 2019, p. 1670 ss., in particolare p. 1671 dove mette in risalto come «l'intelligenza artificiale si basa sui dati».

[17] Cfr. S. Tommasi, '*Digital Services Act' e* '*Artificial Intelligence Act*': *tentativi di futuro da armonizzare*, in *Pers. merc.*, 2023, p. 279 ss.; R. Gellert, *The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual?*, in *Journal of Ethics and Legal Technologies*, 2021, p. 15 ss.

tificazione del rischio, la sua analisi, l'eventuale azione di trattamento e, infine, il monitoraggio.

È un sistema che si propone, quindi, di governare dinamicamente la *techne*, imponendo obblighi e responsabilità proporzionali al grado di rischio che il prodotto tecnologico comporta[18]. Da questo contesto e dalla necessaria collaborazione fra giuristi ed informatici nel regolare tale settore, deriva la predilezione per un approccio di conformazione *ex ante* degli strumenti informatici a livelli di sicurezza prestabiliti[19]. Sicché, nei testi dovrebbe delinearsi – in astratto – una visione comune circa le modalità di responsabilizzazione dei soggetti di volta in volta designati[20].

Di conseguenza, l'assunzione delle diverse misure procedimentali dovrebbe assicurare un livello di sicurezza idoneo agli *standard* di tutti i regolamenti, data la sequenzialità con cui dati, algoritmi e piattaforme si completano vicendevolmente. Ciò nonostante, se è vero che ciascuno di questi regolamenti si fonda sul medesimo approccio al rischio, risulta altrettanto evidente, da un esame dei tre testi, come essi rappresentino espressioni molto diverse di tale logica e connessa *accountability*.

In specie, se nel primo caso (GDPR) gli strumenti di gestione del rischio vengono rimessi del tutto ai privati e servono per determinare la conformità delle misure al quadro normativo, nel secondo caso (IA), invece, è il legislatore a catalogare il livello di rischio implicato nella produzione e fornitura di determinate categorie di sistemi intelligenti, mentre nel terzo (DSA) è stata prediletta una via di mezzo tra queste due prospettive *lato sensu* antitetiche.

La questione che si pone, per servizi come Waymo, è quindi come sintetizzare questo approccio diversamente declinato nei regolamenti entro un unico schema operativo.

3. *Il principio di responsabilizzazione nel GDPR*

Tratteggiate le linee generali si comprende come i tre regolamenti rappresentino un punto di riferimento nella disciplina dei servizi del futuro come Waymo, motivo per cui è opportuno un confronto tra i differenti approcci prospettati.

---

[18] In proposito, G. De Gregorio, P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market L. Rev.*, 2022, p. 473 ss., dove gli Autori mettono in risalto come «In the last years, risk has become a proxy and a parameter characterizing the European regulation of digital technologies».

[19] In tal senso, A. Mantelero, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, a cura di G. Finocchiaro, Bologna, 2019, p. 287 ss.

[20] S. Tommasi, *Digital Services Act*, cit., p. 281.

Partendo dal Reg. 2016/679/UE, esso segue una prospettiva che può essere definita *bottom up*, vale a dire che le misure di mitigazione sono rimesse alla piena discrezionalità del titolare del trattamento, il quale è tenuto a valutare, di volta in volta, l'azione tecnica e organizzativa da prediligere[21]. Il principio di *accountability* – che può essere tradotto con principio di rendicontazione o di responsabilizzazione – rappresenterebbe, dunque, una strategia tesa a ridurre fortemente oneri legislativi imposti 'dall'alto'[22]. Invero, l'approccio fondato sul rischio nel GDPR riguarderebbe quello che può essere definito, in sintesi, un 'rischio di conformità': quanto minore sarà la conformità delle misure specifiche adottate rispetto al livello di sicurezza previsto dal regolamento, tanto maggiori saranno le conseguenze sul piano delle responsabilità[23].

La logica regolativa prescelta punta alla piena responsabilizzazione di coloro che trattano dati personali, dacché la valutazione del rischio è rimessa alla discrezionalità del soggetto individuato come titolare del trattamento[24]. In specie,

---

[21] In generale, sul *risk-based approach* nell'ambito della *data protection law*, si consideri R. Gellert, *We have always managed risk in Data Protection Law: Understanding the similarities and differences between the Rights-based and the Risk-based approaches to Data protection*, in *European Data Protection L. Rev.*, 2016, p. 481 ss.

[22] Il concetto di *accountability*, in realtà, è già presente dal 1980 nelle linee guida OECD *(Organisation for Economic Cooperation and Development)*, secondo cui «*A data controller should be accountable for complying with measures which give effect to the [material] principles stated above*». In proposito anche, G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, p. 1 ss. Si precisa, tuttavia, che la traduzione in principio di responsabilizzazione non riesce a rendere efficacemente la portata del concetto e dunque richiede un ulteriore sforzo interpretativo affinché venga colto per intero il significato. Cfr. D. Barbierato, *Trattamento dei dati personali e «nuova» responsabilità civile*, in *Resp. civ. prev.*, 2019, p. 2151 ss. Così anche E. Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. impr.*, 2018, p. 120, evidenzia come «Quello di *accountability* è un concetto difficilmente traducibile in una parola della nostra lingua e reso, nella versione italiana del regolamento, con il termine responsabilità. In realtà esso si colloca a metà tra la responsabilità e la *compliance*, perché il titolare deve essere *compliant* rispetto alla normativa in esame».

[23] Cfr. G. Gellert, *Understanding the notion of risk in the Generale Data Protection Regulation*, in *Computer Law & Security Rev.*, 2018, p. 279 ss.

[24] G. Amore, '*Fairness', 'Transparency' e 'Accountability', nella protezione dei dati personali*, in *Studium Iuris*, 2020, p. 414 ss., la quale evidenzia come si è passati ad un modello imperniato sul principio di responsabilizzazione del titolare del trattamento. Rispetto alla figura del titolare e del responsabile, si rinvia, inoltre, al contributo di A. Mantelero, *Gli autori del trattamento dati: titolare e responsabile*, in *Giur. it.*, 2019, p. 2799 ss.

ai sensi dell'art. 24 del Reg. 2016/679/UE, a costui viene imposta l'assunzione di misure tecniche e organizzative preventive poste a garanzia della correttezza del trattamento dei dati personali[25]. Parimenti, nell'ipotesi di rischio elevato, il titolare deve compiere una valutazione d'impatto delle misure da lui prescelte; ciò a conferma della rilevanza che il GDPR attribuisce al *risk based approach*[26]. Oltretutto, spetta al titolare fornire le prove del rispetto delle prassi da lui prescelte, ossia della rispondenza delle misure adottate, per metodo e contenuti, a ciò che in base a contesto, costi e finalità poteva essergli effettivamente richiesto. In definitiva, è in capo al titolare la prova della sua *compliance* al regolamento[27].

Il principio di *accountability* presuppone, quindi, che il titolare del trattamento sia il soggetto situato nella migliore posizione possibile per valutare e gestire il rischio[28]. La proattività diviene cardine del sistema, dal momento che al titolare è richiesto, in via prudenziale, un *agere* responsabile, vale a dire la predisposizione – ancor prima dell'inizio del trattamento effettivo – di misure adeguate alla natura, alla finalità, al contesto e all'ambito di applicazione del trattamento[29].

---

[25] Per un'analisi più approfondita dell'art. 24 si vedano M. Siano, *Art. 24*, in *GDPR e Normativa Privacy commentario*, a cura di G.M. Riccio, G. Scorza e E. Belisario, Vicenza, 2022, p. 300 ss.; F. Cairoli, S. Cavalcanti, *Art. 24*, in *Commentario al Regolamento UE 2016/679 e al codice della privacy aggiornato*, a cura di A. D'Agostino, L.R. Barlassina e V. Colarocco, Milano, 2019, p. 175 ss.

[26] Sulla valutazione di impatto si rimanda, in particolare, al commento dell'art. 35 Reg. 2016/679/UE di E. Battelli, G. D'Ippolito, in *Comm. cod. civ. - Delle Persone*, *Leggi Collegate*, II, *Il Regolamento Parlamento Europeo 27 aprile 2016m n. 2016/679/UE*, a cura di A. Barba e S. Pagliantini, Torino, 2019, p. 663 ss.

[27] Cfr. J. Lindqvist, *New challenges to personal data processing agreements: is the GPDR fit to deal with contract, accountability and liability in a world of the Internet of Things*, in *International Jour. of Law and Inf. Tech.*, 2018, p. 45 ss., in spec. p. 57 in cui viene esplicitato come «*a controller must be able to demonstrate in a measurable way that it has complied with the EU data protection obligations*».

[28] In particolare, G. Finocchiaro, *Il principio di 'accountability'*, in *Giur. it.*, 2019, p. 2778 ss., laddove viene fatto presente come l'*accountability* «costituisce il nucleo della riforma europea e realizza un nuovo sistema normativo nel trattamento dei dati personali e nella protezione dei diritti della persona»; Si vedano, inoltre, i contributi, rispettivamente della stessa Autrice, *Quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, nonché di A. Mantelero, *La gestione del rischio*, entrambi in *La protezione dei dati personali in Italia. Regolamento UE 2106/679 e d.lgs. 10 agosto 2018, n. 101*, a cura di G. Finocchiaro, Bologna, 2017, p. 1-26 e p. 473-526.; così anche G.G. Codiglione, *'Risk based approach' e trattamento dei dati personali*, in *La nuova disciplina europea della privacy*, a cura di S. Sica, V. D'Antonio e G.M. Riccio, Padova, 2016, p. 55 ss.

[29] In proposito, D. Poletti, *Le condizioni di liceità del trattamento dei dati*

Di conseguenza, è la stessa inosservanza di questo atteggiamento precauzionale, da parte del titolare, che determina illiceità e ingiustizia nel trattamento. Questo perché, secondo lo spirito del GDPR, la persona affida i dati al titolare sul presupposto per cui quest'ultimo si comporti, in relazione agli stessi, in modo *compliant* al dettato normativo[30]. All'opposto, il titolare del trattamento sarà esente da responsabilità ogniqualvolta dimostrerà – tramite esibizione di certificazioni o documentazioni – l'avvenuta adozione di misure tecniche e organizzative concretamente idonee a prevenire l'evento dannoso[31].

4. *L'"accountability' nell'"Artificial Intelligence Act' e nel 'Digital Services Act'*

Per quanto attiene, invece, il *Digital Services Act* e l'*Artificial Intelligence Act*, come detto, essi andranno a coadiuvare il GDPR nella regolazione dei servizi digitali. Entrambi gli atti normativi si basano su un modello incentrato sul rischio e sulla sua gestione[32]. In particolare, si delinea una logica proporzionale e cumulativa nell'imposizione di obblighi a mano a mano che aumentano i rischi, i quali

---

personali, in *Giur. it.*, 2019, p. 2783 ss., in particolare p. 2784 s.

[30] V. G. Calabrese, *Il danno da perdita di controllo dei dati personali nel pensiero della Corte di Giustizia UE*, in *Nuova giur. civ. comm.*, 2023, I, p. 1112 ss., spec. p. 1113 s.

[31] Precisano, con riferimento al contenuto della prova liberatoria, R. Caterina, S. Thobani, *Il diritto al risarcimento dei danni*, in *Giur. it.*, 2019, p. 2808 ss. che, laddove vi sia stata una violazione del regolamento, il titolare o il responsabile possono essere esonerati da responsabilità «dimostrando di aver adempiuto i propri obblighi e, dunque, che non erano disponibili misure tecniche atte a mitigare il rischio (purché il rischio di verificazione dei danni e l'entità degli stessi fossero sufficientemente bassi, dovendosi altrimenti astenere dal trattamento), o che i costi delle misure di prevenzione erano eccessivi rispetto a una bassa probabilità e/o gravità del rischio».

[32] Rispetto all'approccio all'AI Act si rimanda a G. Finocchiaro, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir. inf. inform.*, 2022, p. 303 ss.; J. Chamberlain, *The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective*, in *European Journal of Risk Regulation*, 2022, p. 1 ss. D. Iacovelli, M. Fontana, *Nuove sfide della tecnologia e gestione dei rischi nella proposta di regolamento europeo sull'intelligenza artificiale: set di training, algoritmi e qualificazione dei dati. Profili critici*, in *Il diritto dell'economia*, 2022, p. 107 ss. Mentre per un'introduzione alle novità del *Digital Services Act*, B. Saavedra Servida, *La responsabilità degli 'internet service provider': dal 'safe harbour' al principio di 'accountability'*, in *Nuove leggi civ. comm.*, 2024, p. 135 ss.; G. Finocchiaro, *Responsabilità delle piattaforme e tutela dei consumatori*, in *Giorn. dir. amm.*, 2023, p. 730 ss.; S. Del Gatto, *Il 'Digital Services Act': un'introduzione*, in *Giorn. dir. amm.*, 2023, p. 724 ss.

– a differenza di quanto accade nel GDPR – vengono predefiniti dal legislatore secondo una prospettiva *top down*[33].

Partendo dal Regolamento sull'intelligenza artificiale, il legislatore europeo ha prediletto, in sintesi, un approccio normativo orizzontale, volto a disciplinare il fenomeno nel suo complesso[34]. Lo scopo sarebbe quello di promuovere un'IA affidabile, nel rispetto dei valori fondamentali centrati sull'uomo e sull'equità, secondo concreti standard di trasparenza e conoscibilità in grado di assicurare robustezza, sicurezza e protezione dei diritti in condizioni effettive di responsabilità.

In proposito, è il legislatore stesso a configurare i livelli di rischio e connessi gradi di responsabilità entro cui vanno fatti rientrare i diversi sistemi di intelligenza artificiale, stabilendo, in via precauzionale, come il rischio vada affrontato[35]. In merito, i diversi livelli hanno una struttura, per così dire, verticale: più

---

[33] S. Tommasi, *Digital Services Act*, cit., p. 281; G. Natale, *Il nuovo regolamento europeo AI Act*, in *Dir. int.*, 2024, p. 201 ss.

[34] In breve, il testo finale del Reg. 2024/1689/UE è stato pubblicato in Gazzetta ufficiale in data 12 luglio 2024 ed è volto a stabilire disposizioni armonizzate sull'intelligenza artificiale; in proposito, è stato prediletto un approccio normativo orizzontale, volto a disciplinare l'intelligenza artificiale nel suo complesso, e non in singoli settori o specifiche materie. Si è trattato di un *iter* molto complesso e una negoziazione molto serrata tra gli Stati membri ma anche tra gli *stakeholders*, soprattutto per quanto riguarda i *General Purpose AI models*. Per maggiori dettagli sul contenuto del regolamento e le vicende legate alla sua approvazione si rimanda a F. Ferri (a cura di), *L'Unione europea e la nuova disciplina sull'intelligenza artificiale: questioni e prospettive*, in *Riv. quad. aisdue*, 2024, p. 6 ss.; A. Amidei, *La proposta di regolamento UE per un 'Artificial Intelligence Act': prime riflessioni sulle ricadute in tema di responsabilità da intelligenza artificiale*, in *Tecn. dir.*, 2022, p. 1 ss.; G. Alpa, *Quale modello normativo europeo per l'intelligenza artificiale?*, in *Contr. impr.*, 2021, p. 1003 ss.; G. Floridi, *The European Legislation on AI: a Brief Analysis of its Philosofical Approach*, in *Philos. technol.*, 2021, p. 215 ss.; G. Finocchiaro, *La proposta di regolamento sull'intelligenza artificiale: il modello basato sulla gestione del rischio*, in *Dir. inf. inform.*, 2022, p. 303 ss.; C. Casonato, M. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal*, 2021, p. 415 ss.; A. Adinolfi, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, a cura di S. Dorigo, Pisa, 2020, p. 13 ss.; M. Zanichelli, *Ecosistemi, opacità, autonomia: le sfide dell'intelligenza artificiale in alcune proposte recenti della Commissione europea*, in *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, a cura di A. D'Aloia, Milano, 2020, p. 67 ss.

[35] Cfr. da ultimo U. Ruffolo, *'Artificial Intelligence Act' e AI generativa*, in *Giur. it.*, 2025, p. 438 ss., spec. p. 443 ss. dove si sofferma sul tema del rischio sistemico; v.

alto è il rischio insito nell'utilizzo di un determinato sistema intelligenza artificiale, maggiori saranno le responsabilità di chi sviluppa, implementa e usa quel sistema, sino a giungere a un divieto di utilizzo delle applicazioni e delle tecnologie il cui rischio è considerato inaccettabile (come prevede l'art. 5)[36]. Il cuore di questo approccio consiste, dunque, nel determinare *ex ante* quali sistemi di IA debbano essere oggetto di intervento normativo[37].

Nel *Digital Services Act*, invece, vi è una struttura che può essere definita 'piramidale' ossia prevede una serie di *due diligence obligations* gravanti sui prestatori di servizi digitali che si strutturano secondo quattro livelli ad intensità crescente: dalla 'base' della piramide ove sono indicate le misure applicabili a tutti i prestatori, fino all'apice, in cui sono previsti gli obblighi più stringenti attribuiti alle piattaforme online e ai motori di ricerca di dimensioni molto grandi[38].

---

anche S. Tommasi, *Digital Services Act*, cit., p. 281; G. Finocchiaro, *La proposta*, cit., p. 309 ss.; T. Mahler, *Between risk management and proportionality: The risk-based approach in the EU's Artificial Intelligence Act Proposal*, in *Nordic Yearbook of Law and Informatics*, 2022, p. 245 ss.

[36] Ai sensi dell'art. 5: «si annoverano i sistemi che sfruttano tecnologie subliminali per manipolare i comportamenti di una persona; quelli che abusano di persone vulnerabili e fragili; modelli volti a categorizzare real-time le persone fisiche in base ai loro dati biometrici per dedurne la razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche, o l'orientamento sessuale. Questi ultimi sistemi possono essere utilizzati per fini di sicurezza pubblica ma esclusivamente nel caso di ricerca di vittime di rapimento, tratta di esseri umani o persone scomparse, o per prevenire una minaccia di un attacco terroristico. Sono vietati poi i sistemi di *social scoring* 'per la valutazione o la classificazione di persone fisiche o di gruppi di essi'. Altri sistemi vietati sono quelli di polizia predittiva, che sfrutta gli algoritmi per prevedere le probabilità con cui può essere commesso un reato e tutte le informazioni ad esso legato. Proibiti sono anche i sistemi AI che svelano le emozioni delle persone sul posto di lavoro o nelle istituzioni scolastiche, ad eccezione in cui tali sistemi non vengano utilizzati per motivi medici o di sicurezza. Nell'ambito produttivo – saranno quindi vietati gli utilizzi di strumenti di sorveglianza *real time* dei dipendenti, ma anche i cd. software di *affective computing*, ossia quelle applicazioni volte a leggere le nostre emozioni per sfruttarle. Un rischio oggi sempre più reale».

[37] R. Gellert, *The role*, cit. p. 26.

[38] Per maggiori dettagli circa le novità introdotte si leggano i contributi di L. D'agostino, *Disinformazione e obblighi di compliance degli operatori del mercato e alla luce del nuovo Digital Services Act*, in *Media Laws*, 2023, p. 16 ss.; M.L. Bixio, *Gli obblighi applicabili a tutti i prestatori di servizi intermediari, ai prestatori di servizi di hosting e ai fornitori di piattaforme online* (artt. 11-32 – Capo III, Sez. 1, 2, 3, 4), in *Dir. int.*, 2023, p. 21 ss.; V. Colarocco, M. Cogode, *Gli obblighi applicabili a piattaforme online di dimensioni molto grandi (Artt. 33-34- Capo III, Sez. 5)*, in *Dir. int.*, 2023, p. 27 ss.; F. Piraino, *La responsabilità dei prestatori di servizi di condivisione di contenuti*

Il passaggio di ogni 'gradone' di *compliance* comporta la sottoposizione dell'operatore all'obbligo di conformarsi ad alcune disposizioni ulteriori che si aggiungono (e non si sostituiscono) a quelle degli stadi precedenti. Si tratta, quindi, di una pervasività graduata degli obblighi gravanti sui prestatori basata sulle specifiche attività compiute dai prestatori[39].

Entrambi i regolamenti lasciano un ampio margine di apprezzamento ai soggetti designati nel definire in dettaglio le misure da assumere, menzionando, in via generale, le *policies* da adottare al fine di gestire e mitigare i rischi connessi all'impatto dei loro servizi sui diritti fondamentali e interessi individuali e collettivi. La strategia prescelta parrebbe essere quella di lasciare liberi i soggetti designati di costruire le proprie 'regole interne' in autonomia secondo una logica *taylor made*.

I regolamenti forniscono indicazioni di carattere ampio sugli obiettivi da raggiungere, come pure una metodologia di analisi dei rischi e un elenco di possibili contromisure da considerare[40]. Sarebbe dunque riduttivo interpretare le previ-

---

online, in *Nuove leggi civ. comm.*, 2023, p. 146 ss.

[39] M.L. Bixio, *Gli obblighi*, cit., p. 21. In particolare, per quanto riguarda le piattaforme di grandi dimensioni, la prima *due diligence obligation* aggiuntiva attiene all'obbligo di effettuare *assesment* concernenti l'individuazione, l'analisi e la valutazione degli eventuali «rischi sistemici» derivanti dalla progettazione, dal funzionamento o dall'uso dei loro servizi e dei relativi sistemi (anche algoritmici). In proposito, l'art. 34 del *Digital Services Act* esige un'analisi specifica «e proporzionata ai rischi sistemici, tenendo in considerazione la loro gravità e la loro probabilità». Non solo, il DSA disciplina anche la fase successiva al *risk assessment*, imponendo l'adozione di «misure di attenuazione ragionevoli, proporzionate ed efficaci, adattate ai rischi sistemici specifici individuati a norma dell'articolo 34, prestando particolare attenzione agli effetti di tali misure sui diritti fondamentali». L'art. 35 contempla poi un elenco molto fitto di alcune possibili *mitigation measures*. Così, L. D'agostino, *Disinformazione*, cit., p. 2 ss.

[40] Sul concetto di *meta-regulation* o *enforced-self regulation*: v. N. Zingales, *The DSA as a Paradigm Shift for Online Intermediaries' Due Diligence*, in *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implications*, ed. by J. van Hoboke, J.P. Quintais, N. Appelman, R. Fahy, I. Buri, M. Straub, Berlin, 2023, p. 213 s., il quale, da un lato, evidenzia che «This approach, which on the one hand leaves businesses with a significant amount of discretion in the implementation of regulatory principles, and on the other involves a process of continuous evaluation and monitoring of the results, has been called 'metaregulation' or 'enforced self-regulation': 'meta' because one (macro) regulator oversees another (micro) regulator in their management of risk; 'enforced' because, in case of inadequacy of the self-regulatory practices, the (macro) regulator has the power to take enforcement measures», e, dall'altro lato, che «while the shift to a meta-regulatory model should be welcomed for enabling reflexive and adaptive regulation, we must also be weary of its risk of collapsing in the absence of well-resourced and independent institutions».

sioni contenute nei due regolamenti come semplici obblighi di condotta; appare invece più corretto ritenere che il legislatore abbia inteso costruire un sistema basato su una forma di *accountability* modulata in base alle circostanze.

Si può dedurre, allora, che Waymo, una volta approdato con le proprie flotte in Europa, sarà sottoposto a gradi diversi di responsabilizzazione, proprio perché i modelli di approccio al rischio prescelti dai regolamenti seguono linee non del tutto convergenti. Di conseguenza, non parrebbe corretto parlare di un unico principio di responsabilizzazione ma di un'*accountability* multilivello, che si modula in base alla scelta del legislatore se predefinire o meno le misure di prevenzione del rischio.

Partendo da questi presupposti, emergono due questioni critiche che meritano approfondimento. La prima riguarda come il concetto di rischio si inserisca all'interno del processo di responsabilizzazione e quali implicazioni quest'ultimo comporti sul tradizionale paradigma della responsabilità giuridica. La seconda, invece, concerne il rapporto che sussiste tra questo piano di anticipazione del rischio e il suo effettivo manifestarsi, con particolare attenzione ai casi di sinistri stradali e alla possibile attribuzione di responsabilità per danni a carico di Waymo.

Tali questioni corrono lungo linee parallele dal momento che, in merito alle auto a guida autonoma, emerge il tema cruciale di come questi sistemi recepiranno le diverse misure di *accountability* e di come la corretta o errata implementazione delle stesse dovrà essere valutata nella determinazione delle responsabilità in caso di incidenti che vedono coinvolti il robot-taxi.

5. *La diversa aggettivazione di rischio e di danno nei regolamenti*

Partendo dal primo dei due punti evidenziati, come accennato, una delle criticità maggiori rilevabili nel disegno regolativo europeo risiede nell'assenza di una definizione uniforme di che cosa si intenda per rischio. In effetti, si è osservata la presenza di aggettivazioni differenti di rischio così come di danno, che potrebbero determinare difficoltà nella classificazione unitaria delle condotte lecite o vietate, come pure nella definizione di *best practice* da adottare in logica coordinazione con il principio di *accountability*[41].

Più precisamente: nel GDPR non si riscontra una definizione predefinita di rischio. Per quanto concerne, invece, il concetto di danno, al *considerando* 75 come pure all'art. 82 esso viene qualificato come danno patrimoniale e non patrimoniale (qualificato testualmente come danno materiale e immateriale)[42].

---

[41] Dello stesso parere S. Tommasi, *Digital Services Act*, cit., p. 293 ss.

[42] Il tema del danno risarcibile ai sensi dell'art. 82 GDPR è questione ampiamente

Nel *Digital Services Act*, invece, assume un ruolo centrale il concetto di rischio sistemico previsto, ai sensi dell'art. 34, esclusivamente per le piattaforme di grandi dimensioni e definito come un rischio inevitabile (appunto inerente al sistema) anche se da attenuare e derivante dalla progettazione, dal funzionamento del servizio e dei relativi sistemi, compresi i sistemi algoritmici[43]. Ebbene, all'interno dell'articolo dedicato ai rischi sistemici non si fa riferimento specifico al concetto di danno, bensì a tutte quelle pratiche che possono determinare effetti negativi per l'esercizio dei diritti fondamentali ovvero causare «gravi conseguenze negative per il benessere fisico e mentale della persona».

Nel caso dell'AI Act, invece, sono indicate diverse categorie di rischio; categorie che, se per un verso, prendono in considerazione le medesime attività descritte dal DSA, per altro verso, non assumono la medesima distinzione legata alla dimensione della piattaforma o del motore di ricerca[44].

Relativamente al concetto di danno, poi, l'art. 5 dell'AI Act, dedicato alle pratiche proibite, dà rilievo non più, solamente, al danno fisico e mentale, ma adotta una concezione più ampia. Esso parla infatti di *significant harm* ovverosia di danno significativo alla persona o ad un gruppo di persone, quale elemento qualificante una pratica di intelligenza artificiale vietata[45]. In considerazione di ciò, tale configurazione potrebbe aprire a frontiere nuove di danno tecnologico,

---

dibattuta in dottrina; per maggiori dettagli si rinvia, *ex multis*, a G.M. Riccio, *Dati personali e rimedi: diritti degli interessati e profili risarcitori*, in *Nuova giur. civ. comm.*, 2022, II, p. 1125 ss.; S. Serravalle, *Il danno da trattamento dei dati personali nel GDPR*, Napoli, 2020; E. Tosi, *funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo*, in *Contr. impr.*, 2020, p. 1115 ss.; Id., *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, in *Danno resp.*, 2020, p. 433 ss.; S. Patti, *Il risarcimento del danno immateriale secondo la Corte di giustizia*, in *Nuova giur. civ. comm.*, 2023, II, p. 1146 ss.; C. Camardi, *Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea*, in *Nuova giur. civ. comm.*, 2023, II, p. 1136 ss.; Id., *Note critiche in tema di danno da illecito trattamento dei dati personali*, in *Jus civile*, 2020, p. 786 ss.; C. Scognamiglio, *Danno e risarcimento nel sistema del Rgpd: un primo nucleo di disciplina euro unitaria della responsabilità civile?*, in *Nuova giur. civ. comm.*, 2023, II, p. 1150 ss.; G. Calabrese, *Il danno da 'perdita di controllo dei dati personali'*, cit., p. 1112 ss.

[43] Cfr. L. D'Agostino, *Disinformazione*, cit., p. 35 ss.

[44] Dello stesso parere S. Tommasi, *Digital Services Act*, cit., p. 293 ss.

[45] Tale articolo ha subito significativi emendamenti rispetto alla versione originaria contenuta nella proposta. In particolare, si fa riferimento, più ampiamente, al concetto di danno significativo per le persone, e non più, invece, al più ristretto ambito del danno fisico o psicologico. Rileva questo aspetto ancora, S. Tommasi, *Digital Services Act*, cit., p. 295 ss.

dal momento che si tratta di una concezione più ampia sia di quella riscontrata nel GDPR che nel DSA.

Rispetto a tali aggettivazioni, si possono evidenziare tratti discrepanti tra i regolamenti che potrebbero causare difficoltà di coordinamento pratico, soprattutto per attività complesse come quella del robot-taxi. Facendo qualche esempio, per quanto attiene la piattaforma mediante cui avverrà l'interazione con Waymo, sarà necessario vagliare se i sistemi di raccomandazione per le offerte commerciali o i sistemi di selezione della pubblicità utilizzati, quandanche ammessi dal DSA quale forma di rischio sistemico, rientrino – al contrario – nelle pratiche di intelligenza artificiale vietate ai sensi dell'art. 5 dell'AI Act, perché ritenuti indebitamente manipolativi della volontà dell'utente. Non sarebbe infatti coerente con il sistema di prevenzione tale divaricazione nella definizione di rischio. Si pone poi la questione se, da un lato, il titolare del trattamento possa valutare liberamente e privatamente il rischio relativo al trattamento dei dati personali; mentre, dall'altro lato, il produttore dei sistemi di IA, che si basano proprio sulla lettura ed elaborazione algoritmica di tali dati, sia invece vincolato a seguire una valutazione già precostituita[46].

6. *'Accountability' e 'liability' a confronto*

A monte del discorso precedente, emerge come i regolamenti siano l'emblema del fatto che la natura della responsabilità sta acquisendo una dimensione polisemica, meglio ancora, polifunzionale. Sicurezza, prevenzione e precauzione del rischio sembrano essere stati assunti infatti nel novero dei principi ordinanti la tecnologia da parte del legislatore europeo[47].

---

[46] Non solo, si pongono numerose criticità tra l'esigenza di disporre di un'ingente mole di dati ai fini dello sviluppo di sistemi di intelligenza artificiale, da un lato, e la necessità di osservare il principio di minimizzazione dettato dal GDPR, dall'altro. Così, G. Finocchiaro, *Intelligenza artificiale. Quali regole?*, Bologna, 2024, p. 80 s.

[47] È opportuno specificare, in proposito, che la dottrina – ben prima dell'entrata in vigore di questi regolamenti – ha più volte riconosciuto i principi di prevenzione e di precauzione in riferimento all'interpretazione dell'art. 2050 c.c. Per maggiori dettagli, si rimanda a U. Izzo, *La precauzione nella responsabilità civile*, Padova, 2007; così anche F. Santonastasio, *Principio di precauzione e responsabilità d'impresa: rischio tecnologico e attività pericolosa per sua natura. Prime riflessioni su un tema di ricerca*, in *Contr. impr. eur.*, 2001, p. 21 ss. il quale ricostruisce l'incidenza del principio di precauzione sulla nozione di attività pericolosa, individuando in esso un concetto suscettibile di estendere l'ambito applicativo dell'art. 2050 c.c. anche nel caso in cui non vi sia certezza in merito al rischio cagionato da talune attività. Sul punto anche E. Del Prato, *Il principio di precauzione nel diritto privato: spunti*, in *Rass. dir. civ.*, 2009, p. 634 ss. Si rinvia, inoltre, a C. Castronovo, *Sentieri di responsabilità civile europea*, in *Eur. dir. priv.*, 2008, p. 787

Si tratta di enunciati che, a dire il vero, lambiscono da tempo la nozione di attività pericolosa; concetto all'interno del quale rientrano anche il trattamento dei dati personali, come pure la progettazione di sistemi di intelligenza artificiale o la moderazione di contenuti[48]. La novità dei regolamenti consiste allora nell'aver formalizzato questo tipo di approccio.

Si assiste ad una determinazione precostituita di obblighi aventi natura perlopiù procedimentale e deflativi del rischio, in favore degli interessati e degli utenti. Viene individuato poi il soggetto gravato di tali obblighi, a cui viene rimesso un certo margine di discrezionalità rispetto a come interpretarli e attuarli.

Sembra costituirsi, dunque, un nesso sempre più inscindibile tra l'attività del trattamento o di produzione da una parte, la dimensione organizzativa dall'altra e, infine, la predisposizione di misure idonee alla salvaguardia degli interessati-utilizzatori[49]. C'è chi ha parlato, a questo proposito, di cambiamento culturale, dal momento che la normativa incoraggia alla proattività sin dalle prime fasi di progettazione[50].

---

ss., per il quale «gli obblighi in cui si concretizza la precauzione [...] dalla prospettiva privatistica non sembrano aggiungere significati diversi a quello che trova sintetica espressione nella categoria della colpa». Da ultimo, si considerino i recenti contributi in materia di A. Cioni, *L'influenza indiretta del diritto europeo: il caso dei danni cagionati dai prodotti pericolosi per una riscoperta dell'art. 2050 c.c.*, in *Riv. dir. civ.*, 2023, p. 956 ss., come anche, C. Ippoliti Martini, *Il principio di precauzione e nuove prospettive della responsabilità civile della Pubblica amministrazione*, Milano, 2022.

[48] A ben vedere, prima dell'entrata in vigore del Reg. 2016/679/UE, era chiaro il rimando all'art. 2050 c.c. contenuto nel d.lgs. 196/2003 all'art. 15 (ora abrogato). In tal senso, il trattamento dei dati personali è stato inteso dall'ordinamento come attività rischiosa di per sé. Per tutti, si rimanda all'attenta ricostruzione di G. Navone, *Ieri, oggi e domani della responsabilità civile da illecito trattamento dei dati personali*, in *Nuove leggi civ. comm.*, 2022, p. 132 ss., il quale precisa come «il nostro legislatore volle riferirsi non soltanto alla lettera, ma anche, e forse soprattutto, alla storia applicativa dell'art. 2050 c.c. Per tal modo, infatti, si estese ai dati conseguenti all'illecito trattamento dei dati personali lo statuto normativo della responsabilità per esercizio di attività pericolose».

[49] Così, relativamente alla dimensione del trattamento dei dati personali, M. Renna, *Sicurezza e gestione del rischio nel trattamento dei dati personali*, in *Resp. civ. prev.*, 2020, p. 1343 ss.

[50] In tal senso, L. Califano, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, in *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, a cura di L. Califano e C. Colapietro, Napoli, 2017, p. 34, la quale evidenzia come «il regolamento intende uscire dalla logica del mero adempimento formale agli obblighi di legge, per approdare ad un cambiamento culturale importante, in cui la prima aspirazione per titolari e responsabili deve essere quella di ridurre,

Alla luce di quanto esposto, il principio di *accountability* sembra orientarsi verso la definizione di una specifica responsabilità di natura procedimentale o, più precisamente, organizzativa, che può essere classificata all'interno della categoria della responsabilità oggettiva per rischio di impresa[51]. È quest'ultimo un modello di responsabilità già adottato dal legislatore europeo anche nella configurazione di altre fattispecie di responsabilità civile, quali la responsabilità da prodotto difettoso (con riferimento al rischio di sviluppo), la responsabilità ambientale e, *de iure condendo*, nell'ambito delle proposte regolative volte a disciplinare la responsabilità derivante dall'utilizzo dell'intelligenza artificiale[52].

In questa prospettiva non pare azzardato ritenere che tutti i testi normativi prediligano una prospettiva di anticipazione dell'evento dannoso derivante da un'attività di impresa. In specie, essi prevedono, al loro interno, una serie di figure che si pongono in logica coordinazione con la prospettiva 'responsabilizzante' del soggetto individuato, di volta in volta, dalla normativa; si pensi, ad esempio, alle informazioni obbligatorie da rendere, agli obblighi di predisposizione di misure tecniche e di sicurezza, alle previsioni in materia di *data governance*, etc.[53].

L'introduzione del principio di *accountability* apre quindi all'idea di un agire responsabile volto alla deterrenza di possibili condotte lesive, sicché in tale modello sembrerebbe determinarsi un riposizionamento all'indietro rispetto alla

---

prevenendoli, i rischi di operazioni non consentite, o comunque non conformi».

[51] Si faccia riferimento, soprattutto, a 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.*, 2020, p. 1115 ss.; A. Mantelero, *Rischio e responsabilità nel reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, p. 144.

[52] Si sofferma sul punto G. Calabrese, *Il danno da perdita di controllo dei dati personali*, cit., p. 1114. Sul tema della sicurezza dei prodotti, per tutti si v. E. Al Mureden, *Sicurezza dei prodotti e responsabilità del produttore*, in *Profili attuali di diritto dei contratti per l'impresa*, a cura di M.N. Bugetti, Torino, 2020, p. 249 ss.; Id., *Il danno da prodotto conforme tra responsabilità per esercizio di attività pericolosa ed armonizzazione del diritto dell'Unione europea*, in *Corr. giur.*, 2020, p. 686 ss.; Id., *Sicurezza ragionevole degli autoveicoli e responsabilità del produttore nell'ordinamento italiano e negli Stati Uniti*, in *Contr. impr.*, 2012, p. 1505 ss.; G. Alpa (a cura di), *La responsabilità del produttore*, Milano, 2019; P. Pardolesi, *Riflessioni sulla responsabilità da prodotto difettoso in chiave di analisi economica del diritto*, in *Riv. dir. priv.*, 2017, p. 87 ss.; R. D'Arrigo, *La responsabilità del produttore. Profili dottrinali e giurisprudenziali dell'esperienza italiana*, Torino, 2006. Più risalente sul punto, F. Galgano, *Responsabilità del produttore*, in *Contr. impr.*, 1986, p. 995.

[53] Cfr. A. Bernes, *Dalla responsabilità civile alla responsabilità sociale d'impresa nella protezione dei dati personali: alla ricerca del rimedio effettivo*, in *Actualidad Juridica Iberoamericana*, 2023, p. 658 ss.

tradizionale linea di responsabilità per danni. In specie, esso si propone come obiettivo principale quello della prevenzione e, solo in subordine, si preoccupa della riparazione dei danni eventualmente cagionati[54]. Proprio per la sua portata innovativa, vi è chi definisce l'*accountability* come 'principio dei principi', dal momento che la sua osservanza garantisce il rispetto di tutti gli altri principi generali[55].

In questa prospettiva, siffatto approccio sembra riflettersi anche sulla figura della *liability* giacché il binomio sicurezza (tutela *ex ante*) e responsabilità (tutela *ex post*) pare sempre più inscindibile[56].

Detta altrimenti, la figura della responsabilità sta assumendo nel contesto tecnologico una veste sempre più sfaccettata e polifunzionale. Tale evoluzione impone dunque una riflessione sui cambiamenti che il paradigma della responsabilità sta assumendo. Alla luce dei principi europei in materia, emerge come questione fondamentale comprendere in che modo il concetto classico del *respondere* stia venendo ridefinito e trasformato dall'innovazione tecnologica e dal quadro normativo che tenta di regolarla.

Nella disamina del significato di responsabilità sembra inserirsi, infatti, un'accezione differente del termine che evoca un'aspettativa più ampia: a monte di un effettivo danno, l'*accountability* traccia l'obbligo di un'attività libera ma vigilata, a tutela dell'affidamento di un livello di sicurezza appropriato. Il presupposto giustificativo di tale arretramento della condotta consterebbe nel fatto che – mediante la prevenzione – sia possibile incidere in modo significativo sull'evento finale. Invero, i doveri di prevenzione, di mantenimento di un livello adeguato di sicurezza e di reazione tempestiva in caso di violazioni della sicurezza divengono funzionali ad assicurare la piena tutela dei diritti e delle libertà delle persone fisiche coinvolte[57].

In tal senso, sembra rinvenirsi una certa forma di pressione su colui che ha coordinato l'attività rischiosa, per indurlo a razionalizzarla nel miglior modo pos-

---

[54] In proposito, ancora, A. Bernes, *Dalla responsabilità*, cit., p. 658 ss.

[55] Si esprime in tal senso, rispetto soprattutto al GDPR, R. Celella, *Il principio di responsabilizzazione: la vera novità del GDPR*, in *Cyberspazio e diritto*, 2018, p. 211 ss.

[56] Rispetto all'approccio olistico dell'Unione, si rimanda a E. Bellisario, *Il pacchetto europeo sulla responsabilità per danni da prodotti e da intelligenza artificiale. Prime riflessioni sulle Proposte della Commissione*, in *Danno resp.*, 2023, p. 153 ss.; si è interrogato recentemente sul tema anche T. De Mari Casareto dal Verme, *Intelligenza artificiale e responsabilità civile. Uno studio sui criteri di imputazione*, Trento, 2024, p. 319 ss.

[57] Così, M. Renna, *Sicurezza e gestione del rischio nel trattamento dei dati personali*, in *Resp. civ. prev.*, 2020, p. 1343 ss.

sibile[58]. L'*agere* deve concretizzarsi, di fatto, in un'utilità effettiva per l'interessato, ovvero garantire quest'ultimo dal verificarsi di eventi lesivi che sono prevedibili e, dunque, risolvibili *ex ante*. Ecco che allora è possibile scorgere, in capo al titolare-fornitore, un obbligo giuridico di diligenza professionale nell'adozione di siffatte misure tecniche e organizzative; un obbligo che va oltre la mera verifica della compatibilità con le disposizioni del Regolamento, poiché le misure prescelte devono volgere alla realizzazione della massima efficacia pratica[59].

Dietro questa logica responsabilizzante di colui che trae utilità dall'utilizzo del bene tecnologico parrebbe configurarsi una visione del diritto civile con funzione regolatoria[60]. In specie, nel contesto dell'impresa *tech*, viene richiesto ai nuovi protagonisti digitali un livello sempre più alto di proattività nell'assunzione delle misure a prevenzione del rischio, accompagnato da una crescente attenzione all'impatto sociale di tali tecnologie innovative da loro sviluppate, come nel caso emblematico di Waymo.

Questa impostazione si riflette in modo significativo, tanto sulla qualificazione della condotta antigiuridica, quanto sull'attribuzione della responsabilità per l'evento dannoso.

La condotta illecita potrebbe infatti configurarsi, in astratto, ogni volta che le misure adottate risultino insufficienti o inidonee rispetto agli *standards* normativamente previsti. L'obbligo risarcitorio, pertanto, emergerebbe in tutti i casi in cui si verifichi una violazione del legittimo affidamento riposto nell'azione conforme (*compliant*) del soggetto designato quale responsabile[61]. In proposito,

---

[58] Della stessa opinione, C. Camardi, *Note critiche*, cit., p. 786 ss.

[59] Ancora, A. Bernes, *Dalla responsabilità*, cit., p. 670.

[60] Sul tema del diritto civile regolatorio si osservi C. Attanasio, *Profili ricostruttivi del diritto privato regolatorio*, Napoli, 2022; A. Zoppini, *Diritto privato generale, diritto speciale, diritto regolatorio*, in *Ars Interpretandi*, 2021, p. 37 ss.; Id., *Il diritto privato e i suoi confini*, Bologna, 2020; A. Gentili, *Il diritto regolatorio*, in *Riv. dir. bancario*, 2020, p. 23 ss.; così anche ai contributi contenuti in A. Zoppini, M. Maugeri (a cura di), *Funzioni del diritto privato e tecniche di regolazione del mercato*, Bologna, 2009. Si segnala, in proposito, anche le recenti riflessioni di T. dalla Massara, E. Nervi, *Il contratto è politica, riflessioni sul contemporaneo in una conversazione con Giuseppe Guizzi*, Torino, 2024.

[61] A questo ultimo tema si collega anche la questione di quale sia la lesione effettivamente patita dall'utilizzatore del sistema di intelligenza artificiale e interessato al trattamento. Tendenzialmente, infatti, la lesione sofferta dall'utente di servizi digitali è difficilmente individuabile in termini di conseguenze dannose prodotte o, comunque difficilmente quantificabile, trattandosi perlopiù di un danno non patrimoniale. Questo anche in ragione del fatto che spesso si tratta di lesioni minime a livello individuale ma che coinvolgono serialmente una pluralità di utenti. Approfondisce il tema, A. Bernes, *Dalla responsabilità*, cit., p. 670.

spetterà al titolare e al fornitore l'onere di dimostrare l'adeguatezza delle misure implementate in relazione allo specifico trattamento o alla progettazione effettuata, determinando così un'inversione dell'onere probatorio rispetto al regime classico della responsabilità civile[62].

7. *Il rapporto tra 'accountability' e 'liability' in caso di sinistri stradali causati da Waymo*

Delineati i tratti caratterizzanti di questa nuova forma di responsabilità, occorre soffermarsi sul secondo nodo critico precedentemente appuntato: come valutare l'interazione tra le misure di *accountability* imposte dai regolamenti e il processo decisionale autonomo di veicoli come Waymo, specialmente nell'ipotesi di incidenti che vedono coinvolto quest'ultimo[63]. La domanda che si pone

[62] Pertanto, l'obbligo risarcitorio non discenderebbe esclusivamente dagli effetti lesivi causati all'esito del trattamento o della progettazione del sistema di intelligenza artificiale, ma anche da ciò che è successo ancora prima che essi si verificassero in concreto, cioè a fronte dell'assenza o della sostanziale inidoneità delle misure tecniche ed organizzative richieste. In merito, F. Bilotta, *La responsabilità civile nel trattamento dei dati personali*, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d. lgs. n. 101/2018. Scritti in memoria di S. Rodotà*, a cura di R. Panetta, Milano, 2019, p. 445 ss., in spec. p. 461 laddove viene specificato che «se il danno si verifica, è del tutto inconferente il grado di colpevolezza che ha caratterizzato la loro condotta: potremmo definirla una responsabilità per pura causalità».

[63] La dottrina si è recentemente interrogata a fondo sul tema della responsabilità da sinistro stradale causato dalla circolazione di un'auto a guida autonoma. V. per tutti, A. Albanese, *Mobilità del futuro e funzione preventiva della responsabilità civile*, in *Eur. dir. priv.*, 2023, p. 439 ss.; G. Calabresi, E. Al Mureden, '*Driverless cars' e responsabilità civile*, in *Dir. bancario*, 2020, p. 7 ss.; E. Al Mureden, *Autonomous car*, cit., p. 895 ss.; M. Ratti, *Riflessioni in materia di responsabilità civile e danno cagionato da dispositivo intelligente alla luce dell'attuale scenario normativo*, in *Contr. impr.*, 2020, p. 1182 ss.; S. Pellegatta, *Automazione nel settore 'automotive': profili di responsabilità civile*, in *Contr. impr.*, 2019, p. 1419 ss.; A. Albanese, *La responsabilità civile per i danni da circolazione dei veicoli ad elevata automazione*, in *Eur. dir. priv.*, 2019, p. 1007 ss.; F.P. Patti, *The European Road*, cit., p. 125 ss.; G. Votano, *La responsabilità da circolazione stradale nella fase di transizione dai veicoli tradizionali alle auto a guida automatica*, in *Danno resp.*, 2019, p. 330 ss.; D. Cerini, A. Pisani Tedesco (a cura di), *'Smart mobility', 'smart cars' e intelligenza artificiale: responsabilità e prospettive*, Torino, p. 2019; A. Davola, *A Model for Tort Liability in a World of Driverless Cars: Establishing a Framework for the Upcoming Technology*, in *Idaho L. Rev.*, 2018, p. 592 ss.; A. Davola, R. Pardolesi, *In viaggio col robot: verso nuovi orizzonti della r.c. auto ('driverless')?*, in *Danno resp.*, 2017, p. 625 ss.; U. Ruffolo, *'Self-driving car', auto 'driverless' e responsabilità*, in *Intelligenza*

è come i sistemi di intelligenza artificiale elaboreranno e applicheranno le misure di *accountability* implementate al loro interno e come ciò potrebbe influire sull'attribuzione delle responsabilità in caso di sinistri.

È necessario tenere a mente, anzitutto, che l'indipendenza che contraddistingue sempre più la cd. volontà macchinica non consente di tracciare una linea diretta tra *input* (la programmazione umana) e *output* (le azioni del veicolo a guida autonoma). Detta altrimenti, i moderni sistemi di intelligenza artificiale sviluppano una capacità decisionale autonoma che crea una discontinuità tra queste fasi precedentemente connesse. Inoltre, questi sistemi algoritmici avanzati si contraddistinguono per un'intrinseca opacità, in quanto assimilabili a scatole nere all'interno delle quali è di fatto impossibile ricostruire il percorso logico che ha portato ad una determinata decisione[64].

---

artificiale e responsabilità, a cura di U. Ruffolo, Milano, 2017, p. 39 ss.; M.C. Gaeta, *Automazione e responsabilità civile automobilistica*, in *Resp. civ. prev.*, 2016, p. 1725. Si segnala, in proposito, come anche negli Stati Uniti sia ancora acceso il dibattito circa il tema della responsabilità in caso d'incidente con autoveicoli a guida autonoma. In proposito, rimane aperta la questione sul soggetto che dovrebbe assumersi siffatta responsabilità. Per un maggior approfondimento del tema si segnalano i contributi di T. Winkle, *Product Development within Artificial Intelligence, Ethics and Legal Risk. Exemplary for Safe Autonomous Vehicles*, Munich, 2022; K. Atkinson, *Autonomous cars: a driving force for change in motor liability and insurance*, in *17 Scripted*, 2020, p. 125 ss.; M. Chatzipanagiotis, G. Leloudas, *Automated vehicles and third-party liability: a European perspective*, in *University of Illinois Journal of Law, Tech. and Policy*, 2020, p. 109 ss.; K.S. Abraham, R.L. Rabin, *Automated vehicles and manufacturer responsability for accidents: a new legal regim for a new era*, in *105 Virginia L. Rev.*, 2019, p. 127 ss.; D. Adkisson, *System-Level Standards: Driverless Cars and the Future of Regulatory Design*, in *University of Hawaii L. Rev.*, 2018, p. 1 ss.; T. Hresko Pearl, *Fast & furious: the misregulation of driverless cars*, in *73 New York University annual survay of american law*, 2017, p. 19 ss.; M. Geistfeld, *A Road Map for Autonomous Vehicles*, cit., p. 1611 ss.; G.E. Marchant, R.A. Lindor, *The Coming Collision between Autonomous Vehicles and the Liability System*, in *Santa Clara L. Rev.*, 2012, p. 1321 ss.

[64] In quella che è stata efficacemente definita come «*Black Box Society*» da F. Pasquale, *The Black Box Society. The secret Algorithms That Control Money and Information*, Cambridge-London, 2015, la trasparenza dei processi che porta all'acquisizione e all'elaborazione delle informazioni relative alle operazioni algoritmiche del software incorporato nel prodotto è una questione centrale nella valutazione della difettosità. Per una prospettiva più ampia v. 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 leggi civ. comm.*, 2018, p. 1209 ss.; C.A. Tschider, *Beyond the Black Box*, in *Denver L. Rev.*, 2018, p. 683 ss.; G. Sartor, F. Lagioia, *Le decisioni algoritmiche tra etica e diritto*, in *Intelligenza artificiale. Il diritto, i diritti, l'etica*, a cura di U. Ruffolo, Milano, 2020, p. 68 ss.

La combinazione di questi due fattori rende particolarmente spinosa l'identificazione e l'attribuzione delle responsabilità qualora si verifichi un sinistro stradale che vede coinvolta una macchina a guida autonoma come Waymo. In simili ipotesi, è ragionevole prevedere l'assenza di un rapporto diretto di causa-effetto tra condotta umana ed incidente, dal momento che tra la programmazione iniziale del veicolo e il sinistro si interpone un sistema di interazioni difficilmente prevedibili *ex ante*; come accennato, la macchina elabora costantemente dati personali e ambientali, prende decisioni in tempo reale e si adatta alle condizioni mutevoli del traffico[65]. Ne deriva che l'avvento dei veicoli autonomi determinerà un sostanziale superamento della tradizionale centralità dell'errore umano quale principale fattore causale degli incidenti stradali.

Pertanto, l'unico parametro di valutazione dell'affidabilità di tali sistemi parrebbe essere la corretta e continuativa implementazione delle misure di sicurezza prescritte dalla normativa di riferimento. Sicché, il processo di responsabilizzazione delle macchine a guida autonoma e *lato sensu* di educazione alla scelta diverrà verosimilmente un fattore piuttosto rilevante nella ponderazione delle

---

[65] In proposito, occorre menzionare il cd. *trolley problem*. La formulazione originale di questo problema coinvolgeva il conducente del tram, il cui ruolo è pienamente analogo al conducente di un veicolo autonomo (il sistema operativo), in proposito v. P. Foot, *Virtues and Vices and other essays in moral philosophy*, Berkeley, 1978, p. 19 ss. Il problema del *trolley* è stato successivamente riformulato nel seguente modo: se, dati due binari, sia o meno corretto ritenere doveroso che un osservatore sia tenuto ad impedire che il tram prosegua sulla propria strada dove si trovano cinque persone, mediante l'azionamento di un interruttore che devierebbe il tram sull'altro binario dove si trova un singolo lavoratore, il quale sarebbe dunque destinato a morire per salvarne cinque. Vedi J.J. Thomson, *The Trolley Problem*, in *94 Yale L. Journ.*, 1985, p. 1395 ss.; Id., *Turning the trolley*, in *Philos Public Aff.*, 2008, p. 359 ss. Questa versione del problema del *trolley* ha attirato considerevole attenzione anche per quanto attiene le *driverless cars.* Si segnalano in proposito: H. Zhan, D. Wan, *Ethical Considerations of the Trolley Problem in Autonomous Driving: A Philosophical and Technological Analysis*, in *World Electr. Veh. Journ.*, 2024, p. 403 ss.; J. Caro Burnett, S. Kaneko, *Is Society Aeady for AI ethical decision making? Lessons from a Study on Autonomous Cars*, in *J. Behav. Exp. Econ.*, 2022, p. 101881 ss.; E. Awad, S. Dsouza, R. Kim, J. Schulz, J. Henrich, A. Shariff, J.F. Bonnefon, I. Rahwan, *The Moral Machine Experiment*, in *Nature*, 2018, p. 59 ss.; J.F. Bonnefon, A. Shariff, I. Rahwan, *The Social Dilemma of Autonomous Vehicles*, in *Science*, 2016, p. 1573 ss.; Id., *Psychological roadblocks to the adoption of self-driving vehicles*, in *Nature Human Behaviour*, 2017, p. 694 ss.; S. Nyhom, J. Smids, *The Ethics of Accident-Algorithms for Self-Driving Cars: an Applied Trolley Problem?*, in *Ethic Theory Moral Practice*, 2016, p. 1275 ss.; F. Kamm, *The trolley mysteries*, Oxford, 2015; N.J. Goodall, *Machine Ethics and Automated Vehicles*, in *Road Vehicle Automation*, eds. by G. Meyer, S. Beiker, Dordrecht, 2014, p. 93 ss.

diverse condotte ritenute concausa dell'incidente, soprattutto nell'ipotesi in cui quest'ultime risultassero non conformi agli *standard* di sicurezza prestabiliti.

Di conseguenza, il fulcro dell'imputazione della responsabilità sembra traslare dall'elemento della condotta attiva, durante la circolazione stradale, alla diligenza nell'amministrazione *ex ante* del sistema, con riferimento soprattutto alla garanzia della sicurezza della circolazione, grazie all'implementazione delle misure imposte. Sicché, il rapporto dialettico tra *accountability* e *liability* risulterà caratterizzato da un vincolo di interdipendenza sempre più stringente, destinato a consolidarsi ulteriormente con la diffusione di tali veicoli automatizzati nel mercato unico.

È ragionevole ritenere, dunque, che il legame tra i due profili di responsabilità (*ex ante* ed *ex post*) costituirà presumibilmente un elemento distintivo del nuovo paradigma normativo in materia di circolazione dei veicoli autonomi.

In virtù del quadro tratteggiato, i soggetti gravati dagli obblighi di *compliance* europea – segnatamente il fornitore dell'algoritmo, il produttore del veicolo e il proprietario dello stesso – saranno tenuti, ciascuno nel proprio ambito di competenza, all'implementazione delle prescritte misure di sicurezza[66].

---

[66] Non si è volutamente accennato, in proposito, al tema dibattuto in dottrina se dotare la macchina stessa di una propria personalità al fine di assicurare una responsabilità diretta, con patrimonio con cui risponderne. In proposito, v. U. Ruffolo, *La 'personalità elettronica'*, in *Il diritto, i diritti, l'etica*, Milano, 2020, p. 213 ss.; Id., *Il problema della personalità elettronica*, in *Journal of Ethics and Legal Technologies*, II, 2020, p. 75 ss.; v. poi P. Moro, *Macchine come noi. Natura e limiti della soggettività robotica*, in *L'intelligenza artificiale*, cit., p. 45 ss.; U. Ruffolo, A. Amidei, *Intelligenza artificiale e diritti della persona: le nuove frontiere del 'transumanesimo'*, in *Giur. it.*, 2019, p. 1658 ss.; E. Quarta, *Soggettività dei robots e responsabità*, in *La nuova proc. civ.*, 2018, p. 1 ss.; non può che essere citato sul tema, infine, G. Teubner, *Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten*, in *Archiv für civilistische Praxis*, 2018, p. 155 ss., trad. it., *Soggetti giuridici digitali? Sullo 'status' privatistico degli agenti software autonomi*, a cura di P. Femia, Napoli, 2019; sul tema, in generale, si rinvia anche ai contributi contenuti nell'ultimo fascicolo monografico 2024 di *Storia Metodo Cultura nella scienza giuridica europea* intitolato emblematicamente *Le soggettività*. Per quanto attiene, nello specifico, al rapporto tra autoveicolo e proprietario dello stesso, vi è chi ha richiamato l'antico rapporto tra schiavo e *dominus*, v. M. Gemelli, *Il robot come 'servus novus': spunti di comparazione e tentativi storici di approccio alla disciplina della odierna intelligenza artificiale*, in *Cammino diritto*, 2023, p. 91 ss.; L. Franchini, *Disciplina romana della schiavitù e intelligenza artificiale odierna. Spunti di comparazione*, in *Dir. mer. tec.*, 2020, p. 1 ss.; N. Busto, *La personalità elettronica dei robot: logiche di gestione del rischio tra trasparenza e fiducia*, in *Ciberspazio e diritto*, 2017, p. 500 ss. Si vedano, inoltre, le interviste pubblicate su rinomate testate giornalistiche di L. Floridi, *Roman Law offers a better Guide to Robot Rights than sci-fi*, in *Financial Times*, 22 febbraio 2017, p. 12 ss.; E. Cantarella, *Chi paga i danni di un robot? La risposta è*

Tale ripartizione degli obblighi trova esemplificazione paradigmatica nel caso di Waymo, laddove la I-Pace, vettura integralmente elettrica prodotta da Jaguar, incorpora il *software* di guida autonoma sviluppato da Google Alphabet; oltre a ciò, si tenga presente che Waymo sta perfezionando numerose *partnership* commerciali con operatori di trasporto non di linea, *in primis* Uber, per la fornitura di veicoli autonomi destinati ai servizi di trasporto passeggeri e consegna alimentare[67].

Tuttavia, si appunta che la complessità tecnico-strutturale intrinseca a questi autoveicoli renderà oltremodo complessa – sul piano del binomio *accountability-liability* – una netta demarcazione degli obblighi e delle connesse responsabilità del produttore del veicolo e lo sviluppatore del *software*, attesa l'interdipendenza dei rispettivi ruoli, sia nella fase iniziale di progettazione e di realizzazione, sia nel successivo stadio di immissione del veicolo sul mercato[68].

In secondo luogo, anche il proprietario si dovrà inserire in questo processo articolato di prevenzione dei rischi, dal momento che avrà l'obbligo di mantenere il veicolo costantemente aggiornato, atteso che eventuali omissioni o inesattezze nell'esecuzione degli aggiornamenti potrebbero concorrere causalmente al verificarsi di eventi dannosi[69].

Ebbene, a fronte di questa prospettiva di azione combinata tra più attori, una possibile soluzione potrebbe essere quella di stilare modelli di *best practice* utili a

---

nell'antica Roma, in *Corriere della Sera*, 24 febbraio 2017, p. 25.

[67] https://waymo.com/blog/2024/09/waymo-and-uber-expand-partnership.

[68] In tutte le vicende che hanno coinvolto auto a guida autonoma, si è riscontrato il tema dell'interconnessione, nella definizione della responsabilità, tra produttore del *software*, produttore del veicolo e conducente (o proprietario). Si osservi, in proposito, il cd. caso Uber-Elain Herzberg, verificatosi nel 2018, a Tempe in Arizona. Si è trattato del primo incidente mortale documentato con un veicolo a guida autonoma. Il veicolo Uber, una Volvo XC90 in modalità autonoma, investì la Signora Herzberg mentre attraversava la strada con la bicicletta. L'analisi tecnica rivelò che il sistema aveva rilevato la sua presenza sei secondi prima dell'impatto, classificandola in modo progressivo come oggetto sconosciuto, veicolo e infine bicicletta. Un secondo e mezzo prima dello scontro, il sistema aveva riconosciuto la necessità di una frenata di emergenza, ma non era progettato per avvisare l'operatore umano, che nel frattempo risultava distratto e non è pertanto intervenuto tempestivamente. Come conseguenza, Uber sospese immediatamente i test sui veicoli autonomi in Arizona e raggiunse un accordo risarcitorio privato con la famiglia della defunta Signora Herzberg. Per maggiori dettagli sulla vicenda si rimanda al seguente articolo, https://www.bbc.com/news/technology-54175359.

[69] Della stessa opinione sono A. Davola, R. Pardolesi, *In viaggio col robot*, cit., p. 620, in cui specificano che «bisogna prendere atto che il ripensamento della responsabilità civile nel settore automobilistico dovrà necessariamente coinvolgere la figura del proprietario del mezzo».

questi soggetti per la ripartizione e gestione delle misure preventive del rischio; tutto ciò nell'ottica di un approccio che punti a nuove forme di co-responsabilizzazione tra i soggetti, soprattutto nel caso di imprevedibili malfunzionamenti del veicolo[70].

Ciononostante, è doveroso evidenziare come – anche all'interno di questa impostazione di prevenzione del rischio condivisa tra più soggetti – permanga un ineliminabile margine di aleatorietà, in quanto gli eventi dannosi potrebbero scaturire, non tanto da un'erronea implementazione di siffatte misure, quanto piuttosto da una concatenazione di micro-decisioni algoritmiche, le quali risultano influenzate da una serie di variabili non prevedibili *ex ante*.

Nelle ipotesi di decisioni autonome da parte della macchina, che deviano da ogni pronostico e che determinano un incidente, occorrerà allora porre dei limiti all'eventuale responsabilità degli attori gravati dagli obblighi di *compliance*[71].

Per un verso, sarebbe, in effetti, sproporzionata l'attribuzione di una responsabilità a questi soggetti anche in un'ipotesi di avveramento del rischio che avviene nonostante la piena conformità del mezzo rispetto agli standard normativi richiesti. Si tratterebbe, a ben vedere, di un caso fortuito[72].

Per altro verso, tuttavia, questa impostazione rischierebbe di far ricadere sui terzi le conseguenze dannose dei rischi non previsti o non evitati che occorrono dalla guida del veicolo[73]. In questa prospettiva, difatti, il corretto adempimento degli obblighi di *accountability* potrebbe assumere una valenza protettiva per fornitori, produttori e proprietari del veicolo a guida autonoma. Difatti, l'assunzio-

---

[70] In proposito, nel caso di difetti di funzionamento del veicolo, nonché da condotte umane anomale, potrebbe continuare ad essere disciplinato ricorrendo alle regole che attualmente governano la responsabilità del fabbricante, in proposito v. E. Al Mureden, *Event data recorder*, cit., p. 402.

[71] In merito, v. sempre E. Al Mureden, *L'Automazione della guida*, cit., p. 167 ss., in cui richiamando la cd. *preemption doctrine*, di tradizione americana, evidenzia come la conformità del veicolo agli *standard* normativi richiesti, costituisce «un limite oltre a cui non è configurabile una responsabilità civile in capo al produttore che abbia immesso sul mercato un veicolo conforme». Di conseguenza, la *regulatory compliance* fungerebbe anche da forma di difesa per i soggetti sottoposti a tali obblighi.

[72] Si rimanda in proposito al recente saggio di A. Gentili, *Regole per l'intelligenza artificiale*, in *Contr. impr.*, 2024, p. 1043 ss. spec. p. 1049 ove l'Autore specifica che «L'apparato normativo di prevenzione sembra indirizzato a far sì che i sistemi risultino conformi all'insieme di requisiti e cautele richiesti dal regolamento. Ciò può far presumere che, se i sistemi sono conformi, l'eventuale avverarsi di un rischio che neppure la conformità ha potuto evitare fuoriesca dall'area di responsabilità di fornitori, importatori, distributori, *deployer*».

[73] Nuovamente, v. A. Gentili, *Regole*, cit., p. 1049.

ne delle misure preventive richieste potrebbe configurarsi, in astratto, come un elemento esimente della responsabilità, data l'accidentalità dell'evento nemmeno sventato dalla corretta *compliance*; aspetto particolarmente significativo se si considera la natura intrinsecamente opaca di sistemi intelligenti come Waymo. Di conseguenza, nel caso di incidenti causati da veicoli conformi agli *standard* legislativi, il tema dell'allocazione dei costi scaturenti dalle attività lesive si rivelerà verosimilmente ancora più spinoso.

In via generale, a seguito dell'introduzione di veicoli intelligenti come Wayo, si porrà sempre più il tema di dover dar vita ad un quadro normativo idoneo a fornire un sufficiente livello di certezza e di prevedibilità riguardo alle responsabilità scaturenti dalla commercializzazione e dalla circolazione di simili mezzi altamente automatizzati ed un'efficace allocazione dei costi degli incidenti causati dalla loro circolazione.

In quest'ottica, alla luce delle diverse criticità emerse, in una prospettiva *de iure condendo* autorevole dottrina suggerisce che una possibile soluzione sarebbe quella di «socializzare i costi dei nuovi incidenti causati dall'automazione». Tale proposta si ispira al modello statunitense del cd. *Market Enterprise Responsability*, che prevede l'istituzione di un fondo collettivo per la gestione del rischio, alimentato direttamente dai contributi degli operatori del settore dell'automazione e finalizzato a garantire il risarcimento dei danni causati da sistemi automatizzati[74]; un'ipotesi che, a ben vedere, si porrebbe in linea con la logica alla base del principio di *accountability* quale forma di responsabilità oggettiva per rischio di impresa.

Detta soluzione offrirebbe un vantaggio duplice: per un verso consentirebbe di superare le criticità probatorie inerenti all'individuazione del nesso causale tra la condotta dei singoli attori e l'evento dannoso; per altro verso assicurerebbe una tutela più efficace ed immediata ai soggetti danneggiati, evitando loro l'onere di complesse e, soprattutto, costose azioni legali contro i giganti del *tech* dall'esito verosimilmente incerto.

Conseguentemente, l'istituzione del fondo realizzerebbe un meccanismo di equa ripartizione del rischio derivante dall'impiego di sistemi caratterizzati da livelli 4 o 5 di automazione tra tutti i soggetti della filiera, evitando una concentrazione sproporzionata degli oneri risarcitori in capo a taluni attori. Tale soluzione consentirebbe l'implementazione di un paradigma di responsabilità solidale e ripartita, idoneo a promuovere l'adozione di prassi virtuose e l'innalzamento degli *standard* di sicurezza da parte di tutti i soggetti coinvolti.

---

[74] Nuovamente sul punto E. Al Mureden, *L'Automazione della guida*, cit., p. 170 s.

Una simile impostazione si porrebbe in linea, peraltro, con quella visione regolatoria del diritto civile a cui precedentemente si accennava, in quanto, anche nell'ipotesi di verificazione dell'evento dannoso, viene richiesto agli operatori del settore un più elevato grado di proattività, nell'ottica della socializzazione del danno e della tutela dei soggetti maggiormente vulnerabili.

8. *Quali nuove responsabilità per Waymo?*

Nella prospettiva dell'evoluzione dei sistemi di trasporto autonomo di livello 4 o 5 di automazione come esemplificato dal caso Waymo, il paradigma della responsabilità civile è chiamato ad assumere una connotazione marcatamente polifunzionale, assurgendo a strumento di regolazione del mercato digitale.

Le *driverless cars* rappresentano il punto di svolta di una rivoluzione *disruptive* del settore della mobilità: esse sono destinate non solo a ridefinire radicalmente il comparto dei trasporti, ma ad imporre, altresì, una rivisitazione sostanziale delle categorie giuridiche tradizionali, le quali dovranno necessariamente essere oggetto di una rilettura attraverso rinnovate prospettive ermeneutiche, al fine di garantirne l'armonizzazione con i principi e le logiche sottese a tali sistemi tecnologicamente avanzati, in un'ottica di efficace contemperamento tra innovazione e tutela dei diritti fondamentali.

Tale processo di adattamento risulta particolarmente significativo, soprattutto con riferimento ai diversi profili della responsabilità che attengono alla circolazione stradale di veicoli a guida autonoma.

In tal senso, il rapporto che astringe *accountability* e *liability* impone una riflessione sulla struttura e sulle funzioni che oggi può svolgere la responsabilità nel regolare la circolazione di veicoli a guida autonoma e i possibili sinistri che vedranno tali auto coinvolte.

L'introduzione sistematica di diversi piani di *accountability* in tutti gli atti regolativi afferenti al settore digitale, unitamente all'estensione del concetto di responsabilità verso una dimensione preventiva multilivello, operante in sinergia con la tradizionale figura della responsabilità per danni, determina una sostanziale ridefinizione del paradigma nel suo complesso. In questa prospettiva, si assiste ad un progressivo arretramento della soglia del *respondere*, tale per cui le diverse declinazioni dell'*accountability* assumono una rilevanza preminente rispetto alla *liability* nei settori caratterizzati da elevata automazione.

La funzione sociale sottesa alla prevenzione del rischio pare porsi in diretta correlazione con una visione del diritto civile con funzione regolatoria. È evidente, infatti, che gli operatori del mercato sono chiamati ad un crescente livello di proattività nell'implementazione delle prescritte misure di *compliance* richieste,

nonché un'attenzione particolare all'impatto sociale che le nuove tecnologie da loro prodotte, come Waymo, possono avere.

Tale impostazione, pur presentando delle criticità applicative, si inserisce coerentemente nel quadro dei principi europei di ultima generazione, volti alla tutela dei diritti fondamentali della persona nel contesto dell'accelerazione tecnologica determinata dall'avvento di sistemi come Waymo.

Si tratta, a ben vedere, di principi che si atteggiano a contro-limiti che tentano di ponderare l'incedere della *techne* e, in un certo senso, di quella che può essere definita la volontà macchinica.

Diritto penale e intelligenza artificiale: il problema della colpa

di **Matthias Da Rold**

1. *Una nuova sfida per il penalista. Note introduttive*

Sono trascorsi più di vent'anni da quando Federico Stella invitava la penalistica italiana a fare i conti coi problemi legati al progresso tecnico-scientifico[1]. Ai suoi tempi, le principali sfide per il diritto penale si ponevano in settori ben delimitati della vita sociale ed economica: parlando dei cosiddetti «problemi della modernità», si faceva soprattutto riferimento alla questione ambientale, alle innovazioni in campo medico, alla grande industria alimentare e così via. Oggi, invece, il penalista è chiamato a confrontarsi con una tecnologia trasversale, che pervade ogni ambito della vita quotidiana e ha impatti niente affatto trascurabili. Che lo si guardi con favore o con scetticismo, l'impiego di tecniche di «intelligenza artificiale» (IA) è ormai un dato di realtà che dev'essere osservato (anche) attraverso le lenti dello studioso di diritto penale[2].

Prima di addentrarci nelle questioni più delicate che, a nostro avviso, questa innovazione tecnologica pone nelle aree di competenza del diritto penale, tuttavia, è giusto il caso di fare qualche precisazione preliminare, anche – e in particolare – per consentire al lettore di conoscere fin da subito i contorni del nostro intervento.

---

[1] F. Stella, *Giustizia e modernità*, Milano, 2001, p. 3.

[2] Così già F. Basile, *Diritto penale e Intelligenza Artificiale*, in «Giurisprudenza italiana», 2019, supplemento, pp. 67-74.

Trattando il tema della «intelligenza artificiale», spesso si tende a incentrare gran parte del discorso sulla possibilità – o impossibilità – di rinvenire in essa delle caratteristiche tipiche dell'essere umano. Anche chi studia il diritto penale si sofferma frequentemente su questioni concernenti l'assimilabilità della macchina all'uomo, e dai risultati di questo confronto fa discendere le proprie conclusioni giuspenalistiche[3]. Senza nulla togliere alle molte riflessioni sull'intelligenza artificiale aventi carattere ontologico, in questa sede vorremmo provare a guardare a tale fenomeno in maniera più concreta e «relativa», apprezzando cioè i suoi effetti nel mondo reale indipendentemente dalla sua natura (nelle pagine seguenti usiamo la locuzione «intelligenza artificiale», o la relativa abbreviazione, solo nella misura in cui non rischia di incidere sull'accuratezza dell'esposizione).

Questo differente approccio – il quale riposa, appunto, su un cambio di prospettiva – facilita e, anzi, promuove un altro tipo di indagine: un'indagine che ha ad oggetto l'ammissibilità di una risposta penale tradizionale a fronte delle peculiarità dell'azione artificiale intelligente. In altre parole, se si focalizza l'attenzione sull'atto (artificiale) e si decide di non indugiare nella «personificazione» di chi lo ha materialmente posto in essere, ci si vede costretti a esaminare la possibilità giuridica di rimproverare il fatto nel suo complesso all'essere umano (sempre che non si condivida la scelta – anzitutto politica – di rinunciare a una reazione statale punitiva nei casi di offese derivanti dall'utilizzo di siffatti sistemi).

---

[3] Particolarmente nutrita è la letteratura – di segno favorevole e contrario – formatasi attorno al tema della responsabilità penale diretta della macchina intelligente. Sul punto, si veda, per l'estero, G. Hallevy, *The Criminal Liability of Artificial Intelligence Entities–from Science Fiction to Legal Social Control*, in «Akron Intellectual Property Journal», 2010, 4, 2, pp. 171-201; G. Seher, *Intelligente Agenten als «Personen» im Strafrecht?*, in *Intelligente Agenten und das Recht*, a cura di S. Gless e K. Seelmann, Baden-Baden, 2016, pp. 45-60; N. Markwalder e M. Simmler, *Zur strafrechtlichen Verantwortlichkeit von Robotern und künstlicher Intelligenz*, in «Aktuelle Juristische Praxis», 2017, 2, pp. 171-182; W. Wohlers, *Die «ePerson»: ein tauglicher Adressat strafrechtlicher Sanktionen?*, in *Schuldgrundsatz. Entstehung – Entwicklungsgeschichte – aktuelle Herausforderungen*, edito da W. Wohlers e K. Seelmann, Tubinga, 2024, pp. 257-278; in Italia, invece, il tema è stato ripreso da pressoché tutti gli autori che si sono occupati di diritto penale e intelligenza artificiale: sia quindi consentito rinviare, su tutti, ad A. Cappellini, Machina delinquere non potest*? Brevi appunti su intelligenza artificiale e diritto penale*, in «Criminalia», 2018, 13, pp. 499-520; C. Piergallini, *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?*, in «Rivista italiana di diritto e procedura penale», 2020, 4, pp. 1745-1774; D. Piva, *Machina discere, (deinde) delinquere et puniri potest*, in *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, a cura di R. Giordano, A. Panzarola, A. Police, S. Preziosi e M. Proto, Milano, 2022, pp. 681-693.

In questo senso, un discorso metafisico finisce dunque col cedere il passo, mentre diviene chiaramente decisivo il grado di dipendenza della condotta artificiale dal fattore umano; ossia, per dirla al contrario, il suo livello di originalità e autonomia.

Ebbene, per non lasciarsi sviare da formule letterali preconfezionate e dal dubbio significato, o da semplificazioni volte più a suggestionare che a chiarire, occorre che anche il giurista, nel compiere le proprie considerazioni sul fenomeno dell'IA, prenda le mosse dal dato tecnico. Ciò vuol dire, in primo luogo, comprendere quali siano i meccanismi di funzionamento fondamentali dei sistemi di intelligenza artificiale, ovvero esplorare i modelli in base ai quali risulta possibile, per un sistema informatico, emanciparsi da un contributo umano totalizzante.

2. *Breve ma indispensabile parentesi tecnica sui sistemi «intelligenti»*

L'uso continuo e indiscriminato della formula «intelligenza artificiale» non contribuisce certo alla chiarezza del dibattito sulla tecnologia in questione. Al di là dell'annoso problema definitorio[4] – che qui scegliamo di non approfondire –, ciò che più importa, ai fini di un'analisi giuridica, è intendersi sulle effettive capacità di questi sistemi informatici emergenti.

Per cogliere in pieno i tratti dell'azione artificiale intelligente (noi preferiamo qualificarla come «autonoma») e poter fare delle osservazioni in punto di diritto penale sufficientemente solide, crediamo sia necessario resistere alla tentazione di ricorrere a espressioni vaghe o comunque imprecise, rifacendosi invece il più possibile agli insegnamenti del sapere tecnico-scientifico. È consultando la letteratura di settore e riportandone fedelmente i risultati, infatti, che il giurista può sperare di non incorrere in errori sui presupposti fattuali del suo discorso.

2.1. Tanto premesso, iniziamo con il dire che l'autonomia di un sistema informatico non può che avere origine nella capacità di interagire con l'esterno.

Già solo da un punto di vista logico, lo studio dell'ambiente in cui il sistema si ritrova a operare precede quello relativo al processo di «decisione-azione»: se il sistema è inserito in un ambiente fisico (è il caso delle applicazioni robotiche dell'IA), la sua capacità di adempiere a un determinato compito, secondo una serie di regole, dipenderà dalla presenza di uno o più sensori (*hardware*) mediante i quali captare e introiettare informazioni sulla realtà circostante[5]. In quest'ottica,

[4] Al riguardo, non possiamo che richiamare lo scritto C. Schank, *What Is AI, Anyway?*, in «AI Magazine», 1987, 8, 4, pp. 59-65.

[5] S. J. Russell e P. Norvig, *Artificial Intelligence. A modern approach*, 4th Edition, Harlow, 2020 [ed. italiana *Intelligenza artificiale. Un approccio moderno*, vol. 1,

più sono gli ingressi sensoriali di cui il sistema è dotato (le informazioni ricavabili dai sensori possono essere di vario tipo: acustiche, visive, termiche, di pressione, ecc.[6]) e maggiore sarà la sua capacità di interpretare correttamente una data situazione di fatto.

Un discorso simile vale naturalmente per i sistemi informatici che non operano in uno spazio fisico, ovvero che lavorano in un ambiente virtuale (pensiamo a un programma deputato all'elaborazione di dati strutturati e classificati, magari ottenuti dal *web*). Sebbene in questi casi non si tratti di raccogliere e raffinare degli *input* sensoriali semplici, resta il fatto che il sistema è alimentato da un insieme più o meno ampio di informazioni ambientali che gli consentono di svolgere la sua funzione in modo efficace.

Se i dati in ingresso sono imprescindibili per far sì che il sistema informatico possa orientarsi nello spazio – qualunque esso sia – e dare il via a una qualche forma di «ragionamento» (su cui vedi *infra*), ciò che invece permette di modificare la realtà esteriore è la presenza di quelli che la scienza informatica usa chiamare «attuatori»[7]. Questi ultimi non sono altro che il canale – o i canali – attraverso il quale l'azione elaborata dal sistema si concretizza nell'ambiente operativo, sia esso fisico o virtuale (esempi di attuatori sono lo schermo di un computer, il braccio meccanico di un robot, la stampante 3D, ecc.)[8].

Ma come viene stabilita l'azione di un sistema informatico?

2.2. La capacità di agire – in modo utile, per non dire razionale – all'interno di un dato ambiente da parte di un sistema informatico richiede ovviamente l'impiego di un qualche linguaggio di rappresentazione della conoscenza. «Un linguaggio di rappresentazione delle conoscenze – si è detto – è un insieme di convenzioni sintattiche e semantiche per descrivere le conoscenze possedute dal sistema»[9]. Tale linguaggio può rappresentare sia conoscenze di tipo procedurale («sapere come»), sia conoscenze solamente dichiarative («sapere che»)[10].

Il classico linguaggio formale – largamente noto e alla base dei sistemi informatici tradizionali[11] – è quello logico e, più nello specifico, quello della logica

---

Quarta edizione, a cura di F. Amigoni, Milano-Torino, 2021, p. 46].

[6] N. J. Nilsson, *Artificial Intelligence: a New Synthesis*, Burlington, 1998 [ed. italiana *Intelligenza artificiale*, Milano, 2002, p. 103].

[7] S. J. Russell e P. Norvig, *Intelligenza artificiale. Un approccio*, vol. 1, cit., p. 46.

[8] *O.l.c.*

[9] D. Fum, *Intelligenza artificiale*, Bologna, 1994, p. 97.

[10] *O.c.*, p. 98.

[11] Il linguaggio logico costituiva il fondamento dei cosiddetti «sistemi esperti»,

proposizionale e di quella del primo ordine (quest'ultima è anche detta «calcolo dei predicati»). Al netto delle peculiarità di ciascuno di questi linguaggi (la logica proposizionale ha il vantaggio di essere semplice e pertanto non ambigua, mentre la logica del primo ordine, grazie alla sua capacità di astrarre, si contraddistingue per una maggiore potenza espressiva[12]), quel che entrambi condividono è la struttura sintattica di fondo, vale a dire la necessità di rappresentare simbolicamente la conoscenza attraverso un meccanismo inferenziale (*if-then*)[13].

La funzione *if-then* è storicamente associata alla logica deduttiva, dove consente di ampliare l'insieme di partenza delle conoscenze tramite la costruzione di un legame tra premessa (nota) e conclusione (ignota): *if* tutti gli uomini sono mortali e *if* Socrate è un uomo, *then* Socrate è mortale, è il classico esempio di scuola; ma potremmo anche dire, in termini assai meno teorici e più pratici, *if* è il tuo turno di gioco, *then* puoi collocare una pietra su un punto libero della scacchiera[14].

Un sistema informatico che opera secondo rigidi schemi di logica deduttiva, tuttavia, se non viene integrato con funzioni aggiuntive, ha ben poche possibilità di farsi strada in contesti complessi. Nemmeno la fissazione di obiettivi – cioè, di situazioni desiderabili[15] – o l'inserimento di una funzione di utilità – che indica i «criteri per decidere quale opzione, fra diverse possibili, risulta più promettente per raggiungere un determinato obiettivo»[16] – paiono essere del tutto risolutivi per la generazione di un comportamento che sia davvero originale e autonomo. Quel che serve, insomma, è un modo per orientarsi efficacemente in situazioni nuove, impreviste e magari solo in parte osservabili, se non addirittura entro ambienti caotici, che per loro stessa natura sfuggono a un unico ragionamento conseguente.

---

affermatisi nei primi anni Ottanta del secolo scorso (cfr. J. Kaplan, *Artificial Intelligence. What Everyone Needs To Know*, Oxford, 2017 [ed. italiana *Intelligenza artificiale. Guida al futuro prossimo*, Roma, 2018, pp. 51-52]).

[12] S. J. Russell e P. Norvig, *Intelligenza artificiale. Un approccio*, vol. 1, cit., pp. 260-261.

[13] *O.c.*, p. 284.

[14] L'esempio del Go, gioco da tavolo cinese, è tratto da S. Russell, *Human Compatible. Artificial Intelligence and the Problem of Control*, New York, 2019, pp. 270-271.

[15] Per capire meglio come la fissazione di un obiettivo (*goal*) possa incidere sull'attività del sistema, vd. M. Mitchell, *Artificial Intelligence. A Guide for Thinking Humans*, Londra, 2020, p. 9 e ss.

[16] D. Fum, *Intelligenza artificiale*, cit., p. 71.

2.3. Basare un sistema informatico su regole logiche di carattere deduttivo significa non solo determinare azioni che, oltre a non gestire l'incertezza, si adattano male ai cambiamenti del mondo (è questo, in pillole, ciò che intende la scienza informatica quando parla di «monotonicità» della logica deduttiva[17]), ma implica anche, nella maggior parte dei casi, la necessità di (pre)compilare manualmente questo insieme di regole.

Il passaggio da un approccio deduttivo ad altre forme di linguaggio – alcune delle quali mantengono una natura simbolica, come la logica induttiva, mentre altre adottano strutture matematiche pure[18] – apre la strada alla c.d. auto-programmazione (*machine learning*), che consiste nel dotare le macchine dell'abilità di «accrescere in modo automatico le proprie capacità senza essere obbligati a costruirle "perfette" sin dall'inizio»[19]. In altre parole, «oggi i computer non hanno più bisogno di essere programmati: lo fanno da soli»[20].

Perché l'autoapprendimento possa avere luogo, tuttavia, il sistema informatico deve avere accesso a dati e informazioni che gli permettano di «scoprire delle regolarità nel mondo che lo circonda ricavando principi di carattere generale da esperienze particolari», nonché «spiegare singoli fatti o eventi riconducendoli a cause e principi di natura più generale»[21]. Solitamente tale processo avviene in fase di programmazione del sistema informatico (nel gergo tecnico si parla di una fase di *training*, cioè di «addestramento», proprio per differenziarla dalla programmazione classica)[22]; fase durante la quale si somministra al sistema un insieme di esempi e controesempi – relativi a un determinato fatto, oggetto o fenomeno di cui «è già conosciuto il risultato di interesse» –, che possano essere direttamente osservati o comunque che siano conoscibili[23].

---

[17] *O.c.*, p. 138 e s.

[18] Per un'ampia panoramica sulle alternative alla logica classica, P. Domingos, *The Master Algorithm. How the Quest for the Ultimate Learning Machine Will Remake Our World*, Londra, 2015 [ed. italiana *L'algoritmo definitivo. La macchina che impara da sola e il futuro del nostro mondo*, Torino, 2020].

[19] D. Fum, *Intelligenza artificiale*, cit., p. 261.

[20] P. Domingos, *L'algoritmo definitivo*, cit., p. 11. Sul tema del *machine learning* si veda anche P. Domingos, *A Few Useful Things to Know About Machine Learning*, in «Communications of the ACM», 2012, 55, 10, pp. 78-87.

[21] D. Fum, *Intelligenza artificiale*, cit., p. 139.

[22] Il *training* può essere suddiviso in ulteriori sottocategorie in base al ruolo ricoperto dall'essere umano: vi è l'addestramento «supervisionato», «non supervisionato» oppure «mediante rinforzo» (cfr. M. Boari, P. Mello, M. Colajanni e D. Luciani, *Intelligenza artificiale. Introduzione, evoluzione e sviluppi, applicazioni mediche*, Bologna, 2019, p. 58).

[23] *O.c.*, p. 57.

Ciò posto in termini generali, i meccanismi grazie ai quali apprendere e riproporre successivamente la conoscenza acquisita possono essere diversi.

Un modo per lavorare sui dati e implementare il *machine learning* all'interno di un sistema informatico è quello di utilizzare algoritmi di logica induttiva che adottino un linguaggio simbolico. In questi casi, la conoscenza viene spesso rappresentata sotto forma di «albero di decisione», sebbene la si possa condensare anche nelle suddette regole *if-then* (di solito si propende per la forma ad albero in quanto il suo processo di costruzione risulta essere tendenzialmente meno complesso dell'equivalente insieme di regole[24]). Che si opti per una forma piuttosto che per l'altra, comunque, resta il fatto che «gli insiemi di regole e gli alberi di decisione sono facili da capire: ci consentono di sapere sempre che cosa sta facendo il *learner*, e soprattutto se quello che sta facendo è giusto o sbagliato, per poter apportare le correzioni opportune, se necessario, e aumentare la fiducia nei risultati»[25].

Accanto a questo tipo di *machine learning* troviamo poi tecniche di apprendimento automatico – comunemente definite «sub-simboliche» – che si basano su modelli matematici non suscettibili di interpretazione simbolica[26]. L'approccio sub-simbolico forse più noto e diffuso è quello che postula la creazione di reti neurali artificiali (*artificial neural networks*), con cui si vorrebbe «simulare direttamente su computer un modello ispirato al funzionamento del cervello umano»[27]. In sostanza, si tratta di sistemi i quali elaborano le informazioni grazie alla presenza di unità computazionali variamente interconnesse, ognuna delle quali applica ai dati di *input* dei valori numerici che vengono via via aggiustati in base agli errori commessi, fino a restituire un *output* che approssimi la soluzione attesa[28]. Per dirla in maniera più semplice e figurata, essi sono «imitatori incredibilmente talentuosi, capaci di trovare le correlazioni e rispondere ai nuovi *input* come se dicessero "questo mi ricorda di…", e, nel fare ciò, di imitare le migliori strategie "distillandole" da un gran numero di esempi»[29].

L'impiego di un linguaggio non simbolico, se da un lato facilita l'elaborazione di dati non strutturati (fenomeno comunemente indicato con l'appellativo di

---

[24] D. Fum, *Intelligenza artificiale*, cit., p. 277.

[25] P. Domingos, *L'algoritmo definitivo*, cit., p. 120.

[26] M. Boari, P. Mello, M. Colajanni e D. Luciani, *Intelligenza artificiale*, cit., p. 65.

[27] *O.l.c*. Sull'argomento delle reti neurali merita di essere consultato anche il testo D. Parisi, *Intervista sulle reti neurali. Cervello e macchine intelligenti*, Bologna, 1989.

[28] Per qualche nozione in più, D. Floreano e C. Mattiussi, *Manuale sulle reti neurali*, Bologna, 2002, pp. 16-19.

[29] J. Kaplan, *Intelligenza artificiale. Guida*, cit., p. 62.

«*big data*») e accresce pertanto l'efficienza e la versatilità del sistema, dall'altro ha un costo non trascurabile in termini di verificabilità dell'iter «logico» seguito dalla macchina (per questo motivo, in letteratura, si parla di «*black box problem*»): nonostante i tentativi di creare degli specifici algoritmi di spiegazione (*explainable AI*), l'operato di questi sistemi rimane molto difficile, se non impossibile, da comprendere per l'essere umano[30].

Riassumendo: un sistema informatico che, nell'espletare una data attività, faccia ricorso a tecniche di *machine learning* simboliche o sub-simboliche è in grado di ricavare dalla propria esperienza le informazioni necessarie al raggiungimento dell'obiettivo fissato; è in grado, inoltre, di evincere dai dati (ambientali) delle conoscenze inedite e, se del caso, di adattare di conseguenza il proprio stato interno. È in questo senso che esso può definirsi autonomo e, per certi versi, «intelligente»[31].

3. *Sulle offese alla persona o alla collettività arrecate da un sistema artificiale autonomo. Rilievi di diritto penale*

Che l'impiego di sistemi capaci di «entrare in connessione stabile con l'ambiente circostante e di interagire in modo autonomo e adattivo con esso»[32] non sia più appannaggio della fantascienza è ormai un dato alla portata di tutti. Ciò di cui ancora non disponiamo è soltanto una casistica numericamente significativa di offese riconducibili all'utilizzo di sistemi autonomi, il che è verosimilmente dovuto alla limitata diffusione di una tecnologia ancora agli albori.

Vi sono alcune notizie di cronaca, per lo più straniera, che riferiscono di incidenti in cui è stato coinvolto un sistema di IA: la maggior parte dei casi riguarda le cosiddette auto a guida autonoma (*self-driving cars*)[33], ma non mancano epi-

---

[30] S. J. Russell e P. Norvig, *Intelligenza artificiale. Un approccio*, vol. 1, cit., Cap. 27.3.4 (*online*).

[31] Sul punto è stato osservato che «l'imparare dall'esperienza, dai propri sbagli, da insegnanti, da altri esseri umani, dall'ambiente che ci circonda, è riconosciuta da tutti come una capacità peculiare e sostanziale dell'intelligenza» (M. Boari, P. Mello, M. Colajanni e D. Luciani, *Intelligenza artificiale*, cit., p. 57).

[32] S. Manzocchi e L. Romano, *Io, robot? L'intelligenza artificiale ai tempi della quarta rivoluzione industriale*, in *Intelligenza artificiale. Politica, economia, diritto, tecnologia*, a cura di P. Severino, Roma, 2022, p. 31.

[33] Ricordiamo in particolare quanto avvenuto in Florida nel 2016 (il fatto è passato alla storia come il primo incidente mortale causato da una *self-driving car*) o in Arizona due anni dopo (qui sembrerebbe che si sia persino accertata la responsabilità della macchina).

sodi in cui l'uso di questi sistemi pare abbia portato a esiti pregiudizievoli anche senza che operassero in una configurazione robotica[34].

Compresi i meccanismi di funzionamento e le potenzialità di questi sistemi, tuttavia, riteniamo che fare delle valutazioni (giuspenalistiche) su possibili offese derivanti da un loro utilizzo possa anche prescindere da un riscontro empirico puntuale.

Nulla vieta di immaginare – alla luce dell'attuale sapere tecnico-scientifico – delle inedite fonti di pericolo per i beni giuridici tutelati dall'ordinamento, e per farlo non occorre nemmeno ricorrere a scenari estremi: pensiamo, ad esempio, a cosa potrebbe accadere se una squadra di soccorso alpino facesse affidamento su una sofisticata analisi meteorologica compiuta da un sistema informatico intelligente, ovvero se le modalità e, prima ancora, la stessa fattibilità dell'intervento di salvataggio dipendessero proprio dall'esito di siffatta analisi. Oppure immaginiamoci un sistema di IA incaricato di gestire delle turbine idroelettriche unitamente alle annesse opere di presa e, quindi, di garantire la sicurezza idraulica di un corso d'acqua in una determinata zona.

Ora, è chiaro che un'eventuale morte o ferimento dei soccorritori intervenuti in condizioni avverse, piuttosto che degli alpinisti abbandonati al loro destino, non potrebbe qualificarsi come «fatto» penalmente irrilevante. Né lo sarebbe l'eventuale inondazione di un centro abitato da cui derivasse un pericolo, se non addirittura un danno, per l'incolumità pubblica[35]. E si potrebbero fare molti altri esempi, toccando i più disparati ambiti e beni giuridici.

Rivolgere l'attenzione a condotte che minacciano o aggrediscono la sfera psicofisica della persona, però, consente di mettere al riparo un'indagine sui rapporti tra IA e diritto penale da problemi legati alla territorialità e alla frammentarietà di quest'ultimo: un'apertura a fattispecie di reato più complesse – cosa che pur si è fatta in dottrina[36] – imporrebbe di sviluppare un'analisi scrupolosa intorno ai requisiti di ciascun fatto tipico. Al contrario, circoscrivere il discorso a fatti offensivi del bene vita o incolumità personale (questi diritti, come noto, godono di una tutela penale a tutto campo), ammette, da un lato, delle considerazioni di

---

[34] Di recente, alcune importanti testate giornalistiche, tra cui il New York Times e il Washington Post, hanno pubblicato la notizia di un giovane che, dopo aver instaurato una relazione affettiva con un *Chatbot*, si è tolto la vita.

[35] Nel nostro ordinamento – ma lo stesso vale tendenzialmente in ogni società moderna –, fatti come quelli che abbiamo descritto potrebbero integrare il reato di omicidio, lesioni o disastri di vario tipo.

[36] Su tutti, F. Consulich, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso di mercato*, in «Banca borsa e titoli di credito», 2018, 2, pp. 195-234.

più ampio respiro sul fenomeno visto nel suo insieme e, dall'altro, aiuta a spostare il focus sull'elemento soggettivo del reato.

Dopo avere approfondito i peculiari meccanismi di funzionamento dei sistemi informatici che agiscono in autonomia abbiamo infatti maturato la convinzione che i maggiori ostacoli alla configurazione di responsabilità penali si trovino sul terreno della colpevolezza. È possibile ricondurre l'offesa materialmente realizzata dal sistema artificiale alla psiche dell'essere umano, produttore, supervisore o utilizzatore che sia? Per dirla diversamente, possiamo costruire un valido legame «soggettivo» tra la condotta umana, che si colloca a monte, e l'evento verificatosi a valle, considerato che vi è stata una mediazione decisiva e, appunto, indipendente da parte del sistema?

Nel tentativo di fare chiarezza sul punto, ovvero per scongiurare quel *responsibility gap* paventato da autorevole dottrina[37], diversi legislatori – tra cui quello europeo – stanno via via dettando delle regole di condotta all'essere umano, segnatamente al produttore dei sistemi di IA; regole che contribuiscono a delineare un comportamento doveroso, ma la cui risolutività sul fronte del penale resta ancora tutta da indagare.

4. *La responsabilità penale dell'uomo per il fatto dell'IA: criticità in materia di colpa*

A seguito di un dibattito pubblico protrattosi per quasi un decennio e di un procedimento legislativo durato più di tre anni, nel giugno 2024 l'Unione europea ha definitivamente varato un regolamento «che stabilisce regole armonizzate sull'intelligenza artificiale» (d'ora in avanti, per brevità, «legge sull'IA»)[38].

Lo scopo dell'intervento legislativo eurounitario è chiaramente quello di accrescere la fiducia dei cittadini nella tecnologia in esame attraverso una classificazione e limitazione dei rischi che ad essa inevitabilmente si accompagnano.

---

[37] In Italia, per la materia penale, il problema del vuoto di tutela viene denunciato, tra i tanti, in G. P. Demuro, *Ripartire da principi: sul rapporto del diritto penale con* big data *e intelligenza artificiale*, in *Studi in onore di Carlo Enrico Paliero*, vol. I, Milano, 2022, p. 73; F. Consulich, *Flash offenders. Le prospettive di accountability penale nel contrasto alle intelligenze artificiali*, in «Rivista italiana di diritto e procedura penale», 2022, 3, p. 1036; P. Severino, *Intelligenza artificiale e diritto penale*, in *Intelligenza artificiale: il diritto, i diritti, l'etica*, a cura di U. Ruffolo, Milano, 2020, p. 535; C. Piergallini, *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?*, in «Rivista italiana di diritto e procedura penale», 2020, 4, p. 1762; R. Borsari, *Intelligenza Artificiale e responsabilità penale: prime considerazioni*, in «MediaLaws», 2019, 3, p. 268.

[38] Regolamento (UE) 2024/1689 del 13 giugno 2024 (pubblicato sulla Gazzetta Ufficiale dell'Unione europea del 12 luglio 2024).

Seguendo questo approccio *risk-based*, il testo regolamentare ha dunque tipizzato, oltre a specifici divieti di impiego, un insieme di requisiti tecnici per ciascun sistema di IA; ha altresì fissato una serie di obblighi per gli operatori del settore, a partire da chi fa parte della catena di approvvigionamento.

Per quanto si possa apprezzare l'impianto normativo dell'UE sul piano politico, ovvero su quello del bilanciamento tra diritti fondamentali e libertà di iniziativa economica, una sua valorizzazione rispetto alla configurazione di responsabilità penali non può certo prescindere da un confronto coi principi regolatori della materia (primo fra tutti, il principio di colpevolezza), nonché con gli insegnamenti dottrinali in tema di colpa[39].

4.1. Se da un lato è vero che la colpa penale – che trova il suo referente costituzionale nell'art. 27 cost. – consiste, in prima battuta, nell'inosservanza di «regole "cautelari", o "di diligenza", finalizzate alla prevenzione del fatto che è stato realizzato»[40] (misura oggettiva della colpa), dall'altro, non va dimenticato che «il rimprovero di colpevolezza [andrebbe] fatto dipendere dall'accertamento dell'attitudine del soggetto che ha in concreto agito ad uniformare il proprio comportamento alla regola di condotta violata»[41] (misura soggettiva della colpa). Ma non solo: nei reati di evento, l'interprete deve anche accertare che sussista un nesso «causale» tra la cautela violata e l'offesa verificatasi, come pure una connessione psicologica tra quest'ultima e l'agente, e questo affinché non si ricada in forme di responsabilità da mero *versari in re illicita*[42].

---

[39] Sembrano voler esaltare le regole europee nella costruzione di responsabilità penali, A. Fiorella, *Responsabilità penale del* Tutor *e dominabilità dell'Intelligenza Artificiale. Rischio permesso e limiti di autonomia dell'Intelligenza Artificiale*, in *Il diritto nell'era digitale*, cit., p. 657; M. Lanzi, *La responsabilità penale per le auto a guida autonoma*, in *Cybercrime*, 2023, cit., p. 1387.

[40] *Ex multis*, D. Pulitanò, *Diritto penale*, Torino, 2009, p. 351. In generale, sulla connessione tra colpa e inosservanza di regole con finalità cautelari, cfr. M. Gallo, voce *Colpa penale (dir. vig.)*, in *Enciclopedia del diritto*, VII, Milano, 1960, p. 636 e ss.

[41] G. Fiandaca ed E. Musco, *Diritto penale. Parte generale*, Bologna, 2010, p. 569. Sul grado di 'soggettivizzazione' (o 'individualizzazione') del giudizio di colpa, invece, è bene consultare D. Castronuovo, *La colpa penale*, Milano, 2009, p. 560 e ss., nonché G. Forti, *Colpa ed evento nel diritto penale*, Milano, 1990, p. 267 e ss. Più in generale, su questo profilo della colpa, V. De Francesco, *Sulla misura soggettiva della colpa*, in *Studi Urbinati di scienze giuridiche, politiche ed economiche*, 1977-1978, 30, pp. 273-343.

[42] In G. Marinucci, *La colpa per inosservanza di leggi*, Milano, 1965, p. 5, viene segnalato molto chiaramente il pericolo a cui si va incontro se si accetta che «la semplice [difformità] della condotta concreta dalle norme scritte [basti] a far presumere, *iuris et de iure*, l'esistenza della colpa».

È con questa struttura dogmatica – la quale circoscrive un'eventuale punizione entro limiti di ragionevolezza e legittimità costituzionale – che deve necessariamente fare i conti qualsivoglia incolpazione dell'uomo per il fatto dell'IA.

5. (Segue) *In tema di misura oggettiva della colpa*

La possibilità di attribuire all'essere umano una responsabilità penale colposa a fronte di un evento dannoso o pericoloso realizzato direttamente da un sistema informatico passa innanzitutto dalla individuazione di una regola cautelare.

A tal riguardo giova svolgere una breve premessa.

In assenza di cautele scritte (c.d. «colpa generica»), il confine tra i profili oggettivi e soggettivi della colpa tende a sfumare o addirittura svanire, dato che la valutazione di prevedibilità e prevenibilità dell'evento, con cui si usa ricercare la regola cautelare, non può che essere unitaria: «condotta "diligente" (in senso lato) è quella conforme a cautele atte a prevenire il realizzarsi di un evento la cui realizzazione, in assenza di quelle cautele, sarebbe prevedibile»[43]. In pratica, quando è l'interprete a dover stabilire la condotta cauta, l'indagine sulla causalità della colpa e quella sulle (reali) possibilità dell'agente finiscono di fatto per coincidere.

Diversa invece è la situazione in cui il comportamento diligente è tipizzato, cioè positivamente indicato dal legislatore. Nelle ipotesi di «colpa specifica», infatti, una valutazione di rischio (astratta) è già stata compiuta «dall'autorità che pone la norma scritta»[44], sicché l'esame di chi ha un compito interpretativo e applicativo nel caso concreto dev'essere sdoppiato: da un lato, permane la necessità di misurarsi con le possibilità dell'agente «in carne e ossa»; dall'altro, diviene fondamentale soffermarsi sulla regola cautelare (pre)scritta, al fine di verificarne l'effettiva pertinenza ed efficacia.

Sarà pur vero, quindi, che un intervento normativo avente ad oggetto l'intelligenza artificiale contribuisce a chiarire i ruoli e le mansioni di tutti coloro i quali vi entrano in contatto (fornitore, supervisore, utilizzatore), ma è parimenti vero che l'indicazione puntuale e precisa della condotta doverosa non alleggerisce – ma anzi complica, sotto certi aspetti – il compito del penalista.

Ciò posto, la legge sull'IA classifica i diversi sistemi in base al rischio che essi comportano per il singolo e/o per la collettività: nel testo europeo ci si concentra principalmente sulle «pratiche di IA vietate» (capo II) e sui «sistemi di IA ad

---

[43] D. Pulitanò, *Diritto penale*, cit., p. 354.

[44] G. Fiandaca ed E. Musco, *Diritto penale*, cit., p. 548.

alto rischio» (capo III), mentre vengono sottoposti a una disciplina speciale – se vogliamo, meno onerosa – i c.d. «modelli di IA per finalità generali» (capo V)[45].

Lasciando per il momento da parte i divieti d'impiego, due sono le direttrici lungo le quali si sviluppa l'azione normativa eurounitaria. Preliminarmente, viene stabilito che i sistemi di IA ad alto rischio devono soddisfare determinati requisiti tecnici, ossia devono possedere *data sets* di qualità e una documentazione tecnica esaustiva, essere in grado di registrare gli eventi (*logs*), funzionare in maniera trasparente ed essere sorvegliati da un umano; ma devono anche garantire accuratezza, robustezza e una protezione adeguata contro gli attacchi informatici. Subito dopo, poi, la legge sull'IA fissa una serie di obblighi in capo agli operatori del settore, tra cui quello di implementare i predetti requisiti, di conservare la documentazione tecnica e i *logs*, di informare le autorità in caso di incidente, e così via.

Ebbene, se il nostro scopo è quello di individuare e isolare norme precauzionali, non possiamo fare a meno di notare che non tutte le regole contenute nella legge sull'IA hanno tale natura. Le disposizioni, per esempio, che impongono al fornitore del sistema di redigere la documentazione tecnica, oppure quelle che lo obbligano a costruire il sistema in maniera tale che sia in grado di registrare i *logs*, nulla aggiungono in termini di prevenzione, mirando evidentemente a soddisfare esigenze di accertamento[46]. Viceversa, sembrerebbero perseguire obiettivi di questo genere le norme che prescrivono la cura dei dati e la supervisione umana, oppure le varie statuizioni relative all'accuratezza e alla robustezza del sistema, o quelle volte a garantirne la c.d. cybersicurezza. Ed è a queste norme che lo studioso di diritto penale può – o anzi deve – rivolgere la propria attenzione.

5.1. La scienza penalistica, come noto, è concorde nel ritenere che, per poter muovere un rimprovero nei reati colposi a evento naturalistico, non è sufficiente la violazione di una qualsiasi regola cautelare, bensì di una regola che tende a prevenire proprio un'offesa del tipo di quella verificatasi *hic et nunc*[47]. Mentre si

[45] Nella precedente versione del regolamento UE, i sistemi di intelligenza artificiale «per finalità generali» (tali sono, secondo la definizione europea, quei sistemi che sono «in grado di svolgere con competenza un'ampia gamma di compiti distinti») dovevano sostanzialmente soddisfare i requisiti tecnici dei sistemi «ad alto rischio».

[46] Crediamo si possa concordare sul fatto che gli obblighi menzionati – e altri dello stesso tipo – servano per lo più a dimostrare alle autorità di controllo che il sistema è conforme ai requisiti di legge, così come a garantire la tracciabilità delle azioni compiute dalla macchina, a beneficio di eventuali valutazioni *ex post facto*.

[47] D. Pulitanò, *Diritto penale*, cit., p. 367; F. Antolisei, *Manuale di diritto penale. Parte generale*, a cura di L. Conti, Milano, 2003, p. 375; G. Fiandaca ed E. Musco, *Diritto penale*, cit., p. 561 e s.; G. Marinucci, E. Dolcini e G. L. Gatta,

può discutere sul «grado» di corrispondenza tra evento astratto ed evento concreto[48], è indubbio che questi debbano avere dei tratti in comune, atteso che in caso contrario l'agente «risponde[rebbe] dell'evento non voluto […] sulla base del solo rapporto materiale di causalità»[49].

Stando così le cose, occorre chiedersi, allora, quale sia il fine perseguito dal legislatore europeo nel momento in cui pone le cautele di cui abbiamo detto poc'anzi (cura dei *data sets*, sorveglianza umana, ecc., ma anche divieti assoluti di impiego di talune forme di IA), ovvero ricostruire per via interpretativa – lasciandosi guidare da logica e comune buon senso – l'area di rischio presa ad oggetto da ciascuna previsione regolamentare.

Una prima indicazioni circa gli scenari d'offesa che si vorrebbero evitare la troviamo, oltre che nei considerando, all'articolo 1 della legge europea: fin dalle battute iniziali, il legislatore ci ricorda che obiettivo del suo intervento è scongiurare tutte quelle situazioni in cui si finisce per sacrificare un «livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali». Ma una siffatta indicazione – invero assai generica – non basta per ciò che qui interessa.

La (vera) *ratio* delle diverse prescrizioni, più che essere segnalata in maniera esplicita dal legislatore, emerge dal tenore letterale e dalla portata della stessa regola di comportamento. Per quel che riguarda i divieti assoluti di impiego, ad esempio, se si analizzano con attenzione le diverse fattispecie prese a riferimento, si vedrà che le conclusioni a cui si giunge in punto di diritto non sono per nulla uniformi. Infatti, mentre una violazione del divieto di utilizzo dei sistemi che manipolano il comportamento delle persone (art. 5, c. 1, lett. a, legge sull'IA) può venire in rilievo dinanzi a eventi che ledono, per effetto di queste tecniche, l'integrità fisica o mentale e financo il bene vita, altrettanto è difficilmente sostenibile se a essere violato è il divieto di usare sistemi di classificazione e identificazione delle persone (art. 1, c. 1, lett. c), dal momento che tale previsione normativa sembra richiamare situazioni del tutto differenti (tra l'altro, fatti di questo tipo raramente integrano illeciti penali colposi)[50].

Manuale di diritto penale. Parte generale, Milano, 2019, p. 401 e ss. Il punto è oggi pacifico anche per la giurisprudenza di legittimità: rinviamo, *ex multis*, a Cass. pen., sez. 4, sentenza n. 40050 del 29 marzo 2018.

[48] In merito a tale problematica, con un occhio anche all'esperienza giudiziaria, G. Civello, *La «colpa eventuale» nella società del rischio. Epistemologia dell'incertezza e «verità soggettiva» della colpa*, Torino, 2013, p. 71 e ss., oltre a G. Forti, *Colpa ed evento*, cit., p. 522 e ss.

[49] F. Antolisei, *Manuale di diritto penale*, cit., p. 375.

[50] Cionondimeno, le disposizioni europee che vietano l'uso di sistemi di IA capaci di discriminare persone o gruppi sociali si potrebbero valorizzare rispetto a ipotesi criminose diverse (magari di mera condotta), pure dolose, come la diffamazione: una

Il discorso risulta invece un po' più lineare relativamente alle regole che disciplinano le modalità di sviluppo e impiego delle pratiche di IA ammesse (si badi che abbiamo già espunto dalla nostra analisi le prescrizioni che non hanno un contenuto cautelare in senso stretto).

Non facciamo particolare fatica a riconoscere come la cura degli insiemi di dati, la progettazione di sistemi accurati e resilienti, la sorveglianza umana, l'adozione di misure correttive nei casi di difformità accertate o a seguito di incidenti, ecc., siano volte a evitare la produzione di *outputs* indesiderati e, perciò, di eventi «anche» lesivi della sfera psicofisica delle persone; di eventi, insomma, che rappresentano proprio la «concretizzazione» del rischio – *rectius* di uno dei rischi – che la norma mirava a contenere.

5.2. Una verifica diversa e forse più insidiosa, ma comunque necessaria, è quella che riguarda l'efficacia preventiva della condotta imposta dall'ordinamento per il tramite di una data regola (cautelare). In buona sostanza, una volta individuata la cautela confacente al caso concreto, bisogna capire «se la condotta rispettosa della regola di diligenza […] avrebbe evitato […] il verificarsi dell'evento»[51]; passaggio cruciale, questo, «giacché il risultato che il soggetto non è in grado di impedire non gli può essere posto a carico, rappresentando nei suoi confronti una mera fatalità»[52].

In questo senso, è appena il caso di ricordare che, un po' come avviene nell'accertamento della causalità materiale, il giudizio di prevenibilità si effettua assumendo l'osservanza di una condotta conforme a dovere da parte dell'agente e confrontandone l'ipotetico risultato con quello realmente verificatosi.

Rispetto al tema che stiamo trattando, quanto appena detto richiede dunque di sottoporre le disposizioni regolamentari, che stabiliscono comportamenti asseritamente cauti, a un puntuale controllo di efficacia, tenendo naturalmente conto del dato tecnico. E non parliamo di un'efficacia apprezzabile in termini meramente statistici, ma di un'efficacia che sussista (pure) nel caso singolo[53]. Ciò

---

volta stabilita l'illiceità del fatto, si tratterebbe di individuare, in aggiunta, un seppur marginale profilo di volontà – anche soltanto in termini di accettazione del rischio (*rectius* evento) – in capo al soggetto umano che tale sistema ha prodotto o impiegato. Rimane naturalmente ferma la necessità di accertare (non solo la «prevedibilità», come nelle ipotesi colpose, ma perfino) la «previsione» dell'evento offensivo realizzatosi *hic et nunc*, con tutte le difficoltà del caso.

[51] G. Marinucci, E. Dolcini e G. L. Gatta, *Manuale di diritto penale*, cit., p. 403.

[52] F. Antolisei, *Manuale di diritto penale*, cit., p. 376.

[53] Avverte l'esigenza di valutazioni di prevenibilità valide in concreto, G. Fiandaca ed E. Musco, *Diritto penale*, cit., p. 562.

significa che, per poter configurare una colpa penale in capo all'operatore che abbia disatteso le prescrizioni normative in materia di IA, dobbiamo poter dire che l'evento offensivo conseguente all'azione artificiale non si sarebbe verificato se questi avesse tenuto il comportamento raccomandatogli dal legislatore.

Ora, pur riconoscendo l'importanza e l'irrinunciabilità di un esame caso per caso, i peculiari meccanismi di funzionamento dei sistemi di intelligenza artificiale ci permettono di fare alcune considerazioni generali di carattere teorico.

Se è vero che un giudizio sull'efficacia preventiva di una determinata regola di condotta presuppone la possibilità di conoscere in pieno le dinamiche del caso concreto e, più in generale, l'esatto svolgersi degli eventi (va da sé che un ragionamento «contro-fattuale» può essere condotto a patto che si sappia come sono andati i fatti), i sistemi che adoperano tecniche di *machine learning* di tipo «simbolico» non sembrano porre nessun problema: come anticipato sopra, questi sistemi sono intelligibili all'essere umano, in quanto utilizzano simboli e inferenze logiche per gestire la conoscenza e portare a termine il loro lavoro. Al contrario, i sistemi autonomi che fanno uso di tecniche sub-simboliche, ossia di modelli matematici, per leggere la realtà e raggiungere l'obiettivo prefissato, sono caratterizzati da uno stato interno assolutamente oscuro, il quale osta allo svolgimento di un'indagine volta a comprendere i motivi delle loro azioni.

L'impossibilità teorica di ricostruire – ancorché in termini approssimativi o di verosimiglianza – la situazione in cui è venuta a realizzarsi l'offesa, i fattori che potrebbero aver inciso sulla catena causale e l'impatto che su di essa potrebbe aver avuto la condotta umana ci impedisce di apprezzare l'idoneità impeditiva della regola cautelare (*id est* del comportamento alternativo lecito). Per esempio, come facciamo a dire che la mancata cura dei *data sets* da parte del fornitore di un sistema autonomo ha causato l'evento X se non sappiamo in base a quali elementi la macchina abbia preso la sua decisione? E ancora, come possiamo escludere, sempre negli scenari con *output* prodotto da un sistema sub-simbolico, la presenza di altri fattori causali (tali potrebbero essere le varie circostanze ambientali o l'intromissione di soggetti terzi), e ciò non solo rispetto alla fase di *training*, ma anche in ordine alla successiva porzione spazio-temporale in cui è avvenuto il fatto «incriminato»?

Sul punto, vale altresì la pena di sottolineare che le suddette difficoltà – le quali accomunano, inevitabilmente, la quasi totalità delle disposizioni che tentano di prevenire eventi offensivi cagionati da un sistema di IA sub-simbolica (fa eccezione solamente l'obbligo di sorveglianza umana[54]) – non verrebbero meno neppure

[54] Riteniamo che la sorveglianza umana – la quale, per ovvie ragioni, cessa di essere passiva soltanto a valle dell'azione del sistema – sia potenzialmente in grado di impedire un evento offensivo *in nuce*, in quanto si concretizzerebbe in un vaglio finale dell'azione artificiale, prima che questa possa produrre i suoi effetti.

se si optasse per l'imputazione dell'evento in base al criterio del c.d. «aumento del rischio» (*Risikoerhöhungslehre*)[55]. Anche in tal caso, si porrebbe il medesimo problema: come rimproverare a un soggetto di aver «aumentato le probabilità» che un certo evento si verificasse «nel caso concreto» se non conosciamo il rischio iniziale, cioè se non possiamo misurare le probabilità di verificazione di quello stesso evento al di là del contributo umano?

In conclusione, poiché il *machine learning* di tipo sub-simbolico non permette, almeno ad oggi, di dissipare i dubbi sulla ricostruzione del fatto storico – che è cosa ben diversa dal dubbio sulla spiegazione causale –, un esame dell'efficacia preventiva della condotta doverosa, rapportato a questa tipologia di sistemi, pare sia destinato ad avere esito negativo.

6. (Segue) *In tema di misura soggettiva della colpa*

Esaurita l'analisi sul piano oggettivo, non ci si può esimere dallo spendere qualche parola sulla posizione soggettiva di chi è chiamato ad attivarsi affinché l'evento dannoso o pericoloso non si realizzi.

A meno di non voler accettare una colpa penale fondata sulla mera disobbedienza (questa sposterebbe però l'intero disvalore del fatto sulla condotta, con tutto ciò che ne consegue), per poter addebitare al soggetto agente un determinato evento offensivo occorre anzitutto rinvenire, in capo a costui, la possibilità di prevederlo[56]. In altre parole, egli deve aver avuto «la possibilità di riconoscere un fatto non ancora verificatosi», vale a dire «la possibilità […] di rendersi conto

---

[55] Secondo la teoria dell'aumento del rischio, di matrice tedesca, «per l'imputazione dell'evento a titolo di colpa è sufficiente […] che la condotta inosservante abbia "aumentato" le probabilità della lesione», cosicché, all'atto pratico, l'attribuzione di responsabilità è giustificata «dal mero dato dell'esistenza di qualche maggiore possibilità di salvare il bene in caso di condotta osservante/dovuta» (M. Donini, *La concausa omissiva e l'imputazione «per l'aumento del rischio». Significato teorico e pratico delle tendenze attuali in tema di accertamenti eziologici probabilistici e decorsi causali ipotetici*, in «Rivista italiana di diritto e procedura penale», 1999, 1, pp. 41-42). Per maggiori approfondimenti sulla *Risikoerhöhungslehre*, rimandiamo a C. Roxin, *Pflichtwidrigkeit und Erfolg bei fahrlässigen Delikten*, in «Zeitschrift für die gesamte Strafrechtswissenschaft», 1962, 74, 3, p. 411 e ss.; G. Stratenwerth, *Bemerkungen zum Prinzip der Risikoerhöhung*, in *Festschrift für Wilhelm Gallas zum 70. Geburtstag am 22. Juli 1973*, edito da K. Lackner, H. Leferenz, E. Schmidt, J. Welp e E. A. Wolff, Berlino-New York, 1973, p. 227 e ss.; I. Puppe, *Zurechnung und Wahrscheinlichkeit. Zur Analyse des Risikoerhöhungsprinzips*, in «Zeitschrift für die gesamte Strafrechtswissenschaft», 1983, 2, p. 287 e ss.

[56] Al riguardo, in dottrina, F. Mantovani e G. Flora, *Diritto penale. Parte generale*, Milano, 2023, p. 351.

delle probabilità di verificazione di tale fatto»[57]. E non basta certo una prevedibilità generica, del tipo di quella richiesta in fase di individuazione della regola cautelare, ma prevedibile dovrà essere un evento parte di una categoria di eventi altamente caratterizzata, cioè di una categoria che replichi in astratto le peculiarità del caso concreto, con la sola esclusione degli elementi irripetibili di unicità. Solo così ragionando si potrà ritenere l'agente realmente emancipato dalla previsione scritta – la quale conserverà una funzione di indirizzo – e gli si potrà infine attribuire l'evento (non voluto ma) cagionato tramite la sua azione od omissione «cosciente» e «volontaria» (del resto, se così non fosse, i profili di colpa venutisi a formare sul piano oggettivo sarebbero del tutto virtuali e si rischierebbe ancora una volta un ritorno al mero *versari*).

Applicando tali coordinate ermeneutiche al caso dell'IA, il discorso sulla possibile responsabilità penale colposa dell'operatore si fa ancor più complesso.

Proviamo a ripensare per un attimo al fornitore del sistema e al suo obbligo di curare adeguatamente i dati da utilizzare in fase di addestramento (il ragionamento non cambierebbe se si prendesse come esempio un altro dei compiti da espletare prima dell'elaborazione dell'*output*). Perché il fornitore possa rispondere di un evento lesivo connesso a un *output* indesiderato del sistema (sia chiaro, ci stiamo riferendo ai sistemi che impiegano un linguaggio simbolico – il cui *iter* logico è quindi ricostruibile *ex post* in termini di certezza –, dato che, per gli altri, l'analisi si è arenata già sul terreno obiettivo della colpa) dobbiamo potergli rimproverare non solo di non aver garantito la qualità dei *data sets* (violazione della regola cautelare), ma di non averlo fatto nonostante fosse «prevedibile» che, attraverso tale condotta, potesse verificarsi esattamente *quell'* offesa che poi si è di fatto verificata (per rimanere sull'esempio fatto sopra, l'evento offensivo potrebbe essere «inondazione di un centro abitato dovuta alla mancata apertura delle paratoie di alleggerimento a fronte di una situazione idraulica che imponeva un abbassamento immediato del livello idrometrico»). Considerando che i sistemi autonomi basano le loro scelte d'azione, oltre che sull'addestramento ricevuto, sulla loro particolare «esperienza di vita», possiamo ragionevolmente contestare al fornitore, che non abbia adempiuto ai suoi obblighi, di non avere previsto proprio lo scenario verificatosi in fase operativa?

Mentre la distanza spazio-temporale che vi è tra addestramento e offesa suggerisce di escludere che il fornitore potesse prevedere l'evento per come verificatosi *hic et nunc*, assai diversa sembra essere la posizione del soggetto «supervisore» (rileva a poco o nulla, in questo caso, il fatto che si tratti di un'IA simbolica piuttosto che sub-simbolica). Contrariamente all'operatore che dovrebbe orientare le decisioni del sistema intervenendo in uno stadio preliminare, chi è gravato di un

[57] G. Forti, *Colpa ed evento*, cit., p. 207.

compito di sorveglianza gode di un innegabile vantaggio: egli si trova a ridosso dell'azione e, pertanto, ha accesso al medesimo patrimonio informativo del sistema, per cui dovrebbe essere assicurata – almeno teoricamente – una maggiore capacità di previsione. Ma questo non significa che il supervisore di un'IA debba automaticamente rispondere ogniqualvolta vi sia un evento avverso; significa, piuttosto, che la sua eventuale colpa penale dipenderà dalla concreta possibilità di tenere la condotta prestabilita.

6.1. Un rimprovero per colpa che non volesse cedere a eventuali difficoltà probatorie o assecondare impulsi repressivi di vario genere dovrebbe tenere in debita considerazione (finanche) le «possibilità» dell'agente del caso singolo, più o meno idealizzato. Questo vorrebbe dire, da un lato, vagliare l'opportunità di esigere il comportamento doveroso e, dall'altro, sincerarsi che il soggetto fosse comunque nelle condizioni materiali di poter soddisfare le aspettative dell'ordinamento.

Sappiamo che nella dottrina penalistica, specialmente in quella italiana, si parla della «inesigibilità» di un comportamento in presenza di «circostanze concomitanti anormali» (caso fortuito, forza maggiore, ecc.), cioè di situazioni che influiscono «in modo irresistibile sulla […] volontà o sulle […] capacità psicofisiche», al punto da invalidare politicamente la pretesa punitiva dello Stato[58]. E sappiamo altresì che, pur essendoci stati diversi studi al riguardo[59], quello dell'inesigibilità della condotta fatica ancora a diventare un criterio di portata generale. Ciononostante, siamo fermamente convinti che, nell'affrontare il tema della responsabilità (penale) connessa all'impiego di sistemi intelligenti, interrogarsi apertamente sull'esigibilità della condotta da parte dell'uomo (in particolare, di chi sorveglia l'operato di un sistema autonomo) possa aiutare l'interprete a non cadere in tranelli ermeneutici e a rifuggire da meccanismi presuntivi.

Guardando alla posizione di chi è incaricato di vigilare sul funzionamento del sistema, è possibile scorgere due potenziali profili di criticità legati al *modus operandi* di questa tecnologia.

Un primo aspetto che, a parer nostro, potrebbe mettere in discussione la stabilità di un addebito colposo dell'evento riguarda l'opportunità di esigere una verifica puntuale dell'*output*. Chiedere al supervisore di controllare ed eventualmente approvare il risultato dell'elaborazione compiuta dal sistema significa, di

---

[58] G. Marinucci, E. Dolcini e G. L. Gatta, *Manuale di diritto penale*, cit., p. 423.

[59] Rinviamo il lettore al noto saggio H. Henkel, *Zumutbarkeit und Unzumutbarkeit als regulatives Rechtsprinzip*, in *Festschrift für Edmund Mezger zum 70. Geburtstag*, edito da K. Engisch e R. Maurach, Monaco-Berlino, 1954, p. 249 e ss.; tra gli italiani, invece, segnaliamo L. Scarano, *La non esigibilità nel diritto penale*, Napoli, 1948 e, più di recente, G. Fornasari, *Il principio di inesigibilità nel diritto penale*, Padova, 1990.

fatto, costringerlo a rivedere e rivalutare tutte le informazioni raccolte nel corso del tempo, salvo che non ci si voglia accontentare di un intervento limitato e superficiale (né può dirsi sufficiente un semplice vaglio di «non lesività» del risultato proposto, atteso che talvolta l'offesa consiste nel non averne elaborato uno diverso, magari meno lesivo). Ora, se è vero che i sistemi di intelligenza artificiale «*are in fact based on decision-making and operational capabilities that replace human activities with far greater speed, precision and security*»[60] – come dimostra il crescente interesse nei loro confronti –, quale sarebbe il senso di rifarsi sulla persona fisica che non sia stata in grado di replicare «a mano» il lavoro svolto in modo automatizzato (ammesso e non concesso che siffatta attività sia umanamente praticabile)[61]?

Ma ancor più ingiusta rischierebbe di apparire un'incolpazione del supervisore per non essere riuscito a muoversi in anticipo sul sistema (emblematico è il ruolo del «conducente potenziale» nelle *self-driving cars*). Proprio perché alcune applicazioni dell'IA si connotano per interazioni costanti ed estremamente repentine (tanto con l'ambiente, quanto con gli utenti), una colpa penale conforme a costituzione non potrebbe certo ignorare la (im)possibilità materiale o «fisica» di tenere il comportamento prescritto e, in ultima battuta, di assicurare la liceità dell'opera artificiale (*ad impossibilia nemo tenetur*). Non resta che chiedersi, allora, se si possa davvero esigere dal soggetto un contegno che gli permetta di anticipare l'*output* della macchina e, idealmente, impedire il realizzarsi dell'evento offensivo.

Le questioni appena viste concorrono a formare, al pari di quelle sulla dimensione «impersonale» della colpa, un legame lineare tra l'atteggiamento umano e l'offesa. Un legame senza il quale non è possibile, secondo noi, aprire a responsabilità penali giuridicamente sostenibili e politicamente accettabili.

7. *Un bilancio provvisorio*

Sempre più raramente ormai un discorso sul diritto può rimanere svincolato dal sapere tecnico-scientifico. Come abbiamo visto, occuparsi del problema

---

[60] L. Picotti, *The challenges of new technologies for European criminal law*, in *Of swords and shields: due process and crime control in times of globalization. Liber amicorum prof. dr. J.A.E. Varvaele*, edito da M. Luchtman, The Hague, 2023, p. 806.

[61] Meriterebbe di essere presa in esame pure la naturale propensione dell'essere umano ad adeguarsi – il più delle volte, inconsciamente – al calcolo svolto dalla macchina: in fin dei conti, «quale umano […] avrà mai il coraggio […] per "ribaltare" l'*output* proveniente da un complesso sistema automatizzato?» (E. Daly, AlphaZero *batte* Stockfish *28 a 0. Intelligenza Artificiale, gioco degli scacchi e scelte strategiche*, in «Rivista di Filosofia del Diritto», 2023, 1, p. 208).

dell'aggressione ai beni giuridici fondamentali in un'ottica penale implica, in questo come in molti altri campi, doversi confrontare col dato specialistico. Neppure la presenza di un *corpus* di norme scritte autorizza l'interprete a rinunciare a un approccio critico al fenomeno in parola.

Pur comprendendo il bisogno – forse più diffuso tra gli addetti ai lavori che non all'interno del pubblico generico – di una reazione punitiva a fronte di offese cagionate (*rectius* cagionabili) da sistemi artificiali autonomi, ci preme evidenziare come vi siano diversi ostacoli alla configurazione di una colpa penale in capo all'uomo: ostacoli teorici, ma anche ostacoli pratici.

Superato il vaglio di pertinenza di una data regola cautelare rispetto a un determinato tipo di evento, le prime difficoltà si registrano in punto di verifica dell'efficacia impeditiva della condotta prescritta dall'ordinamento. Quest'ultima, se rapportata alla produzione dei sistemi di IA c.d. «sub-simbolica», non può che manifestarsi in tutta la sua inadeguatezza, specie dinanzi alle esigenze di prevenzione proprie del caso singolo (non abbiamo invece motivo di escludere che alcune cautele abbiano una loro validità apprezzabile in termini statistici). Si badi, però, che la questione giuridica non è affatto meno complicata nelle ipotesi di progettazione maldestra di sistemi «simbolici», se si considerano le implicazioni in tema di prevedibilità legate al tempo che fisiologicamente intercorre tra la condotta umana e l'*output* della macchina. Infine, come se non bastasse, con specifico riguardo alla posizione del supervisore, occorre persino fare i conti con i limiti intellettuali e fisici dell'essere umano, valutando se si possa considerare pienamente colposo il contegno di chi non abbia prontamente corretto un sistema che ha sbagliato o, peggio, che sta per sbagliare (naturalmente *nulla quaestio* per quanto concerne la colpa nei casi più gravi, contrassegnati da errori macroscopici).

Non potendo fare a meno di delineare quello che appare, *de iure condito*, come un quadro alquanto desolante, ci sia concesso di mettere brevemente in luce alcune possibili risposte a legittime istanze di tutela, ma senza per questo dismettere i panni del penalista.

Se si vuole rimanere sul terreno del penale, una strada senz'altro praticabile – e già indicata dalla dottrina – è quella dell'abbandono del «diritto penale d'evento» a favore di un «diritto penale del comportamento»[62]: in questa prospettiva, la gestione del rischio d'offesa, ovvero gli effetti di prevenzione speciale e generale

[62] Su questa linea F. Consulich, *Flash offenders. Le prospettive di accountability penale*, cit., p. 1051 e ss. Più in generale, sul tema del disvalore d'azione, vd. M. Mantovani, *Contributo ad uno studio sul disvalore di azione nel sistema penale vigente*, Bologna, 2014, e, per un superamento di una colpa penale condizionata alla verificazione di un evento offensivo, da ultimo, L. Cornacchia, *Responsabilità colposa: irrazionalità e prospettive di riforma*, in «Archivio penale», 2022, 2, pp. 1-18.

della pena, verrebbero promossi sanzionando qualsiasi mancata (corretta) osservanza degli obblighi imposti dalla normativa di settore, indipendentemente dalle conseguenze derivanti di volta in volta dalla condotta difforme (questo è il paradigma «punitivo» sostanzialmente adottato dall'UE laddove commina sanzioni amministrative per decine di milioni di euro agli operatori inadempienti). Ma vi è di più: davanti a un soggetto, *id est* l'uomo, «ormai privo di un reale ed effettivo potere di governo ed intervento sull'attività algoritmica»[63], non sembra nemmeno così peregrina l'idea di chi propone di rivolgere l'attenzione alla pericolosità sociale della macchina, magari ammettendo che lo Stato – per il tramite di suoi organi tecnicamente competenti – si intrometta direttamente nella produzione/gestione di questi sistemi (l'azione pubblica ben potrebbe concretizzarsi in un nuovo *training* o, qualora la situazione dovesse richiederlo, nella messa fuori servizio del sistema)[64].

In ogni modo, al netto di qualche considerazione su come il diritto «dovrebbe» o «potrebbe» essere, lo scopo principale di questa trattazione era chiaramente quello di problematizzare attorno allo stato dell'arte, ovvero di far emergere i nodi più complessi della configurazione di una responsabilità dell'uomo per il fatto della macchina; quei nodi che, a ben vedere, esprimono appieno il senso della sfida lanciata dall'intelligenza artificiale al mondo del diritto.

---

[63] L. Romanò, *La responsabilità penale al tempo di ChatGPT: prospettive de iure condendo in tema di gestione del rischio da intelligenza artificiale generativa*, in «Diritto penale contemporaneo-Rivista trimestrale», 2023, 1, p. 85.

[64] D. Piva, *Machina discere*, cit., pp. 691-692.

Autori

Salvatore Amato, Dottorando di ricerca in Scienze delle pubbliche amministrazioni – Università degli Studi di Messina

Giulia Bazzoni, Assegnista di ricerca – Università degli Studi di Verona

Francesca Casciaro, Dottoressa di ricerca in Principi giuridici ed istituzioni fra mercati globali e diritti fondamentali – Università degli Studi di Bari Aldo Moro

Enza Cirone, Assegnista di ricerca in Diritto dell'Unione europea – Università degli Studi di Firenze

Alice Civitella, Dottoranda di ricerca in Scienze strategiche e giuridiche dell'innovazione per la difesa e la sicurezza – Università degli Studi di Torino / Centro Alti Studi per la Difesa

Matthias Da Rold, Assegnista di ricerca in Diritto penale – Università Bocconi

Francesca De Vincentiis, Dottoranda di ricerca in Diritto tributario – Università degli Studi di Teramo

Thomas Di Candia, Assegnista di ricerca in Diritto processuale penale – Università degli Studi dell'Insubria

Sabrina Akram Ibrahim El Sabi, Dottoressa di ricerca in Principi giuridici ed istituzioni fra mercati globali e diritti fondamentali – Università degli Studi di Bari Aldo Moro

Lorenzo Mariconda, Ricercatore a tempo determinato in Diritto commerciale – Università degli Studi di Napoli Federico II

Lorenzo Rodio Nico, Post-doctoral researcher – Regione Puglia / Università degli Studi di Bari Aldo Moro

Luigi Prosia, Assegnista di Ricerca in Filosofia del diritto, Informatica giuridica e Biogiuridica –Università degli Studi di Roma Tor Vergata

Riccardo Lazzardi, Dottorando in Scienze giuridiche – Università degli Studi di Cagliari

Giacomo Angelo Puggioni, Dottorando in Scienze giuridiche – Università degli Studi di Cagliari

Ludovica Serreli, Dottoranda di ricerca in Scienze giuridiche – Università degli Studi di Cagliari

Andrea Tronci, Dottorando in Scienze giuridiche – Università degli Studi di Cagliari

Pietro Villaschi, Ricercatore in tenure track in Diritto costituzionale e pubblico – Università degli Studi di Milano

UNIVERSITÀ DEGLI STUDI DI CAGLIARI

Pubblicazioni del Dipartimento di Giurisprudenza

Serie I (Giuridica)

Edizioni CEDAM

1. E. Bussi, *Il diritto del Sacro Romano Impero alla fine del XVIII secolo*, 1957, in 8°, pp. XI-217.
2. G. Ardau, T*eoria giuridica dello sciopero*, 1962, in 8°, pp. XVI-275.
3. R. Socini, *Gli accordi internazionali delle organizzazioni intergovernative*, 1962, in 8°, pp. XXXII-295.
4. A. Malinverni, *Principi di diritto penale tributario*, 1962, in 8°, pp. VII-278.
5. R. Socini, *La competenza pregiudiziale della Corte di giustizia delle Comunità europee*, 1967, in 8°, pp. XII-234.

Edizioni Giuffrè

6. D. Barillaro, C*onsiderazioni preliminari sulle confessioni religiose diverse dalla cattolica, seconda edizione*, 1968, in 8°, pp. 142.
7. *Congresso giuridico nazionale in memoria di Carlo Fadda* (Cagliari-Sassari 23-26 maggio 1955), 1968, in 8°, pp. 168.
8. A. Porcella, *La tutela dei legittimari*, 1969, in 8°, pp. VIII-212.
9. S. Lariccia, *Considerazioni sull'elemento personale dell'ordinamento giuridico canonico*, 1971, in 8°, pp. IV-136.
10. G. Contini, *La revisione costituzionale in Italia*, 1971, in 8°, pp. IV-344.
11. A. Masi, *Ricerche sulla «Res privata» del «Princeps»*, 1971, in 8°, pp. IV-136.
12. L. Vacca, *Ricerche in tema di «actio vi bonorum raptorum»*, 1971, in 8°, pp. IV-176.
13. G. D'amelio, *Indagini sulla transazione nella dottrina intermedia con un'appendice sulla scuola di Napoli*, 1972, in 8°, pp. IV-192.
14. A. Luminoso, *La tutela aquiliana dei diritti personali di godimento*, 1972, in 8°, pp. IV-388.
15. A. Pace, *Il potere d'inchiesta delle assemblee legislative - Saggi*, 1973, in 8°, pp. XII-240.
16. R. Corona, *Contributo alla teoria del condominio negli edifici*, 1974, in 8°, pp. IV-252.
17. S. Lariccia, *Diritto ecclesiastico italiano*, 1974, in 8°, pp. VIII-336.
18. G. Palermo, *Contratto di alienazione e titolo dell'acquisto*, 1974, in 8°, pp. IV-160.
19. L. Vacca, *Contributo allo studio del metodo casistico nel diritto romano, ristampa con appendice*, 1982, in 8°, pp. IV-192.
20. *Studi in memoria di Giuliana d'Amelio*, vol. primo, 1978, in 8°, pp. VIII-428.
21. *Studi in memoria di Giuliana d'Amelio*, vol. secondo, 1978, in 8°, pp. VIII-400.
22. F. Sitzia, *Studi sulla superficie in epoca giustinianea*, 1979, in 8°, pp. IV-120.
23. A. Luminoso, *Il mutuo dissenso*, 1980, in 8°, pp. IV-420.

24. O. Diliberto, *Ricerche sull'«auctoramentum» e sulla condizione degli «auctorati»*, 1981, in 8°, pp. IV-120.
25. I. Birocchi, *Per la storia della proprietà perfetta in Sardegna*, 1982, in 8°, pp. IV-552.
26. *Legge, giudici, giuristi. Atti del convegno tenuto a Cagliari nei giorni 18-21 maggio 1981*, 1982, in 8°, pp. IV-332.

Edizioni Jovene

27. G. Zuddas, Il contratto di factoring, 1983, in 8°, pp. XII-264.
28. I. Castangia, *Il criterio della cittadinanza nel diritto internazionale privato*, 1983, in 8°, pp. XVI-244.
29. G. Filanti, *Inesistenza e nullità del negozio giuridico*, 1983, in 8°, pp. XII-316.
30. F. Sitzia, *Le Rhopai*, 1984, in 8°, pp. VIII-208.
31. R. Corona, *Convivenza intollerabile e separazione dei coniugi*, 1984, in 8°, pp. XX-320.
32. O. Diliberto, S*tudi sulle origini della 'cura furiosi'*, 1984, in 8°, pp. VIII-140.
33. M. Dogliani, I*ndirizzo politico*, 1985, in 8°, pp. XII-232.
34. G. Pau, *Le droit interne dans l'ordre international*, 1985, in 8°, pp. VIII-74.
35. P. Masi, *Articolazioni dell'iniziativa economica e unità dell'imputazione giuridica*, 1985, in 8°, pp. XVI-504.
36. G. Rolla, *Indirizzo politico e Tribunale costituzionale in Spagna*, 1986, in 8°, pp. VIII-368.
37. G. Paganetto, *Poteri del parlamento e governo dell'economia*, 1987, in 8°, pp. VIII-120.
38. G. Cocco, *La bancarotta preferenziale*, 1987, in 8°, pp. XII-372.
39. I. Castangia, *Sovranità, contiguità territoriale e isole in una controversia internazionale del XVIII secolo*, 1988, in 8°, pp. XII-216.
40. V. Mannino, I*l calcolo della* «quarta *hereditatis*» *e la volontà del testatore*, 1989, in 8°, pp. XII-176.
41. A. Pintore, *La teoria analitica del concetti giuridici*, 1990, in 8°, pp. VIII-336.
42. M. Ronco, *Il controllo penale degli stupefacenti*, 1990, in 8°, pp. XII-396.
43. P. Floris, *Autonomia confessionale*, 1992, in 8°, pp. VIII-300.
44. G. Paganetto, *Il potere governativo di nomina*, 1994, in 8°, pp. VIII-148.
45. M.V. Giangrieco Pessi, *Ricerche sull'actio de pauperie. Dalle XII tavole ad Ulpiano*, 1995, in 8°, pp. X-343.
46. G. Demuro, *Le delegificazioni: modelli e casi*, 1995, in 8°, pp. X-226.

Edizioni Giappichelli

47. M. Deiana, *I liens nei contratti di utilizzazione della nave*, 1995, in 8°, pp. XII-304.
48. L. Murtas, *Efficacia probatoria e costitutività della polizza di carico*, 1996, in 8°, pp. X-150.
49. A. Pintore, *Il diritto senza verità*, 1996, in 8°, pp. X-270.
50. V. Caredda, *Le liberalità diverse dalla donazione*, 1996, in 8°, pp. X-302.
51. P. Floris, *L'ecclesiasticità degli enti. Standards normativi e modelli giurisprudenziali*, 1997, in 8°, pp. VIII-332.
52. G. Zilio Grandi, *Parti sociali e contratto collettivo nell'Unione europea*, 1998, in 8°, pp. X·210

53. L. Cavallini Cadeddu, *L'autonomia delle Università. Aspetti finanziari e contabili*, 1998, in 8°, pp. VIII-296.
54. E. Loffredo, *Economicità e impresa*, 1999, in 8°, pp. VIII·300.
55. M. Piras, *L'assistenza a terra nel trasporto aereo. Profili privatistici*, 1999, in 8°, pp. VIII-224.
56. E. Dovere, *De iure. Studi sul titolo I delle Epitomi di Ermogeniano*, 2001, in 8°, pp. X-170.
57. E. Colarullo(a cura di), *Rappresentanza politica e gruppi delle assemblee elettive. Atti del Convegno tenutosi a Cagliari il 25 settembre 1999*, 2001, in 8°, pp. VIII-200.
58. C. Chessa, *La trattativa nella disciplina delle clausole abusive*, 2001, in 8°, pp. VIII-128.
59. R. Corona, *Proprietà e maggioranza nel condominio negli edifici*, 2001, in 8°, pp. XVI-560.
60. A.P. Ugas, *Il negozio giuridico come fonte di qualificazione e disciplina di fatti*, 2002, in 8°, pp. XII-304.
61. L. Cavallini Cadeddu (a cura di), *Controlli interni nelle pubbliche amministrazioni e decreto legislativo n. 286 del 1999. Atti del Convegno tenutosi a Cagliari il 6-7 ottobre 2000*, 2002, in 8°, pp. X-306.
62. R. Fercia, *Criteri di responsabilità dell'exercitor. Modelli culturali dell'attribuzione di rischio e 'regime' della nossalità nelle azioni penali* in factum contra nautas, caupones et stabularios, 2002, in 8°, pp. XII-312.
63. G. Demuro, *Regole costituzionali non scritte tra diritto ed altre scienze*, 2003, in 8°, pp. VIII-128.
64. L. Cavallini Cadeddu (a cura di), *Linee di riforma dei bilanci pubblici. Atti del Convegno tenutosi a Cagliari il 7-8 giugno 2002*, 2003, in 8°, pp. XVIII-350.
65. F. Botta (a cura di), *Il diritto giustinianeo fra tradizione classica e innovazione. Atti del Convegno. Cagliari, 13-14 ottobre 2000*, 2003, in 8°, pp. VIII-336.
66. V. Caredda, *Autoresponsabilità e autonomia privata*, 2004, in 8°, pp. X-214.

Edizioni Jovene

67. A.M. Mancaleoni, *I contratti con i consumatori tra diritto comunitario e diritto comune europeo*, 2005, in 8°, pp. VIII-312.
68. R. Pilia, *I diritti sociali*, 2005, in 8°, pp. XVIII-330.
69. R. Fercia, *Dovere di diligenza e «rischi funzionali»*, 2005, in 8°, pp. X-290.
70. S. Puddu, *Contributo ad uno studio sull'anormalità dell'atto amministrativo informatico*, 2006, in 8°, pp. XVI-312.
71. M. Perreca, *La congruità dello scambio contrattuale*, 2006, in 8°, pp. VIII-272.
72. I. Ruggiu, *Contro la Camera delle Regioni. Istituzioni e prassi della rappresentanza territoriale*, 2006, in 8°, pp. XII-452.
73. R. Cherchi, *Il governo di coalizione in ambiente maggioritario*, 2006, in 8°, pp. XII-484.
74. R. Fadda, *La riparazione e la sostituzione del bene difettoso nella vendita. Dal codice civile al codice di consumo*, 2007, in 8°, pp. X-318.
75. P. Cotza, *Potere autoritativo e modelli consensuali nel diritto dell'amministrazione pubblica (contributo metodologico)*, 2007, in 8°, 2 tomi, pp. XXVIII-800.

76. G. De Giudici, *Il governo ecclesiastico nella Sardegna sabauda (1720-1761)*, 2007, in 8°, pp. XIV-294.
77. M. Tola, *Opa e tutela delle minoranze*, 2008, in 8°, pp. XX-332.
78. S. Tatti, *La* «nuova» *partecipazione al procedimento amministrativo*, 2009, in 8°, pp. VIII-200.
79. C. Dore jr., *L'impossibilità della prestazione per fatto del creditore*, 2010, in 8°, pp. X-134.
80. L. Sitzia, *Pari dignità e discriminazione*, 2011, in 8°, pp. X-350.
81. L. Cavallini Cadeddu (a cura di), *Il coordinamento dinamico della finanza pubblica. Atti del Convegno di Cagliari, 15-16 ottobre 2010*, 2012, in 8°, pp. X-478.
82. R. Fadda, *La tutela preventiva dei diritti di credito*, 2012, in 8°, pp. X-318.
83. P. Cotza, *Dell'interesse pubblico e di altri "incidenti" nell'annullamento d'ufficio e nella convalida delle fattispecie precettive di diritto amministrativo*, 2012, in 8°, pp. XVI-728.
84. R. Fercia, «*Fiduciam contrahere*» e «*contractus fiduciae*». *Prospettive di diritto romano ed europeo*, 2012, in 8°, pp. XVI-384.
85. M.V. Sanna, *Matrimonio e altre situazioni matrimoniali nel diritto romano classico. Matrimonium iustum-matrimonium iniustum*, 2012, in 8°, pp. VIII-240.
86. A. Cherchi, *Ricerche sulle* «*usurae*» *convenzionali nel diritto classico*, 2012, in 8°, pp. XII-244.
87. S. Trevisanut, *Immigrazione irregolare via mare: diritto internazionale e diritto dell'Unione europea*, 2012, in 8°, pp. XXIV-360.

UNIVERSITÀ DEGLI STUDI DI CAGLIARI

Pubblicazioni del Dipartimento di Giurisprudenza

Serie II

Edizioni Jovene

1. G. Coinu, *Per un diritto costituzionale all'istruzione adeguata*, 2012.
2. R. Cherchi, *Lo straniero e la Costituzione. Ingresso, soggiorno e allontanamento*, 2012.
3. P. Cotza, *Il "merito amministrativo". Contenuto, rilievo giuridico e correlata "giurisdizione"*, 2012.

Edizioni ESI

4. G. Lorini e M. Masia (a cura di), *Antropologia della vendetta*, 2015.
5. C. Zuddas, *Strumenti e modelli per la tutela giuridica delle espressioni culturali tradizionali*, 2015.
6. S. Deplano, *Le obbligazioni negative*, 2014.
7. C. Cicero e V. Caredda, Rent to buy. *Atti del XXV incontro del Coordinamento nazionale dei dottorati di ricerca di diritto privato*, 2016.
8. D. Durisotto, *Istituzioni europee e libertà religiosa. CEDU e UE tra processi di integrazione europea e rispetto delle specificità nazionali*, 2016.
9. C. Dore, *La delegazione di pagamento nel quadro dei negozi sull'esecuzione del rapporto obbligatorio*, 2017.
10. O.G. Loddo, *Ideologie e concetti in aziende. Un'analisi filosofica degli usi aziendali*, 2017.
11. A. Viana, *La pubblicità nella vendita immobiliare*, 2017.
12. L. Ancis, *Informazione e assistenza del passeggero nel trasporto aereo. Il mutamento dei connotati dell'obbligo di protezione*, 2017.
13. F. Botta e F. Cordopatri (a cura di), *Il processo e le sue alternative. Storia, teoria, prassi*, 2017.
14. P. Cotza, *L'«interesse legittimo» alla luce di un discorso teoretico-giuridico sul rapporto amministrativo ed il suo processo*, 2017.
15. O. Dessì, *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. lav.*, 2017.
16. A.P. Ugas, *Delle obbligazioni divisibili e indivisibili*, 2018.
17. M. Martis, *Contributo allo studio della discrezionalità nel diritto tributario*, 2018.
18. V. Corona, *Il rischio del nolo fra disciplina legale e* charterparties, 2019.
19. C. Cicero (a cura di), *I danni punitivi. Tavola rotonda*, 2019.
20. D. Carta, *L'istruttoria tributaria sui dati finanziari*, 2019.
21. M. Rinaldo, *La teorica dell'invalidità dell'atto iniquo. Regole di validità e di responsabilità nel diritto privato*, 2019.
22. L. Filippi, M.F. Cortesi e A. Chelo (a cura di), *Il «processo delle cose». Atti della prima sessione del Convegno «Il «processo alle cose» e le «nuove» impugnazioni: un bilancio a 30 anni dal «nuovo» codice»*, 2019.

23. S. Corso (a cura di), *Startup e PMI innovative: scelte statutarie e finanziamento. Atti del Convegno di Studi*, 2019.
24. M.V. Sanna e M. Masia (a cura di), *Donne: libertà, diritti e tutele*, 2019.
25. M. Betzu (a cura di), *Diritto all'acqua e servizio idrico integrato*, 2019.
26. G. De Giudici, Sanctitas legatorum. *Sul* «fondamento» *dell'indipendenza giurisdizionale in età moderna*, 2020.
27. *Studi economico-giuridici – volume LXII, 2009-2020. Annali 2020*, I, 2020.
28. V. Corona e M.F. Cortesi (a cura di), *Emergenza e diritti tra presente e futuro*, 2020.
29. *Studi economico-giuridici – volume LXII, 2009-2020. Annali 2020*, II, 2020.
30. P. Corrias e E. Piras (a cura di), *I soggetti vulnerabili nell'economia, nel diritto e nelle istituzioni*, 2021.
31. F. Lubrano, *Miscellanea 1971-2003*, 2021.
32. C. Cicero, *Giuristi 'notevoli' dell'Università di Cagliari. Ritratti del Novecento*, 2021.
33. A. Berlinguer (a cura di), *Il commercio internazionale nel Mediterraneo*, 2021.
34. E.M. Mastinu, *Stato, Regioni e sindacato nella disciplina del lavoro alle dipendenze delle autonomie regionali*, 2021.
35. G. Coinu (a cura di), *Libera circolazione: Regioni, colori, provvedimenti*, 2021.
36. P. Corrias e E. Piras (a cura di), *I soggetti vulnerabili nell'economia, nel diritto e nelle istituzioni*, vol. II, 2021.
37. G. Demuro, G. Coinu, R. Montaldo(a cura di), *Governance dei Big Data e politiche pubbliche*, 2021.
38. Aa.Vv., *Scritti in onore di Pietro Ciarlo*, 3 tomi indivisibili, 2022.
39. C. Cicero (a cura di), *Le categorie generali nell'emergenza sanitaria*, 2022.
40. C. Dore, *Il prestito vitalizio ipotecario tra tutela del credito e attuazione del programma negoziale*, 2022.

Edizioni Cacucci

41. Daniele Amoroso e Andrea Deffenu (a cura di), *Intelligenza artificiale, dati e diritto*, 2025.