A.C. Amato Mangiameli, P. Simone, C. Venturini (a cura di), *Nuove tecnologie e diritto. Opportunità e rischi per la società del XXI secolo*

Comitato scientifico:
Prof.ssa Agata Cecilia Amato Mangiameli, Prof.ssa Arianna Andreangeli, Prof. Rainer Arnold, Prof. Vincenzo Baldini, Prof. Stéphane Bauzon, Prof. Andrea Biondi, Prof. Andrea Buratti, Dott.ssa Maria Novella Campagnoli, Prof. Emanuel Castellarin, Prof. Cláudio Roberto Cintra Bezerra Brandão, Prof. Roberto Cisotta, Dott.ssa Cristina Colombo, Prof. Cristiano Cupelli, Prof. Antonio D'Atena, Prof. Alessandro Dani, Prof. Luigi Daniele, Prof.ssa Maria Rosa Di Simone, Prof.ssa Encarnación Fernández Ruiz-Gálvez, Prof. Marco Fioravanti, Prof.ssa Rosa Maria Geraci, Prof.ssa Alessandra Gianelli, Prof. Giovanni Guzzetta, Prof. José Luis Iriarte Angel, Prof.ssa Christine Kaddous, Prof. Carlo Longari, Prof. Raffaello Lupi, Prof.ssa Stefania Mabellini, Prof. Stelio Mangiameli, Prof. Venerando Marano, Prof. Francesco Saverio Marini, Prof. Francesco Martucci, Prof. Gian Piero Giuseppe Milano, Prof.ssa Donatella Morana, Prof.ssa Federica Mucci, Prof. Nino Paolantonio, Prof. Vasco Pereira Da Silva, Prof. Fabrice Picod, Prof. Eugenio Picozza, Prof. Aristide Police, Prof. Pietro Pozzaglia, Prof. Roberto Rampioni, Prof. Adolfo Scalfati, Dott. Pierluigi Simone, Prof. Fabio Spitaleri, Prof.ssa Elda Turco Bulgherini, Prof.ssa Chiara Vagaggini, Prof.ssa Samantha Velluti, Prof.ssa Alessia Vignoli.

Direzione:
Prof.ssa Agata Cecilia Amato Mangiameli

Comitato di redazione:
Laura Ancora, Melania Carteri, Lorenzo Corda, Susanna De Stefani, Fiammetta Nanni, Luigi Prosia (Coordinatore), Diana Tenenbaum, Caterina Tarquini, Silvia Ventrelli.

La corrispondenza inviata alla direzione o alla redazione della Collana va indirizzata a *quaderni.pubblico@gmail.com*.

I contributi sono sottoposti alla procedura di referaggio anonimo, conformemente al Regolamento della Collana dei Quaderni del Dottorato di ricerca in Diritto Pubblico, pubblicato sul sito *www.dot.dirittopubblico.uniroma2.it.*

UNIVERSITÀ DEGLI STUDI DI ROMA "TOR VERGATA"
COLLANA DELLE PUBBLICAZIONI DEL DIPARTIMENTO DI GIURISPRUDENZA
QUADERNI DEL DOTTORATO DI RICERCA IN DIRITTO PUBBLICO
6

Nuove tecnologie e diritto
Opportunità e rischi per la società del XXI secolo

a cura di
Agata C. Amato Mangiameli
Pierluigi Simone
Chiara Venturini

Wolters Kluwer CEDAM

Il presente volume è stato pubblicato con i fondi del Dottorato di ricerca in Diritto Pubblico del Dipartimento di Giurisprudenza dell'Università degli Studi di Roma "Tor Vergata".

Copyright 2025 Wolters Kluwer Italia S.r.l.
Via Bisceglie n. 66 - 20152 - Milano

È espressamente vietato ogni utilizzo di questa opera per l'addestramento di **processi di apprendimento automatico e intelligenza artificiale**, tra cui in particolare di IA generativa. In caso di violazione, l'editore si riserva il diritto di intraprendere le opportune azioni legali a tutela dei propri diritti.
I diritti di traduzione, di memorizzazione elettronica, di riproduzione e di adattamento totale o parziale, con qualsiasi mezzo (compresi i microfilm e le copie fotostatiche), sono riservati per tutti i Paesi.
Le fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume/fascicolo di periodico dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941, n. 633.
Le riproduzioni diverse da quelle sopra indicate (per uso non personale - cioè, a titolo esemplificativo, commerciale, economico o professionale - e/o oltre il limite del 15%) potranno avvenire solo a seguito di specifica autorizzazione rilasciata da EDISER Srl, società di servizi dell'Associazione Italiana Editori, attraverso il marchio CLEARedi Centro Licenze e Autorizzazioni Riproduzioni Editoriali. Informazioni: www.clearedi.org.

L'elaborazione dei testi, anche se curata con scrupolosa attenzione, non può comportare specifiche responsabilità per eventuali involontari errori o inesattezze.

Stampato da GECA - Divisione Libri di CISCRA S.p.A.
Via Belvedere, 42 - 20862 Arcore (MB)

INDICE

Notizie sugli Autori IX

Agata C. Amato Mangiameli, Pierluigi Simone, Chiara Venturini, Presentazione XI

Sezione Prima

CONTRIBUTI DEI CURATORI

Agata C. Amato Mangiameli, Intelligenza artificiale generativa e metaverso. A proposito di menti e corpi fusi con IA 3

Pierluigi Simone, Verso l'individuazione di una "via europea" allo sviluppo tecnologico. Alcune riflessioni sul regolamento (UE) 2024/1689 che stabilisce norme armonizzate sull'intelligenza artificiale 15

Chiara Venturini, The Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law promoted by the Council of Europe: Some Critical Issues 43

Sezione Seconda

LEZIONI

Arianna Andreangeli, Algoritmi di prezzo e legge sull'intelligenza artificiale: navigare in acque inesplorate tra il diritto della concorrenza e la regolamentazione tradizionale delle tecnologie autonome 63

Vincenzo Ricciuto, La costruzione di un mercato antropocentrico dell'intelligenza artificiale tra diritto dell'Unione e diritto nazionale 85

Alberto Zito, L'esercizio della funzione amministrativa attraverso l'intelligenza artificiale: potenzialità e limiti del suo utilizzo da parte delle pubbliche amministrazioni 95

© Wolters Kluwer Italia

SEZIONE TERZA

LE QUESTIONI CONNESSE ALL'USO DELLE NUOVE TECNOLOGIE NEL PROCESSO E LA GIUSTIZIA PREDITTIVA

LAURA ANCORA, La giustizia amministrativa digitale 115
MATTEO CECILIA, Giudizio di diritto, prevedibilità delle decisioni e intelligenza artificiale 125
GIANLUIGI SCALA, Riflessioni sull'uso dell'intelligenza artificiale nel giudizio di fatto 133
MATTEO DE BIASE, L'impatto dell'evoluzione tecnologica nei processi decisionali amministrativi di tipo ambientale 145
IACOPO CHIANELLO, Processo penale e *digital evidence*: sfide irrisolte nell'acquisizione di conversazioni digitali 155

SEZIONE QUARTA

DIVIETO DI DISCRIMINAZIONE E TUTELA DEI DIRITTI DELLA PERSONA

SILVIA VENTRELLI, Il rischio di discriminazione algoritmica nel mercato del lavoro dell'era digitale: le norme dell'Unione europea nel quadro della *gig economy* 167
EMILIO ADAMO, Le tecnologie impiegate nei controlli alle frontiere esterne dell'Unione europea ed il relativo impatto sulla tutela dei diritti fondamentali 177
DOMENICO ANDREA PISANI, Principio di precauzione e intelligenza artificiale 191
GABRIELLA CATALDI, La presunzione di subordinazione nel lavoro tramite piattaforme digitali 201
MELANIA CARTERI, Il lavoro che cambia e si adegua all'era della trasformazione digitale 211
GIANLUCA FASANO, Decisioni automatizzate: il futuro dei diritti nella società digitale 223

SEZIONE QUINTA

STRUMENTI DIGITALI E PROBLEMI DI RESPONSABILITÀ

ORIANA LOMBARDI, Responsabilità penale dell'uomo per l'utilizzo di sistemi di intelligenza artificiale 237
FEDERICA PALOMBA, La responsabilità delle decisioni amministrative automatizzate 247

© Wolters Kluwer Italia

Arianna Giacchino, I criteri di imputazione della responsabilità da reato degli agenti non umani: *machina delinquere potest*? 257

Sezione Sesta

NUOVE TECNOLOGIE E REALTÀ TRASFORMATE

Susanna De Stefani, Il pluralismo dell'informazione al vaglio delle piattaforme digitali 271
Luigi Prosia, *E-health* e IA generativa. Un richiamo alle più alte garanzie nella cura della persona 283
Lorenzo Corda, Unione europea, "*cyber threats*" e sanzioni: un approccio multifase 295
Valerio Maggio, Arte e tecnologia: tracciabilità e intelligenza artificiale 307
Marina Righi, L'economia digitale e le nuove regole sulla tassazione minima 319

Appendice 329

© Wolters Kluwer Italia

NOTIZIE SUGLI AUTORI

Agata Cecilia Amato Mangiameli, Professoressa ordinaria di Filosofia del diritto, Informatica giuridica e Biogiuridica presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Roma "Tor Vergata"

Arianna Andreangeli, Professoressa di *Competition Law* presso l'Università di Edimburgo, *School of Law*

Vincenzo Ricciuto, Professore ordinario di Diritto civile presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Roma "Tor Vergata"

Pierluigi Simone, Ricercatore confermato di Diritto dell'Unione europea presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Roma "Tor Vergata"

Chiara Venturini, Ricercatrice di Diritto internazionale presso il Dipartimento di Scienze Giuridiche ed Economiche dell'Università degli Studi di Roma "UnitelmaSapienza"

Alberto Zito, Professore ordinario di Diritto amministrativo presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Roma "Tor Vergata"

Emilio Adamo, Dottorando di ricerca in Diritto Pubblico, *indirizzo*: Diritto dell'Unione europea, XXXVIII ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

Laura Ancora, Dottoranda di ricerca in Diritto Pubblico, *indirizzo*: Diritto amministrativo, XXXVII ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

Melania Carteri, Dottoranda di ricerca in Diritto Pubblico, *indirizzo*: Diritto del lavoro, XXXIX ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

Gabriella Cataldi, Dottoranda di ricerca in Diritto Pubblico, *indirizzo*: Diritto del lavoro, XXXIX ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

Matteo Cecilia, Dottorando di ricerca in Diritto Pubblico, *indirizzo*: Diritto tributario, XXXVIII ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

© Wolters Kluwer Italia

IACOPO CHIANELLO, Avvocato e Dottorando di ricerca in Diritto Pubblico, *indirizzo*: Diritto penale, XXXIX ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

LORENZO CORDA, Dottorando di ricerca in Diritto Pubblico, *indirizzo*: Diritto dell'Unione europea, XXXIX ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

MATTEO DE BIASE, Dottorando di ricerca in Diritto Pubblico, *indirizzo*: Diritto amministrativo, XXXVII ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

SUSANNA DE STEFANI, Dottoranda di ricerca in Diritto Pubblico, *indirizzo*: Diritto dell'Unione europea, XXXVII ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

GIANLUCA FASANO, Dottorando di ricerca in Diritto Pubblico, *indirizzo*: Diritto costituzionale, XXXVIII ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

ARIANNA GIACCHINO, Dottoranda di ricerca in Diritto Pubblico, *indirizzo*: Diritto penale, XXXVIII ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

ORIANA LOMBARDI, Dottoranda di ricerca in Diritto Pubblico, *indirizzo*: Diritto penale, XXXIX ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

VALERIO MAGGIO, Avvocato stabilito e Dottorando di ricerca in Diritto Pubblico, *indirizzo*: Diritto tributario, XXXIX ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

FEDERICA PALOMBA, Dottoressa di ricerca in Diritto Pubblico, *indirizzo*: Diritto amministrativo, XXXV ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

DOMENICO ANDREA PISANI, Dottorando di ricerca in Diritto Pubblico, *indirizzo*: Diritto costituzionale, XXXVII ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

LUIGI PROSIA, Dottore di ricerca in Diritto Pubblico, *indirizzo*: Teoria generale dello Stato, XXXVI ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

MARINA RIGHI, Dottoressa di ricerca in Diritto Pubblico, *indirizzo*: Diritto tributario, XXXVI ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

GIANLUIGI SCALA, Avvocato e Dottorando di ricerca in Diritto Pubblico, *indirizzo*: Diritto tributario, XXXIX ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

SILVIA VENTRELLI, Dottoranda di ricerca in Diritto Pubblico, *indirizzo*: Diritto dell'Unione europea, XXXVIII ciclo, presso l'Università degli Studi di Roma "Tor Vergata"

© Wolters Kluwer Italia

PRESENTAZIONE

Il presente Volume, curato da Agata C. Amato Mangiameli, Pierluigi Simone e Chiara Venturini, è il n. 6 dei *Quaderni del Dottorato di Ricerca in Diritto Pubblico* dell'Università degli Studi di Roma "Tor Vergata". I *Quaderni* costituiscono una Serie speciale, parte integrante della *Collana delle pubblicazioni del Dipartimento di Giurisprudenza*, a cui il Dottorato in Diritto Pubblico afferisce.

Al pari degli anni precedenti, il Quaderno n. 6 raccoglie i contributi dei dottorandi (diciannove in questa edizione) che hanno scelto di affrontare, ciascuno nell'ambito della materia inerente al proprio *curriculum* di studio, nel rispetto del carattere multisettoriale del Dottorato, il tema del rapporto esistente tra nuove tecnologie e diritto.

Il Volume si compone di sei Sezioni.

Gli scritti dei dottorandi, come di consueto, sono stati arricchiti, nella Sezione Seconda, dai testi di due lezioni tenute rispettivamente da Arianna Andreangeli, Professoressa di *Competition Law* nell'Università di Edimburgo, e da Alberto Zito, Professore ordinario di Diritto amministrativo nel Dipartimento di Giurisprudenza dell'Università degli Studi di Roma "Tor Vergata". La lezione della Professoressa Andreangeli ha ad oggetto il rapporto tra la disciplina della concorrenza ed il nuovo regolamento sull'intelligenza artificiale dell'Unione europea, il c.d. *AI Act*. La lezione del Professor Zito verte, invece, sull'esercizio della funzione amministrativa tramite l'impiego dell'intelligenza artificiale. I Curatori, poi, hanno ritenuto opportuno inserire nella suddetta Sezione anche un contributo di Vincenzo Ricciuto, Professore ordinario di Diritto privato anch'egli nel Dipartimento di Giurisprudenza dell'Università degli Studi di Roma "Tor Vergata", sul tema della costruzione di un mercato antropocentrico dell'intelligenza artificiale, così da valorizzare l'opera con l'apporto di un giurista privatista.

Confluiscono, inoltre, nel Volume anche i saggi dei tre Curatori. La complessità degli argomenti affrontati ha infatti reso opportuni, anteponendoli nella Sezione Prima, degli approfondimenti i quali, senza presunzione di completezza, diano comunque contezza delle prospetti-

© Wolters Kluwer Italia

ve della filosofia del diritto, del diritto dell'Unione europea e del diritto internazionale.

L'intrinseca relazione sussistente tra fatto e diritto ha determinato, peraltro con particolare naturalezza, l'individuazione del tema di questo n. 6. L'inarrestabile sviluppo delle nuove tecnologie e il loro impiego in vari settori del diritto hanno imposto l'approfondimento scientifico che questo testo ambisce a offrire. Tutti i contributi analizzano in chiave critica sia i vantaggi che l'utilizzo di nuove tecnologie può fornire all'operatore giuridico, sia gli aspetti più problematici che derivano dall'applicazione di macchine nell'esercizio di poteri pubblici. Le facilitazioni derivanti dall'impiego di nuove tecnologie in vari settori di interesse pubblico sono del tutto evidenti: semplificazione delle procedure, efficienza dei risultati e riduzione dei costi. Sono tuttavia innegabili i molteplici rischi che possono sorgere. È appena il caso di citare i problemi legati al rispetto della riservatezza dei cittadini o alla realizzazione di forme di controllo e/o di repressione dei crimini (informatici e non). Altrettanto noti, ormai, sono i benefici del processo di digitalizzazione sull'ambiente, tali da permettere di ridurre gli sprechi, di promuovere un'economia di tipo circolare e di ottenere uno sviluppo sostenibile. Allo stesso tempo, l'impiego di tecnologie avanzate impone agli Stati di dotarsi di sistemi di sicurezza adeguati a prevenire attacchi informatici a infrastrutture sensibili o in materia di immigrazione. È inoltre necessario considerare l'impatto della tecnologia sul tessuto sociale. Quest'ultima ha un duplice effetto: da un lato, alimenta l'inclusione, connettendo gli individui più velocemente e agilmente (con la possibilità di lavorare da remoto, di impiegare piattaforme *web* per fornire e/o usufruire di servizi o di informarsi); dall'altro, se si serve di algoritmi predittivi, può generare disuguaglianze, classificazioni e discriminazione. Analizzare in una prospettiva prettamente giuridica sia gli aspetti critici, sia le potenzialità dello sviluppo tecnologico è sembrato, quindi, quantomai opportuno.

La Sezione Terza è dedicata a "*Le questioni connesse all'uso delle nuove tecnologie nel processo e la giustizia predittiva*". In essa, Laura Ancora si sofferma sui due modelli di applicazione dell'intelligenza artificiale nel processo amministrativo: il primo vedrebbe l'eliminazione del controllo umano dall'attività decisionale, mentre il secondo vede l'intelligenza artificiale come uno strumento che coadiuva il giudice nel suo operato. L'Autrice analizza i vantaggi e gli svantaggi di entrambi gli approcci. Matteo Cecilia e Gianluigi Scala trattano l'impiego dell'intelligenza artificiale nel processo amministrativo, giungendo

© Wolters Kluwer Italia

alla conclusione che è pressoché impossibile evitare il controllo umano rispetto all'elaborazione algoritmica di una decisione, poiché non è raccomandabile eliminare il margine di apprezzamento del giudice. Ancora, Iacopo Chianello analizza il problema dell'acquisizione della *digital evidence* nel processo penale, rispetto alla quale l'attuale normativa nazionale risulta del tutto inadeguata. Infine, Matteo De Biase, occupandosi della compatibilità delle nuove tecnologie con il processo amministrativo, evidenzia la complementarità esistente tra la transizione verde e l'evoluzione tecnologica, e osserva come la seconda possa impattare sulla prima.

Particolare attenzione merita l'incidenza della tecnologia sulla tutela dei diritti della persona: si pensi alla questione della discriminazione prodotta da algoritmi programmati con un particolare *bias* e applicati a vari settori produttivi. A ciò è dedicata la Sezione Quarta, intitolata "*Divieto di discriminazione e tutela dei diritti della persona*". Silvia Ventrelli analizza la normativa europea in materia di *gig economy* e discriminazione dei lavoratori di piattaforme digitali, i quali rischiano la cessazione del rapporto di lavoro per mezzo di decisioni automatizzate. Gabriella Cataldi e Melania Carteri si soffermano sulle distorsioni che la tecnologia produce nel mondo del lavoro, analizzando, rispettivamente, la presunzione di subordinazione nel lavoro tramite piattaforma digitale e la necessità dell'ordinamento giuslavorista di adattarsi al processo di digitalizzazione (è il caso del lavoro da remoto). Emilio Adamo analizza le potenziali violazioni dei diritti fondamentali della persona generati dall'impiego di strumenti digitali alle frontiere esterne dell'Unione europea. Domenico Andrea Pisani si sofferma sulla necessità che i processi decisionali affidati all'intelligenza artificiale siano rispettosi del principio di precauzione, sia nella sua accezione generale, sia in quella di matrice ambientale. Da ultimo, Gianluca Fasano ragiona sull'ambito e sulle ricadute dei procedimenti decisionali totalmente automatizzati rispetto al futuro dei diritti nella società digitale, primo fra tutti il diritto all'oblio comportamentale.

L'uso dell'intelligenza artificiale nella formulazione di decisioni di diritto pubblico ha portato i dottorandi ad interrogarsi sulle situazioni connesse alla responsabilità. Nella Sezione Quinta "*Strumenti digitali e problemi di responsabilità*", Oriana Lombardi approfondisce la tematica della responsabilità penale dell'individuo, in particolare per negligenza, dovuta all'impiego di sistemi di intelligenza artificiale nel suo operato. Arianna Giacchino si sofferma sui criteri di imputazione della responsabilità penale di agenti non umani. Federica Palomba

© Wolters Kluwer Italia

studia la responsabilità per le decisioni amministrative automatizzate e i possibili rimedi per superare l'"opacità" nell'attribuzione della responsabilità stessa.

Se i contributi sin qui richiamati hanno approfondito in particolar modo le deviazioni o gli aggiustamenti prodotti dall'applicazione di nuove tecnologie a realtà giuridiche e fattuali già esistenti, è altrettanto vero che lo sviluppo tecnologico produce anche fattispecie nuove, che necessitano di regolamentazione. Nella Sezione Sesta su "*Nuove tecnologie e realtà trasformate*", i dottorandi non hanno mancato di dedicarsi a questi aspetti particolarmente innovativi. Susanna De Stefani nel suo elaborato analizza il pluralismo dei *media* e dell'informazione tramite piattaforme digitali, mettendo in risalto soprattutto le *policies* da adottare per combattere la disinformazione causata dalla moltitudine di fonti di informazione. Luigi Prosia ha studiato l'*e-health*, ovvero l'applicazione di nuove tecnologie al sistema di cura e diagnostico. Marina Righi si occupa di tassazione minima ed economia digitale, mentre Valerio Maggio si è interessato dell'impiego di nuovi strumenti tecnologici per migliorare la tracciabilità delle opere d'arte e, di conseguenza, la *compliance* con le norme in materia di tassazione. Infine, così come nuove sono le fattispecie, nuovi sembrano essere i rischi: il riferimento è agli attacchi *cyber*, di cui si occupa il contributo di Lorenzo Corda.

È d'obbligo ringraziare tutti coloro che hanno partecipato al presente Volume, permettendo così alla *Collana* di arricchirsi di un nuovo, prezioso elemento. Un doveroso e riconoscente pensiero va inoltre a tutti i membri del Comitato di Redazione, per essi al Coordinatore Luigi Prosia: il loro impegno costante e la loro dedita, capace collaborazione hanno reso possibile questo risultato.

AGATA C. AMATO MANGIAMELI
PIERLUIGI SIMONE
CHIARA VENTURINI

© Wolters Kluwer Italia

Sezione Prima

CONTRIBUTI DEI CURATORI

INTELLIGENZA ARTIFICIALE GENERATIVA E METAVERSO. A PROPOSITO DI MENTI E CORPI FUSI CON IA *

AGATA C. AMATO MANGIAMELI

SOMMARIO: 1. Menti e corpi fusi con IA. – 1.1. Il progetto scientifico-artistico di Avital Meshi. – 1.2. Gli impianti di interfaccia cervello-*computer*. – 2. IA e metaverso: nuovi attributi. – 3. Nuove dimensioni ancora da regolare.

Abstract: Generative Artificial Intelligence and Metaverse are the key expressions of our age. Expressions that everyone talks about, but which many misunderstand. This essay aims to highlight precisely the elements of continuity and novelty of both dimensions. The basic idea is that – faced with an increasingly intense integration between body-mind and AI – it is necessary to move from a new paradigm.

1. Menti e corpi fusi con lA

1.1. *Il progetto scientifico-artistico di Avital Meshi*

Vivere indossando vari dispositivi, vivere conversando con IA e rispondendo da IA, ovvero ripetendo quel che GPT sostiene! È, in questo momento, la vita che conduce Avital Meshi [1], al contempo, biologa comportamentale e *new media artist*, che, avvolta da cavi, legata a pul-

* Contributo sottoposto a doppio referaggio in forma anonima.

[1] Per il suo profilo, per le sue interviste e un elenco delle sue installazioni e *performance* (tra queste negli ultimi anni: *Move-me*, *AI Séance*, *GPT-me*, *Calling myself self*, *An ontology of becoming*, *This person is not me*, *The cyborg project*) v. il sito *avitalmeshi.com*.

© Wolters Kluwer Italia

santiere colorate e connessa a meccanismi alimentati da IA, ripete quel che la macchina le sussurra senza sosta e, nel frattempo, *GPT-Me* influenza il suo eloquio e il suo discorso, come pure il suo modo di interagire con l'altro (e gli altri), la sua maniera di provare ed esprimere sentimenti ed emozioni. Si tratta di piani diversi, ma si intravedono sin da subito i passaggi assai significativi che dalle espressioni verbali arrivano fino ai comportamenti e alle azioni.

Come è intuitivo, l'esperimento è quanto mai interessante. In generale, gli odierni e formidabili strumenti di informazione e comunicazione migliorano sia le capacità di investigazione e di prestazione, sia l'abilità di connettersi e di interagire, benché non di rado conducano ad esiti singolari, qualche volta inattesi e talaltra bizzarri. In particolare, con riguardo all'esperimento richiamato, si tratta, innanzitutto, di riuscire a trovare un possibile equilibrio tra l'ascolto di IA, che bisbiglia ininterrottamente all'orecchio, e l'interazione con la persona (o le persone) con cui si conversa. Diventare, inoltre, il portavoce di IA può generare (e genera) crisi di identità, tanto da spingere l'individuo a chiedersi se le parole formulate possano essere considerate come proprie, se le azioni eseguite possano essere valutate come proprie, o se, molto più semplicemente, tanto le une, quanto le altre, non siano solamente il risultato dei condizionamenti della stessa IA che, a seconda dei casi, parla, suggerisce, risponde. D'altra parte, i dispositivi qui usati consentono di intrattenere centinaia di conversazioni individuali, di esplorare di volta in volta diverse personalità e persino di affrontare le c.d. dimensioni del paranormale, trasformandosi all'occorrenza in una sorta di *medium* per sedute spiritiche in grado di evocare defunti più o meno noti. Avital Meshi è riuscita così a impersonare diverse persone (ad esempio: Leonard Cohen, Albert Einstein, Mahatma Gandhi, Alan Turing), va da sé che si tratta pur sempre di quelle persone che in qualche modo hanno lasciato delle impronte e/o tracce digitali idonee e funzionali ad addestrare GPT. Altrimenti detto, la portata di questi dispositivi è tale da immaginare continue aperture diacroniche fra presente e passato, e poi anche sul futuro, come pure occasioni determinanti per le scelte personali da intraprendere.

Al di là di risvolti particolari, l'esperimento di Meshi mostra in ogni caso le importanti potenzialità dell'integrazione tra corpi-menti e IA: in primo luogo, le conversazioni si arricchiscono, le sempre possibili lacune vengono colmate, gli eventuali ritardi si riducono notevolmente; i percorsi speculativi, inoltre, diventano, e possono diventare, originali e creativi, grazie all'ampiezza delle informazioni e alla ricchezza degli approcci; da ultimo, è la stessa intelligenza umana a ritrovarsi arricchita e potenziata, poiché quel che è poco noto o sconosciuto

© Wolters Kluwer Italia

all'uomo è efficacemente colmato dall'IA che, in tempo reale, non solo propone soluzioni e prospettive, ma fa sì in concreto che l'incontro con l'altro avvenga in condizioni idonee ed eguali.

È indubbio che in un mondo fatto di *corpi fusi con IA*, ossia con una IA sempre più integrata nella nostra vita quotidiana, si corre il serio rischio di affidarsi totalmente ai vari dispositivi, col pericolo che possano diminuire le nostre stesse capacità di pensare in modo indipendente e di distinguere la realtà da quei contenuti che, invece, sono generati e prospettati dall'IA. Le nuove tecnologie possono, inoltre, essere utilizzate per monitorare e influenzare il comportamento, alimentando pregiudizi, favorendo manipolazioni e sollevando problemi di *privacy*. Del resto, il timore di Avital Meshi consiste proprio in questo:

> A volte quando non lo indosso mi trovo a imitare alcune delle sue risposte quasi come se l'IA mi avesse addestrato a comportarmi in modo diverso. Questa influenza può essere vista in due modi: da un lato, sto cercando di adattarmi in modo più efficace a una nuova cultura, l'IA potrebbe essere uno strumento utile. D'altro canto, se altera in modo sottile le mie opinioni politiche o manipola le mie convinzioni, stiamo correndo un rischio serio come società [2].

1.2. *Gli impianti di interfaccia cervello*-computer

Le tecnologie hanno sempre avuto una grande influenza sugli individui e sulle società, e d'altra parte i più profondi rinnovamenti culturali e sociali sono stati ogni volta legati alle grandi invenzioni (dapprima la scrittura, poi la stampa, e di recente: *Internet*, i *social media*, i *big data*). A maggior ragione quanto detto vale nel caso di tecnologie che siano basate sull'IA, il loro uso, infatti, sta trasformando pressoché ogni settore, introducendo nuove modalità (ad esempio: di apprendimento, di elaborazione, di visione, di mobilità) e dischiudendo inedite possibilità (ad esempio: per la finanza, per l'istruzione, per la produzione, per la salute). Anche gli automi – soprattutto i robot umanoidi somiglianti agli esseri umani sia nell'aspetto e sia nel comportamento – grazie all'IA generativa diventano sempre più intelligenti, versatili, agili. Le loro prestazioni sono decisamente migliorate, percepiscono ormai l'ambiente e riconoscono gli oggetti, e tali capacità sensoriali permettono loro di eseguire compiti decisamente complessi (assem-

[2] Cfr. E. Rosso, *La donna che si è fusa con un'Intelligenza artificiale: "Ha trasformato la mia identità"*, intervista a Avital Meshi, in *Fanpage.it*, 9 ottobre 2024.

© Wolters Kluwer Italia

blaggio componenti, raccolta oggetti, manipolazione delle cose, modifica dei movimenti, assistenza e soccorso). I nuovi automi – tra gli altri: *Atlas*, *Atomo*, *Digit*, *Figure 0.1*, *Gr-1*, *H1*, *Optimus gen 2*., *Phoenix*, *Robee* – interagiscono in modo efficace con gli esseri umani nei più disparati luoghi (di lavoro, di cura, di gioco, ecc.). Attraverso la combinazione-integrazione di IA avanzata, di GPT per il *training*, di meccanica di precisione, i robot hanno potenziato le loro capacità di calcolo, incrementato la comprensione del linguaggio naturale, rafforzato l'abilità a ragionare e a muoversi. È il caso di *Alter3* che opera con la ricca base di conoscenze e le istruzioni motorie generate da GPT-4, di qualità nettamente superiore rispetto a quelle create secondo le tecniche tradizionali di addestramento robotico, perché la sua risposta è parecchio veloce, più ampia, e persino empatica. Sin qui, qualche nome di robot in grado di fornire, in contesti diversi, risposte e attività precise e importanti.

Per il nostro tema, di grande interesse è senz'altro la combinazione-integrazione di intelligenza umana e IA. Detto altrimenti, la ricostruzione si deve spostare dai robot umanoidi alle interfacce cervello-*computer*. Si pensi agli studi sugli impianti cerebrali, pensati per aiutare in modo particolare quei pazienti che, a causa di malattie, versano in condizioni neurologiche particolarmente difficili. Di recente, Neuralink ha conseguito il via libera da parte della *Food and Drug Administration* a proseguire l'attività di ricerca. Si tratta di un impianto – denominato *Telepathy* – che, con l'aiuto di un robot-chirurgo, deve essere collocato nella regione del cervello che controlla l'intenzione di muoversi, in modo da permettere al paziente di riuscire a muovere il cursore del *computer* con il solo pensiero. Possono essere, così, migliorate le prestazioni della mente e, cosa ancora più importante, possono essere ripristinate alcune funzioni che sembravano essere definitivamente perse.

Lo studio (*Precise Robotically Implanted Brain-Computer Interface*) è stato sperimentato su un giovane paziente paralizzato dal collo in giù, che è riuscito a fare alcune cose con l'uso dell'interfaccia cervello-*computer wireless*. L'impianto – che può essere inserito sotto il cuoio capelluto e che può essere infatti utilizzato senza alcun collegamento fisico a dispositivi esterni – in pratica traduce i segnali del pensiero (i c.d. *pattern* neuronali) in un'azione. In particolare, *Telepathy* è un dispositivo composto da cinque elementi fondamentali: una capsula esterna realizzata in materiale biocompatibile, una batteria ricaricabile, i *microchip* che traducono i segnali cerebrali e li trasmettono ai dispositivi, e da fili ed elettrodi collegati al cervello. In considerazione della difficoltà a maneggiare dei fili pressoché impalpabili, è stato progettato

© Wolters Kluwer Italia

un robot-chirurgo (*R1*) in grado di inserire e posizionare correttamente i fili nella corteccia cerebrale. E sono stati proprio questi fili sottilissimi a creare, nelle settimane successive all'intervento, delle complicanze, visto che alcuni si sono allontanati dal cervello e hanno causato una significativa diminuzione di elettrodi efficaci. A tal proposito, sul sito di Neuralink, si legge che per ovviare al distacco dei fili e, quindi, alla perdita di funzionalità degli elettrodi il robot inserirà i prossimi dispositivi più in profondità nel cervello (a circa 8 millimetri, piuttosto che a 5 del primo intervento [3]).

Oltre a *Telepathy*, è stato progettato anche un altro dispositivo: *Blindsight*, il cui *chip* è sempre impiantabile nel cervello in questo caso con lo scopo di far tornare a vedere chi sia affetto da cecità. Neuralink non è comunque l'unica azienda che sperimenta interfacce cervello-*computer*, anche Synchron ha già impiantato il proprio dispositivo in alcuni pazienti e si prepara a una sperimentazione clinica più ampia avendo lanciato un registro *online* per tutti quei pazienti che sono interessati [4].

2. IA e metaverso: nuovi attributi

Menti e corpi fusi con IA rinviano agli sviluppi, sia, della c.d. intelligenza artificiale generativa – che può essere usata per attività che richiedono un *know how* anche molto sofisticato e che coinvolgono veri e propri processi decisionali – e, sia, del metaverso che, al momento, sembra essere in crisi, e, in ogni caso, ridotto ad uno stadio embrionale, quale mera piattaforma che utilizza la *blockchain* come tecnologia di base e che ha un'economia interna edificata sugli oggetti digitali in formato NFT (*token* non fungibili) e gestita con le criptovalute. Conviene qui riprendere, pur nella sintesi, alcuni aspetti dell'IA (*i*) e del metaverso (*ii*).

i) A connotare l'IA c.d. avanzata è senza dubbio la capacità di produrre – e in senso proprio di generare – contenuti in maniera completamente autonoma. Contrariamente all'algoritmo dell'IA per così dire classica (che processa una considerevole quantità di dati di esempio e, con questi, auto-apprende, riuscendo in tal modo a ricondurre un nuovo

[3] Cfr. R. Mazzaracca, *Il primo impianto di Neuralink su un essere umano e Telepathy: come funziona l'interfaccia cervello-computer?*, in *Osservatorioterapieavanzate.it*, 12 giugno 2024.

[4] M. Manfrin, *Negli Stati Uniti si prepara la prima sperimentazione su larga scala di impianti cerebrali*, in *Lindipendente.online*, 11 aprile 2024.

© Wolters Kluwer Italia

esempio a una delle casistiche di addestramento), l'algoritmo di *GAI* (*Generative AI*) – pur essendo basato sempre sulla statistica – è in condizione di creare contenuti del tutto nuovi rispetto a quelli di addestramento. Ed è in ragione di questa sua peculiarità, che l'intelligenza artificiale generativa riesce a redigere testi di qualunque forma, estensione e genere (brevi carteggi epistolari, novelle, componimenti poetici, romanzi), adottando, a seconda delle esigenze e delle più specifiche richieste, registri comunicativi e stilistici assai differenti (può emulare la narrazione coinvolgente di famosi scrittori, ma è anche capace di prospettare uno stile tutto suo). Si aggiunga, poi, che *GAI* non solo produce testi, ma riesce persino a replicare, a manipolare e a produrre *ex novo* immagini, audio e video, che, pure quando sono frutto di un'alterazione palese, risultano comunque molto verosimili. In questo ambito grande interesse suscita soprattutto l'intelligenza artificiale conversazionale *text-oriented*: come noto, il primo *consumer chatbot* di IA generativa – basato sul modello di rete neurale GPT (acronimo di *generative pretrained transformer*) – è divenuto disponibile al pubblico nell'autunno del 2022.

Diversamente dall'IA tradizionale (con i tradizionali sistemi di *machine learning*) – che è basata su dati etichettati utilizzando tecniche di apprendimento supervisionato e che è orientata a eseguire attività molto specifiche e, se vogliamo, anche circoscritte (rilevare frodi, guidare mezzi di trasporto, ecc.) – l'intelligenza artificiale generativa è addestrata su *set* di dati considerevoli e multiformi e si avvale di un apprendimento non supervisionato (dove i dati non sono etichettati e al *software* IA non viene fornita alcuna guida esplicita). Va da sé che queste peculiarità di *GAI* siano destinate ad avere delle ricadute notevoli, in termini di progresso, in parecchi ambiti. A riprova di ciò è sufficiente pensare che, secondo le previsioni contenute in un recente *report* della McKinsey & Company, entro il 2025 oltre il 30% dei nuovi farmaci e dei materiali sarà scoperto grazie all'uso di tecniche di intelligenza artificiale generativa; ancora, grazie agli strumenti di IA è (e sarà) possibile comprendere gli effetti dei farmaci su grandi fasce della popolazione. Si prevede, inoltre, che nei prossimi decenni l'intelligenza artificiale soppianterà l'umano nello svolgimento di parecchie mansioni: dalla guida automobilistica alla consulenza/assistenza alle vendite, alla scrittura di testi, all'esecuzione di operazioni e interventi delicatissimi. L'IA generativa – grazie alle sue interfacce semplici e basate su *chat* – riuscirà a rispondere a tutte le esigenze e a sopperire ad ogni lacuna (ad esempio, potrà individuare la presenza di errori nella comunicazione, migliorandola, riuscirà a tradurre testi in ogni idioma, rendendo forse inutile la presenza di traduttori simultanei). Scenari, che,

© Wolters Kluwer Italia

con ogni probabilità, potrebbero tradursi in un incremento di produttività, di efficacia, di precisione, di correttezza, come pure in un più alto grado di soddisfazione da parte degli utenti/clienti [5].

ii) Il metaverso è (o meglio prova ad essere) un mondo-ambiente che consente di vivere nuove esperienze, con inedite forme di interazione e di comunicazione con sé stessi e con altri in un variegato ventaglio di mondi virtuali in 3d, interconnessi con mondi reali e popolati da *avatar* [6]. Da questo punto di vista, il metaverso, più che un'autentica novità, potrebbe ritenersi l'evoluzione sia dei *social media* sia di *Internet*. Ad esempio, con il metaverso possono essere oltrepassati i molti limiti di una comunicazione ancorata alla distanza fisica e, al contempo, ci si apre a una maggiore interazione sociale per mezzo di un'infrastruttura in grado di gestire (di archiviare, di elaborare, di trasmettere) una quantità enorme di informazioni (i c.d. *big data*), al fine di interconnettere diversi mondi (dedicati di volta in volta alla formazione, al gioco, allo *shopping*, e così via). A ben vedere, il metaverso sembra soprattutto la naturale evoluzione dell'interazione uomo-macchina, che sino ad oggi ha letto la continuità naturale-artificiale nel nome di un essere che rinvigorito e aumentato possa vivere e sopravvivere in differenti ambienti (ospitali o al contrario ostili) e con una serie variegata di innesti e/o di estensioni (*cy-fy-borg*). Dal *cyborg* al metaverso, dagli studi sul *cybernetic-organism* (anni '60 del secolo scorso) e dalla letteratura *cyberpunk* (anni '90) alle attuali tecnologie e alla nuova serie di applicazioni.

Sono fondamentalmente tre le componenti del metaverso: *a)* il contenuto, e cioè quanto viene creato, condiviso e vissuto dalle persone all'interno di questo spazio virtuale (ad esempio città, edifici, paesaggi), tramite *avatar* e identità virtuali; *b)* il *software*, ovvero l'infrastruttura, l'insieme di applicazioni, che rende possibile l'interazione tra ambienti reali e ambienti digitali, così da partecipare a eventi e attività di vario tipo (sociali, economiche, ecc.); *c)* l'*hardware*, ossia dispositivi che consentono di accedere al metaverso, quali visori (di realtà virtuale, di realtà aumentata, di realtà mista), sensori di tracciamento e di po-

[5] Ulteriori considerazioni in A.C. Amato Mangiameli, *Intelligenza artificiale generativa: brevi note*, in *L'Ircocervo*, 1/2024, pp. 101 ss.

[6] Qui è agevole il rinvio al romanzo *cyberpunk* di N. Stephenson (*Snow Crash*, London, 1992), che come noto è ambientato in una America dall'economia capitalistica fuori controllo e Hiro è un *hacker* che nella vita reale è un fattorino di una grande azienda di Los Angeles e che, al contempo, conduce un'esistenza parallela nel metaverso, ovvero nella realtà virtuale 3d quale spazio aperto e libero creato da programmatori indipendenti in cui si interagisce e ci si muove tramite i propri *avatar*.

© Wolters Kluwer Italia

sizione, dispositivi per esperienze multisensoriali, *computer* e *laptop* ad alte prestazioni, e poi ancora strumenti diversi e con caratteristiche specifiche (del tipo: lenti, guanti, scarpe, giubbotti aptici) che potenziano l'immersività e l'interazione con il virtuale. Di qui, la diversa esperienza che può essere vissuta nel metaverso, a seconda che il tentativo di essere immersi in un ambiente virtuale – che stimola i sensi (vista, udito, olfatto, tatto) e che consente una interazione con dimensioni digitali come se fossero reali – si traduca, ora, in mera visualizzazione del metaverso, ora, in prospettazione di una realtà aumentata, ed ora, ancora, in realtà virtuale. Queste due realtà sono, com'è intuitivo, particolarmente significative per le potenzialità e gli effetti prodotti.

Con l'espressione realtà aumentata si intende una realtà potenziata e incrementata grazie alle tante informazioni digitali che si ottengono ad esempio via *smartphone*, oppure tramite occhiali (con incorporati *display* e telecamera) e connessione *Internet* su oggetti o su persone. Si pensi alla visita in un museo: davanti a un monumento l'uso di un'*app* di realtà aumentata fa sì che la vista venga perfezionata da tutte quelle ulteriori notizie che certamente saranno utili per la conoscenza di quell'opera d'arte e per la sua stessa valutazione. Si pensi, ancora, alle nuove forme di esperienze teatrali: per alcune di queste si parla di *enhanced theatre*, in cui la scena è aumentata, caleidoscopica, di immagini frammentate e proiettate su più schermi, di comunicazioni ramificate e interattive, di attori sintetici che recitano insieme ai loro doppi in carne e ossa, di un pubblico che è sollecitato dalla compresenza di più punti di vista e sensorialmente coinvolto. La realtà aumentata mescola, comunque, il mondo fisico con quello digitale.

Con l'espressione realtà virtuale, invece, si rinvia ad una realtà sostanzialmente parallela, nella quale sono coinvolti alcuni sensi (in particolare la vista e l'udito) e, in taluni casi, persino gli altri. In quest'ultimo caso, la realtà virtuale è di tipo (totalmente) immersivo. Il tutto è diventato via via possibile grazie al combinarsi e allo sviluppo, di *software* per creare ambienti 3d e di algoritmi di IA, come pure di tecnologie *wireless*, di componenti minutissimi e di servizi in *cloud*. Nella realtà virtuale, che è tutta digitale, si accede attraverso visori con *display* ad altissima definizione, attraverso sensori (accelerometri e giroscopi) che rilevano i diversi movimenti della testa o che migliorano le simulazioni (ad esempio, di una corsa, pur restando fermi nella realtà) e la percezione tattile degli oggetti, come se si tenesse in mano l'oggetto reale. Grazie a visori, guanti, tute, dispositivi d'ogni genere, si accentua l'interazione tra realtà fisica e realtà virtuale, che costituisce il tratto essenziale proprio del metaverso, non riducibile né al *Blockchain*, né al *Not Fungible Token*. Nel metaverso è già possibile godersi

© Wolters Kluwer Italia

un concerto immersi in un teatro virtuale, svolgere attività professionali in uffici virtuali, accedere con il proprio *avatar* a eventi sportivi, e ancora tanto altro a secondo delle piattaforme usate (ad esempio: *Horizon Worlds*, *Mesh*, *Omniverse, Sandbox, Decentraland, Gala, Celebrity Atlas, Blocktopia*) che le aziende (ad esempio: *Meta, Microsoft, Epic, Roblox, Vive*) mettono a disposizione.

Com'è intuitivo, il metaverso suscita un notevole interesse per la ricerca medica e per il trattamento di alcune patologie. L'uso delle nuove tecnologie, in particolare di quei diversi strumenti d'accesso alla realtà virtuale, in combinazione con altre terapie, nel caso di riabilitazione (di tipo motoria, cognitiva, ecc.) è certo visto con favore perché idoneo a promuovere l'attività fisica e quella cognitiva anche in soggetti affetti da grave disabilità, non solo riuscendo a ridurre gli ostacoli fisici e sociali, ma anche consentendo l'accesso a nuove modalità e pratiche riabilitative in ambienti controllati e sicuri. Basterebbe qui pensare all'efficacia che potrebbero avere, con riferimento ad alcune patologie, sia la rappresentazione virtuale della persona, ovvero l'*avatar*, *alter ego* digitale la cui forma più diffusa è quella in 3d, di tipo umanoide e molto realistica, e sia il teletrasporto virtuale, ossia il *virtual teleportation*, che consente di portare una persona nel metaverso tramite una riproduzione decisamente realistica.

3. Nuove dimensioni ancora da regolare

Le menti e i corpi fusi con IA introducono un nuovo paradigma, allontanandosi per un verso dalla domanda: *possono pensare le macchine?* e per l'altro superando l'argomento su somiglianze/differenze uomo/macchina [7]. Del resto, se già intorno alla metà del secolo scorso si sottolineava l'incongruenza di pretese differenze, ciò vale a maggior ragione nell'ipotesi dell'IA generativa che con la sua forte capacità di autoapprendimento certo travalica l'idea che a differenziare la macchina dall'uomo è l'automatismo della prima e la coscienza di sé del secondo, non fosse altro perché c'è una continua interazione tra attività umana, dispositivi e piattaforme (esemplare è il c.d. *Internet of Things – IoT*) e inoltre i risultati proposti dall'IA generativa spesso colgono

[7] Come già proposto da Turing nel suo Test dell'imitazione, giocato fra la macchina a stati discreti (nella parte di B – uomo), il calcolatore digitale (nella parte di A – donna) e C (l'interrogante) che non sarebbe capace di distinguerli (v. A. Turing, *Macchine calcolatrici e intelligenza*, in A. Turing, *Intelligenza meccanica*, Torino, 1994, pp. 122 ss.).

© Wolters Kluwer Italia

impreparati persino i suoi stessi programmatori. Forse le resta precluso il *senso* delle sue stesse decisioni e operazioni, quel che tuttavia è chiaro è che gli odierni dispositivi e gli attuali applicativi sono dotati di comprensione semantica, e che i diversi *chatbot*, se interrogati, contestualizzano perfettamente il discorso e aggirano le varie difficoltà lungo il percorso. In ogni caso, i sistemi di IA hanno ormai un'influenza altissima sulle preferenze e sulle scelte umane, che ne risultano indiscutibilmente orientate [8].

Le menti e i corpi fusi con IA sono (e appartengono a) individui (in carne e ossa) che vivono utilizzando i sistemi di IA e che abitano anche realtà parallele e/o il metaverso, sfruttando le numerose potenzialità che i sistemi e le realtà (aumentata e virtuale) offrono, ma anche correndo i rischi che tanto i primi quanto le seconde introducono. Le potenzialità sono veramente tante, altrettanto sono i rischi: tra *fake news*, *bias cognitivi*, *allucinazioni* – le cui cause sono diverse, ma tutte fondamentalmente legate al modello di apprendimento dell'IA che può essere ora mancante di dati rappresentativi e ora così ricco di dati da interpretarli erroneamente – diventa sempre più necessario validare le informazioni e le risposte ricevute dall'IA tramite il confronto con quelle di altri modelli o di esperti umani. In particolare, perché vengano ridotti in maniera significativa i possibili rischi, bisogna che: *i)* siano implementati i meccanismi di controllo e di regolazione dell'*output* dell'IA, *ii)* siano usate architetture di rete neurali semplici e interpretabili, *iii)* siano introdotti metodi di addestramento basati sulla coerenza dell'*output*. Le problematiche qui accennate richiamano, anche a fini di contrasto rispetto ai rischi, la necessità di regolare le diverse dimensioni sotto il profilo normativo.

Il recente *AI Act* [9], dopo alcune prime definizioni (ad esempio: sistema di IA, rischio, fornitore, *deployer*, uso improprio ragionevolmente prevedibile, dati di addestramento) e una prima imposizione in capo a fornitori e *deployer* dei sistemi di IA (art. 4: alfabetizzazione in materia di IA), vieta quelle pratiche che violano l'autonomia e la *privacy* degli individui (art. 5: tecniche subliminali, manipolative o ingannevoli, come pure le tecniche di valutazione del rischio criminale basate su

---

[8] Cfr. A.C. AMATO MANGIAMELI, *Tecno-diritto/regolazione*, in A.C. AMATO MANGIAMELI - G. SARACENI, *Cento e una voce di informatica giuridica*, Torino, 2023, pp. 469-475.

[9] Regolamento UE 2024/1689 sull'intelligenza artificiale, adottato dal Parlamento e dal Consiglio dell'Unione europea per regolare le opportunità che le nuove tecnologie, e innanzitutto l'IA, offrono e per rispondere alle sfide che queste pongono agli individui e alle comunità.

© Wolters Kluwer Italia

profilazione e l'identificazione biometrica, salvo che queste due ultime siano richieste da specifiche circostanze e da motivi di sicurezza). Per il nostro tema, è particolarmente significativo l'art. 14. Qui, infatti, nel prospettare i sistemi di IA ad alto rischio è richiesto che questi siano progettati e sviluppati con strumenti di interfaccia uomo-macchina in grado di potere essere efficacemente supervisionati dalle persone durante il periodo in cui sono in uso (p. 1). Questo al fine di ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali, sia in caso di uso previsto e sia in quello di uso improprio ragionevolmente prevedibile (p. 2). Inoltre, le misure di sorveglianza – individuate e integrate dai fornitori, e adatte ad essere attuate dai distributori – devono essere commisurate ai rischi, al livello di autonomia e al contesto di utilizzo del sistema di IA (p. 3). Perché ciò si realizzi è necessario che le persone alle quali è affidata la sorveglianza abbiano la capacità: *a)* di monitorare il funzionamento del sistema, individuando e affrontando anomalie, disfunzioni e prestazioni inattese; *b)* di evitare la c.d. distorsione dell'automazione, e cioè l'eccessivo affidamento sull'*output* prodotto dal sistema di IA; *c)* di interpretare correttamente l'*output*, *d)* di decidere in situazioni particolari di non usare il sistema, come pure *e)* di intervenire sul funzionamento, interrompendo il sistema stesso in condizioni di sicurezza.

Al di là di questo e di altri articoli (dedicati ai modelli di IA per finalità generali: artt. 51 ss.) che direttamente o indirettamente la riguardano, l'IA generativa non è pienamente affrontata nel regolamento, in ogni caso permangono diversi dubbi su interpretazione e valutazione dei sistemi di IA e d'altra parte c'è la necessità di approfondire le questioni quali: protezione dei dati personali, diritti della proprietà intellettuale, divario digitale, sostenibilità. Per il nostro tema (menti-corpi fusi con IA), poi, l'*AI Act* è certo utile per individuare competenze, limiti, divieti, resta il fatto che esso non si applica alle attività di ricerca (anche se "*le prove in condizioni reali non rientrano in tale esclusione*": art. 2, p. 8) e che, nei momenti di grande trasformazione e oltre il mercato, sono pur sempre i criteri e gli obiettivi del diritto (eguaglianza, responsabilità, *neminem laedere*, ragionevolezza, proporzionalità, terzietà) a costituire la cornice entro la quale collocare ogni discorso sul soggetto, anche quando è già mente-corpo fuso con IA.

© Wolters Kluwer Italia

VERSO L'INDIVIDUAZIONE DI UNA "VIA EUROPEA" ALLO SVILUPPO TECNOLOGICO. ALCUNE RIFLESSIONI SUL REGOLAMENTO (UE) 2024/1689 CHE STABILISCE NORME ARMONIZZATE SULL'INTELLIGENZA ARTIFICIALE *

PIERLUIGI SIMONE

SOMMARIO: 1. Introduzione. La "lunga marcia" per assicurare un quadro etico e giuridico adeguato all'intelligenza artificiale. – 2. I contenuti principali del regolamento (UE) 2024/1689. – 3. Intelligenza artificiale, rispetto dei diritti fondamentali e protezione dei dati personali. – 4. Il regolamento (UE) 2024/1689 come mezzo per migliorare il funzionamento del mercato interno. – 5. Rilievi sulla conformazione della *governance* e sull'attività di vigilanza nazionale. – 6. I sistemi di intelligenza artificiale tra efficienza competitiva e promozione di diritti, libertà e valori. Conclusioni.

Abstract: Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act) tries to balance two different elements: innovative experimentation and economic growth to spread AI in the internal market and to compete with other international players; protection of rights, freedoms and values which underpin the European integration process. In achieving this goal, the AI Act is a combination of light and shadow. The risk-based approach and the resulting rigid classification of AI systems may be inadequate to deal with algorithmic discrimination and not resilient enough to keep up with the later developments in AI. The success of Regulation (EU) 2024/1689 will have to be tested in practice, and will depend on the qualities of those empowered to apply and enforce it.

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

1. Introduzione. La "lunga marcia" per assicurare un quadro etico e giuridico adeguato all'intelligenza artificiale

Nel panorama della rivoluzione digitale tipica di queste prime decadi del XXI secolo, l'intelligenza artificiale (IA) è un fattore di progresso indubbiamente affascinante, tale però da incutere al tempo stesso un diffuso timore. Teorizzata fin dal 1956, quando l'informatico statunitense John McCarthy (una delle figure di spicco del nascente settore della computazione dedicata alla crescita di *smart system*) ne coniò l'espressione nel corso di un convegno tenuto al Dartmouth College di Hanover (New Hampshire), conferendole così una fisionomia propria, essa corrisponde, nel suo significato più ampio, alla capacità di un sistema informatico di simulare e riprodurre l'intelligenza umana attraverso l'ottimizzazione di funzioni matematiche [1].

L'IA, in altre parole, è un insieme di tecnologie che consente di generare, classificare ed eseguire prestazioni avanzate (vista, apprendimento, comprensione e traduzione del linguaggio scritto e parlato, ragionamento, autocorrezione, analisi dei dati, suggerimento, e altro) ritenute finora, nell'ottica dell'osservatore comune, di esclusiva pertinenza della mente dell'uomo [2].

L'intelligenza artificiale può procurare una vasta gamma di benefici a tutto lo spettro delle attività sociali e industriali. Il suo uso consono garantisce il miglioramento delle previsioni, il perfezionamento delle operazioni e dell'assegnazione delle risorse, e la personalizzazione dell'erogazione dei servizi: è dunque in grado di fare ottenere risultati certamente favorevoli per la collettività, nonché agevolazioni competitive essenziali per le imprese e per l'economia, con ripercussioni

---

[1] Cfr. D. CREVIER, *AI: The Tumultuous Search for Artificial Intelligence*, New York, 1993; R. CORDESCHI, *L'intelligenza artificiale*, in L. GEYMONAT (a cura di), *Storia del pensiero filosofico e scientifico. Il Novecento*, vol. VIII, Milano, 1996, pp. 145 ss.; M. SOMALVICO - F. AMIGONI - V. SCHIAFFONATI, *Intelligenza artificiale*, in S. PETRUCCIOLI (a cura di), *Storia della scienza*, vol. IX, Roma, 2003, pp. 615 ss.; P. MCCORDUCK, *Machines who Think*, II ed., Natick, Massachusetts, 2004; J. KAPLAN, *Generative Artificial Intelligence: What Everyone Needs to Know*, Oxford, 2016; K. CRAWFORD, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, New Haven, Connecticut, 2021; M.E. KLONTZAS - S.C. FANNI - E. NERI (eds.), *Introduction to Artificial Intelligence*, Cham, 2023.

[2] Si tratta, cioè, non solo di intelligenza intesa come capacità di calcolo o di conoscenza di dati astratti, ma anche e soprattutto di tutte quelle differenti forme di intelligenza che sono riconosciute dalla c.d. teoria di Gardner, e che vanno dall'intelligenza spaziale a quella sociale, dall'intelligenza cinestetica a quella introspettiva. Per un quadro analitico degli studi di settore, v. A.C. AMATO MANGIAMELI, *Informatica giuridica*, Torino, 2015.

© Wolters Kluwer Italia

importanti sulla medicina, sul mercato azionario, sulla robotica, sul diritto, sull'istruzione, sulla ricerca scientifica [3]. Altrettanto manifesti, peraltro, sono i rischi e i contraccolpi negativi, per le persone fisiche o per la società, virtualmente insiti nell'impiego stesso dell'IA e nelle tecniche che la alimentano: si pensi ai meccanismi decisionali opachi dettati dalle asimmetrie informative del processo algoritmico, alle discriminazioni di genere o di diversa natura, alle intromissioni nella vita privata, alla potenziale destinabilità a scopi criminali o dolosi [4].

L'Unione europea ha sempre mostrato di essere perfettamente consapevole di questi benefici e di questi rischi.

L'attenzione iniziale dell'Unione al fenomeno in esame risale a poco meno di un decennio fa [5]. Già nelle comunicazioni su "*Digitalizzazione dell'industria europea. Cogliere appieno i vantaggi di un mercato unico digitale*" del 19 aprile 2016 e su "*Investire in un'industria intelligente, innovativa e sostenibile. Una nuova strategia di politica industriale dell'UE*" del 13 settembre 2017, la Commissione aveva riconosciuto all'IA e a una serie di tecnologie (l'IoT, i *big data*, il *cloud computing*, la stampa 3D) l'attitudine a stimolare opportunamente i metodi di lavorazione in modo da poter rispondere meglio alle aspettative dei consumatori in termini di sicurezza, comodità ed efficienza energetica [6].

---

[3] Si pensi in proposito a vari settori ad alto impatto: quelli, tra gli altri, dei cambiamenti climatici e dell'ambiente in generale, della sanità, della pubblica amministrazione, della finanza, della mobilità, degli affari interni, dell'agricoltura.

[4] L'elencazione nel testo è, ovviamente, tutt'altro che esaustiva. Le conseguenze deleterie, a ben vedere, possono essere sia materiali (quando incidono sulla salute e sulla sicurezza delle persone, provocando perdite di vite umane o danni patrimoniali), sia immateriali (quando causano una perdita della riservatezza, restrizioni alla libertà di espressione, pregiudizi alla dignità umana o discriminazioni, ad esempio nell'accesso all'occupazione). Sulle opacità del processo algoritmico, cfr. A.C. Amato Mangiameli, *Tecno-regolazione e diritto. Brevi note su limiti e differenze*, in *Dir. inform*., 2/2017, pp. 147 ss.

[5] Ne ripercorrono cronologicamente i passaggi G. Contaldi, *La proposta di regolamento sull'intelligenza artificiale e la protezione dei dati personali*, in G. Caggiano - G. Contaldi - P. Manzini (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021, pp. 208 ss.; e N.T. Nikolinakos, *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies – The AI Act*, Cham, 2023, pp. 23 ss.

[6] Punti 2 e 4.2.2. della comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni su "*Digitalizzazione dell'industria europea. Cogliere appieno i vantaggi di un mercato unico digitale*", doc. COM(2016)180 def. del 19 aprile 2016, pp. 4 s. e 12; punto 1 della comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo, al Comitato delle Regioni e

© Wolters Kluwer Italia

Dopo che il Parlamento europeo ebbe approvato, il 16 febbraio 2017, il Rapporto Delvaux, nel tentativo di rintracciare i princìpi giuridici, etici e deontologici riguardanti i sistemi cibernetici, i sistemi autonomi, i robot autonomi intelligenti e le loro sottocategorie [7], le comunicazioni su "*L'intelligenza artificiale per l'Europa*" del 25 aprile 2018 e sul "*Piano coordinato sull'intelligenza artificiale*" del 7 dicembre 2018, avevano preparato il terreno per l'adeguato sfruttamento dell'IA, lanciando, di concerto con gli Stati membri, una iniziativa volta sia a dare impulso alla infrastruttura tecnologica e industriale dell'Unione e all'adozione dell'IA in tutti i settori economici; sia a preparare la società e l'economia ai mutamenti dovuti all'IA [8].

Il Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia del 19 febbraio 2020, aveva poi illustrato le opzioni strategiche per uno sviluppo affidabile dell'IA, i cui principali elementi costitutivi erano ravvisati nelle misure per allineare gli sforzi a livello europeo, nazionale e regionale affinché, tramite un partenariato pubblico-privato, si mobilitassero risorse "*(...) per conseguire un «ecosistema di eccellenza» lungo l'intera catena del valore [...] e creare i giusti incentivi per accelerare l'adozione di soluzioni basate sull'IA, anche da parte delle piccole e medie imprese (PMI)*"; e nella creazione di un "ecosistema di fiducia" unico che avrebbe dovuto dare ai cittadini, per l'appunto, "*(...) la fiducia di adottare applicazioni di IA e alle imprese e alle organizzazioni pubbliche la certezza del diritto necessaria per innovare utilizzando l'IA*" [9].

I documenti appena passati in rassegna insistono con chiarezza su due concetti inscindibili: l'interesse, innanzitutto, a preservare la *lea-*

---

alla Banca europea degli investimenti su "*Investire in un'industria intelligente, innovativa e sostenibile. Una nuova strategia di politica industriale dell'UE*", doc. COM(2017)479 def. del 13 settembre 2017, p. 2.

[7] V. la risoluzione del Parlamento europeo del 16 febbraio 2017 recante *raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, doc. P8_TA(2017)0051. La scarsa originalità del Rapporto Delvaux è messa in evidenza da A. ZORNOZA - M. LAUKYTE, *Robotica e diritto: riflessioni critiche sull'ultima iniziativa di regolamentazione in Europa*, in *Contr. impr. Eur.*, 2/2016, pp. 811 ss., e da G. CONTALDI, *Op. cit*., pp. 208 s.

[8] Punti 1, 3 e 3.2. della comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni su "*L'intelligenza artificiale per l'Europa*", doc. COM(2018)237 def. del 25 aprile 2018, pp. 3, 6 ss. e 12 ss.; punto 2 della comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni sul "*Piano coordinato sull'intelligenza artificiale*", doc. COM(2018)795 def. del 7 dicembre 2018, pp. 2 ss.

[9] Punto 1 del Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia, doc. COM(2020)65 def. del 19 febbraio 2020, p. 3.

© Wolters Kluwer Italia

dership tecnologica dell'Unione europea, a farne un polo attrattivo e dinamico di caratura mondiale nella elaborazione di una IA sicura per la quale l'Unione medesima, utente e produttrice, solleciti gli investimenti a ciò opportuni; la necessità, in secondo luogo, di assicurare che i cittadini europei possano godere dell'intelligenza artificiale in conformità ai valori definiti dall'art. 2 TUE, alla Carta dei diritti fondamentali dell'Unione europea e ai princìpi generali del diritto dell'Unione. Entrambi gli obiettivi hanno motivato in seguito la proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, presentata dalla Commissione il 21 aprile 2021 [10].

Tenendo fede all'impegno di Ursula von der Leyen, annunciato negli orientamenti politici per la Commissione 2019-2024 "*A Union that Strives for More. My Agenda for Europe*", di voler giungere, nell'immediato futuro, "(...) [to] put forward legislation for a coordinated European approach on the human and ethical implications of Artificial Intelligence" [11], e rispondendo altresì a richieste esplicite del Consiglio europeo e del Parlamento europeo, la proposta del 2021 si è mossa su quattro fronti: fare sì che i sistemi di IA immessi sul mercato dell'Unione e utilizzati "*(...) siano sicuri e rispettino la normativa vigente in materia di diritti fondamentali e i valori dell'Unione*"; assicurare la certezza del diritto "*(...) per facilitare gli investimenti e l'innovazione nell'intelligenza artificiale*"; migliorare la *governance* e l'applicazione effettiva della normativa esistente "*(...) in materia di diritti fondamentali e requisiti di sicurezza applicabili ai sistemi di IA*"; facilitare l'espansione "*(...) di un mercato unico per applicazioni di IA lecite, sicure e affidabili nonché prevenire la frammentazione del mercato*" [12].

---

[10] 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, doc. COM(2021)206 def. del 21 aprile 2021.

[11] European Commission, *A Union that Strives for More. My Agenda for Europe*, *Political Guidelines for the Next European Commission 2019-2024*, Brussels, 2019, p. 13.

[12] Così il punto 1.1. della proposta di regolamento del 2021, cit., p. 3. V. altresì il punto 4 della coeva comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni su "*Promuovere un approccio europeo all'intelligenza artificiale*", doc. COM(2021)205 def. del 21 aprile 2021, pp. 6 ss., nonché A. Simoncini, *La proposta di regolazione europea dell'intelligenza artificiale. Prime riflessioni*, 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, pp. 5 ss.

© Wolters Kluwer Italia

Da tale proposta è scaturito il provvedimento i cui aspetti di maggiore richiamo si è in procinto di approfondire: il regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce norme 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) [13].

2. I contenuti principali del regolamento (UE) 2024/1689

Il regolamento (UE) 2024/1689 è assai corposo (comprende ben 180 "considerando", 113 articoli e 13 allegati) ed è stato approvato sulla base di un accordo provvisorio raggiunto il 9 dicembre 2023 in esito ai negoziati interistituzionali tra i rappresentanti del Parlamento europeo, del Consiglio e della Commissione (c.d. triloghi) per concordare il testo da sottoporre ai colegislatori. È entrato in vigore il 1° agosto 2024 ed è destinato a essere eseguito dal 2 agosto 2026, con scadenze differite (tra il 2 febbraio 2025 e il 2 agosto 2027) per i Capi I-III, V, VII e XII [14].

Il fine dichiarato è quello di migliorare il funzionamento del mercato interno e di promuovere la diffusione di una intelligenza artificiale 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, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente (...)*", contro gli effetti nocivi dei sistemi di IA nell'Unione [15]. Al riguardo, con un metodo che può essere definito "orizzontale", vengono fissate regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA nell'Unione; regole di trasparenza armonizzate per determinati sistemi di IA; regole armonizzate per l'immissione sul mercato di modelli di IA per finalità generali [16]. Il "sistema di IA", diversamente dalla proposta del 2021, è declinato all'art. 3, n. 1, come "*un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità do-*

[13] In G.U.U.E. L/2024/1689 del 12 luglio 2024, pp. 1 ss.
[14] Art. 113 del regolamento (UE) 2024/1689.
[15] Art. 1, par. 1, del regolamento (UE) 2024/1689.
[16] Art. 1, par. 2, lett. a), d) ed e), del regolamento (UE) 2024/1689.

© Wolters Kluwer Italia

*po 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*" [17]. Sono invece "modelli di IA per finalità generali" i modelli di IA, integrabili "*(...) in una varietà di sistemi o applicazioni a valle (...)*", caratterizzati da una generalità significativa e dalla idoneità a svolgere con competenza molti compiti distinti, indipendentemente dalle modalità con cui sono immessi sul mercato [18].

A termini dell'art. 2, par. 1, il regolamento in questione, fondato sugli art. 16 e 114 TFUE, si applica a soggetti pubblici o privati (persone fisiche o giuridiche, autorità pubbliche, agenzie o altri organismi) quali i fornitori e i *deployer* dei sistemi di IA stabiliti o ubicati nell'Unione o in uno Stato terzo, laddove immettano sul mercato o mettano in servizio detti sistemi o modelli di IA nell'Unione ovvero l'*output* prodotto dal sistema sia utilizzato nell'Unione; gli importatori e i distributori di sistemi di IA; i fabbricanti di prodotti che immettano sul mercato o mettano in servizio un sistema di IA insieme al loro prodotto, con il loro nome o marchio; i rappresentanti autorizzati di fornitori, non stabiliti nell'Unione; le persone interessate che si trovino nell'Unione [19].

Gli oneri a cui sono sottoposti i fornitori, i *deployer*, gli importatori, i distributori, i fabbricanti di prodotti e i rappresentanti autorizzati (associabili tutti alla denominazione omnicomprensiva di "operatore"), vengono graduati sulla scorta del rischio ("inaccettabile", "alto", "basso" o "minimo") che l'intelligenza artificiale può generare. Il danno, pertanto, non discende da un difetto di progettazione o di realizzazione del sistema di IA, perché è l'operatore ("oggettivamente" responsabile, si potrebbe dire) a dover dimostrare di aver adempiuto tutte le prescrizioni. Il regolamento (UE) 2024/1689, in particolare, prevede al Capo

---

[17] La descrizione inserita dalla Commissione nella proposta del 2021 è stata infatti modificata, allineandola alla visione dell'Organizzazione per la cooperazione e lo sviluppo economici (OCSE), in modo da includervi i modelli innovativi (fondativi o di base) risultato degli sviluppi tecnologici più recenti. Cfr. M. Carta, *Il regolamento UE sull'intelligenza artificiale: alcune questioni aperte*, in *Eurojus*, 3/2024, p. 200.

[18] V. l'art. 3, n. 63, del regolamento (UE) 2024/1689.

[19] Nessun pregiudizio è arrecato alle competenze degli Stati membri in materia di sicurezza nazionale, né alle attività di ricerca e sviluppo scientifici o di prototipazione precedente l'immissione sul mercato o la messa in servizio, né ancora ai *deployer* persone fisiche che impieghino l'IA per motivi non professionali: cfr. l'art. 2, par. 3, 6, 8 e 10, del regolamento (UE) 2024/1689. Per le nozioni di "fornitore", "*deployer*", "rappresentante autorizzato", "importatore", "distributore", "immissione sul mercato" e "messa in servizio" si rinvia all'art. 3, nn. 3-7, 9 e 11, dello stesso atto.

© Wolters Kluwer Italia

II (art. 5) la proibizione di talune pratiche di IA, nonché al Capo III (art. 6-49) requisiti specifici per i sistemi di IA ad alto rischio e obblighi per gli operatori di tali sistemi [20].

In estrema sintesi, le relative disposizioni possono essere riassunte, complessivamente, come segue.

L'art. 5 vieta le pratiche di IA deliberatamente manipolative, ingannevoli o distorsive che sfruttano le vulnerabilità delle persone, o di gruppi di persone, e impiegano tecniche subliminali [21]. La norma interdice poi i sistemi di IA che consentono di attribuire una sorta di "punteggio sociale" mediante classificazione o valutazione degli individui sulla base del comportamento sociale o di caratteristiche personali o della personalità "*(...) note, inferite o previste (...)*"; l'estrazione non mirata di immagini facciali da *Internet* o da filmati di telecamere a circuito chiuso per la creazione o l'ampliamento di banche dati; nonché i sistemi di riconoscimento delle emozioni delle persone fisiche sul luogo di lavoro e negli istituti di istruzione, quando non vi siano giustificazioni mediche o di sicurezza [22]. Fatte salve appropriate eccezioni, non sono ammesse le applicazioni di polizia predittiva circa il pericolo che una persona commetta un reato. Sono inoltre preclusi, sempre con eccezioni, i sistemi di categorizzazione biometrica per trarre deduzioni o congetture, rispetto alle persone fisiche, in merito a "*(...) razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita [...] o orientamento sessuale*"; e i sistemi di identificazione biometrica "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto [23].

Per i sistemi di IA ad alto rischio (definiti dall'art. 6, par. 1, ed elencati nell'All. III, modificabile dalla Commissione con atti delegati da adottare *ex* art. 7 e 97), idonei come tali ad avere conseguenze negative sulla salute, sulla sicurezza o sui diritti delle persone, occorre che i fornitori ne dimostrino la conformità ai requisiti di affidabilità (inerenti alla qualità dei dati, alla documentazione e tracciabilità, alla trasparenza, alla sorveglianza umana, all'accuratezza, robustezza e ci-

---

[20] Art. 1, par. 2, lett. b) e c), del regolamento (UE) 2024/1689.

[21] Art. 5, par. 1, lett. a) e b), del regolamento (UE) 2024/1689.

[22] Art. 5, par. 1, lett. c), e) e f), del regolamento (UE) 2024/1689.

[23] Art. 5, par. 1, lett. d), g) e h), del regolamento (UE) 2024/1689. Per degli accenni ai sistemi di IA a rischio inaccettabile v. G. CONTALDI, *Op. cit*., p. 214; G. FINOCCHIARO, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir. inform*., 2/2022, pp. 311 ss.; A. SIMONCINI, *Op. cit*., pp. 8 s. e 19 s.; N.T. NIKOLINAKOS, *Op. cit*., pp. 374 ss.

© Wolters Kluwer Italia

bersicurezza) riportati nel dettaglio dagli art. 10-15 [24]. Costoro, a tutela degli utenti, realizzano un sistema di gestione del rischio, ossia un processo ripetitivo continuo, pianificato ed eseguito nel corso dell'intera vita di un sistema ad alto rischio, con un riesame e un aggiornamento costanti e precisi [25]. Istituiscono altresì un sistema di gestione della qualità documentato in modo scrupoloso e ordinato "*(...) sotto forma di politiche, procedure e istruzioni scritte (...)*", comprensivo almeno degli aspetti enumerati nell'art. 17, par. 1 [26]. Ai *deployer*, anche qualora siano organismi di diritto pubblico o enti privati fornitori di pubblici servizi, si richiede, anteriormente al primo uso dei sistemi, l'avvenuta effettuazione di una valutazione di impatto sui diritti fondamentali [27]. Per garantire il rispetto dei parametri richiesti, occorre seguire una procedura di certificazione che sfocia nella redazione, a cura del fornitore, di una dichiarazione di conformità UE (art. 47) e nell'apposizione, a cura del fabbricante o del suo mandatario, sul sistema di IA ovvero sull'imballaggio o sui documenti di accompagnamento, della marcatura CE "*(...) visibile, leggibile e indelebile*", se del caso anche digitale (art. 48) [28]. La Commissione, in collaborazione con gli Stati membri, crea e mantiene, ai sensi dell'art. 71, una banca dati dell'UE nella quale i fornitori, i rappresentanti autorizzati e i *deployer* (autorità pubbliche, istituzioni, organi e organismi dell'Unione o persone che agiscono per loro conto) si registrano e, prima di immetterli sul mercato, di metterli in servizio o di utilizzarli, registrano e/o selezionano i propri rispettivi sistemi ad alto rischio [29].

---

[24] V. l'art. 43 del regolamento (UE) 2024/1689.

[25] V. l'art. 9 del regolamento (UE) 2024/1689.

[26] L'attuazione degli aspetti di cui al par. 1 è proporzionata alle dimensioni dell'organizzazione del singolo fornitore, il quale rispetta, in ogni caso, il grado di rigore e di protezione necessari per garantire la conformità del suo sistema di IA ad alto rischio al diritto dell'Unione. Se i fornitori sono istituti finanziari soggetti a requisiti in materia di *governance*, dispositivi o processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, l'obbligo di istituire un sistema di gestione della qualità si considera soddisfatto se sono adempiute le regole sui dispositivi o i processi di *governance* interna ai sensi del suddetto pertinente diritto dell'Unione.

[27] Cfr. l'art. 27 del regolamento (UE) 2024/1689.

[28] La marcatura CE è soggetta ai princìpi generali di cui all'art. 30 del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti.

[29] Art. 49, par. 1-3, del regolamento (UE) 2024/1689. Il par. 4 aggiunge che "*(...) nei settori delle attività di contrasto, della migrazione, dell'asilo e della gestione del controllo delle frontiere, la registrazione [...] si trova in una sezione sicura non pubblica della banca dati dell'UE di cui all'articolo 71 (...)*". Sulla categoria dei sistemi di

© Wolters Kluwer Italia

Sono sistemi di IA a rischio basso o minimo, invece, i prodotti, non inclusi nelle due precedenti categorie, destinati a relazionarsi direttamente con le persone fisiche [30]. In proposito, viene incoraggiata e agevolata l'elaborazione di codici di condotta volontari [31]. Vigono inoltre requisiti minimi di trasparenza sostanziati in precisi obblighi di comunicazione in quanto, al momento del primo contatto o della prima esposizione, i fornitori e i *deployer* devono avere informato i fruitori del fatto di stare interagendo con un sistema di IA (a meno che non sia evidente dalle circostanze e dal contesto di utilizzo) e di essere dinanzi a immagini o a contenuti audio o video (seppur fortemente somiglianti a persone, oggetti, luoghi o eventi reali e veritieri) generati o manipolati artificialmente da un sistema simile [32].

Completano l'assetto normativo le regole sul monitoraggio del mercato, la vigilanza del mercato, la *governance*, l'esecuzione; e le misure a sostegno dell'innovazione, con riguardo alle piccole e medie imprese (PMI), incluse le *start-up* [33].

3. Intelligenza artificiale, rispetto dei diritti fondamentali e protezione dei dati personali

Dalla sommaria disamina appena ultimata si evince che il regolamento sull'intelligenza artificiale, al pari della proposta del 2021, riprende la medesima logica sottesa alla disciplina della responsabilità per prodotti difettosi, ma, a differenza di quella, risponde altresì al paradigma prioritario di tutela dei diritti fondamentali (nelle fasi di progettazione, di addestramento e di controllo sul funzionamento del *software*), e di salvaguardia del processo democratico, secondo i dettami dei Trattati istitutivi, della Carta dei diritti fondamentali dell'Unione europea e della Convenzione europea dei diritti dell'uomo (CEDU) [34].

IA ad alto rischio cfr. G. CONTALDI, *Op. cit*., pp. 214 ss.; G. FINOCCHIARO, *Op. cit*., pp. 313 ss.; A. SIMONCINI, *Op. cit*., pp. 8 s.; N.T. NIKOLINAKOS, *Op. cit*., pp. 412 ss.

[30] Art. 6, par. 3, 1° e 2° co., e 4, del regolamento (UE) 2024/1689.

[31] Art. 95 del regolamento (UE) 2024/1689.

[32] V. l'art. 50, par. 1, 2 e 4, del regolamento (UE) 2024/1689, nonché G. CONTALDI, *Op. cit*., p. 216; G. FINOCCHIARO, *Op. cit*., p. 320; A. SIMONCINI, *Op. cit*., pp. 8 e 10; N.T. NIKOLINAKOS, *Op. cit*., pp. 591 ss.

[33] Art. 1, par. 2, lett. f) e g), del regolamento (UE) 2024/1689.

[34] D. BOMHARD - M. MERKLE, *Regulation on Artificial Intelligence. The EU Commission's Proposal of an AI Act*, in *J. Eur. CML*, 6/2021, pp. 257 ss.; L. FLORIDI, *The European Legislation on AI: A Brief Analysis of its Philosophical Approach*, in *Phil. Tecn*., 34/2021, pp. 215 ss.; G. RESTA, *Cosa c'è di "europeo" nella proposta di regolamento UE sull'intelligenza artificiale?*, in *Dir. inform*., 2/2022, p. 327.

© Wolters Kluwer Italia

L'IA, in teoria, è idonea a favorire il rispetto di alcuni diritti: lo ha messo bene in luce la Commissione nella relazione su "*Tutela dei diritti fondamentali nell'era digitale – Relazione annuale 2021 sull'applicazione della Carta dei diritti fondamentali dell'Unione europea*" del 10 dicembre 2021, laddove non si è mancato di sottolineare importanti effetti positivi per la libertà di espressione e di informazione, per l'assistenza sanitaria e per aspetti di interesse generale, quali la sicurezza o la sanità pubbliche [35].

Le applicazioni di intelligenza artificiale, fortemente favorite da ragioni economiche, se utilizzate senza controlli di qualità adeguati per automatizzare o sostenere i processi decisionali possono tuttavia incidere anche negativamente sui diritti delle persone. Certe loro caratteristiche (scarsa trasparenza, complessità, dipendenza dai dati, comportamento autonomo) rendono complicato prevenire, rilevare e dimostrare eventuali violazioni (talvolta propagate su larga scala), impedendo di risalire a errori o a malfunzionamenti del sistema [36]. A fronte della assoluta genericità dell'art. 1, par. 1, del regolamento (UE) 2024/1689 di cui si è detto [nel quale si parla della protezione "*(...) della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea (...)*"], riflesso della difficoltà (o forse della poca volontà?) di essere precisi, è sempre la relazione del 2021 a fornire degli esempi puntuali. Così, l'IA usata per ricavare informazioni sulle persone può incidere sulla protezione dei dati e sulla vita privata, mentre le distorsioni negli algoritmi o nei dati di addestramento possono portare (provocandole o aumentandole) a discriminazioni di genere, etniche o razziali [37]. Può sorgere un contrasto con i di-

---

[35] Cfr. il punto 5 della relazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni su "*Tutela dei diritti fondamentali nell'era digitale – Relazione annuale 2021 sull'applicazione della Carta dei diritti fondamentali dell'Unione europea*", doc. COM(2021)819 def. del 10 dicembre 2021, p. 18. V. in proposito A. Adinolfi, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in A. Pajno - F. Donati - A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol. I, *Diritti fondamentali, dati personali e regolazione*, Bologna, 2022, p. 130; F. Donati, *Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale*, ivi, p. 114.

[36] Punto 5 della relazione su "*Tutela dei diritti fondamentali nell'era digitale – Relazione annuale 2021 sull'applicazione della Carta dei diritti fondamentali dell'Unione europea*", cit., pp. 18 s.

[37] Cfr. 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 giu-*

© Wolters Kluwer Italia

ritti relativi alla dignità umana, alla buona amministrazione, alla protezione dei consumatori, alla sicurezza e all'assistenza sociale, alla libertà di espressione, alla libertà di riunione, all'istruzione, all'asilo, alla contrattazione e all'azione collettiva, alle condizioni di lavoro giuste ed eque, all'accesso all'assistenza preventiva, alla diversità culturale e linguistica, nonché con i diritti di gruppi vulnerabili (come i minori) e con i limiti imposti dalla bioetica [38]. Quando impiegati nelle attività di contrasto o giudiziarie, i sistemi di IA possono incidere sulla presunzione di innocenza e sul diritto a un processo equo e alla difesa. Inoltre, l'inaccessibilità o l'assenza di informazioni pertinenti sui sistemi automatizzati ostacola l'effettiva applicazione degli obblighi in materia di diritti fondamentali e l'accesso ai mezzi di ricorso [39].

A questi si affiancano dei "nuovi" diritti meritevoli di protezione. Tra gli altri, un "diritto di accesso all'algoritmo", per scongiurare l'esito discriminatorio che può sorgere dal relativo processo decisionale e poter verificare, previa traduzione dei modelli matematici in un linguaggio comprensibile, la conformità o meno ai diritti fondamentali dei criteri sui quali il processo stesso si basa; un "diritto alla disconnessione", espressione della tutela della salute e dei diritti dei lavoratori; un "diritto alla libertà cognitiva", con il divieto di ricorrere a tecniche che influenzano il comportamento umano in modo occulto; oppure un "diritto all'autonomia della persona nei confronti della macchina", non soltanto in rapporto alla manipolazione delle opinioni e dei comportamenti, quanto specialmente, come raccomandato dal Comitato economico e sociale nei pareri del 19 settembre 2018 e del 22 settembre 2021, per indicare "*(...) un limite nell'interazione tra lavoratori e macchine intelligenti, in modo che l'essere*

---

ridico nell'età dell'intelligenza artificiale, Pisa, 2020, pp. 29 s.; EAD., *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, cit., p. 146; A. ODDENINO, *Intelligenza artificiale e tutela dei diritti fondamentali: alcune notazioni critiche sulla recente proposta di regolamento della UE con particolare riferimento all'approccio basato sul rischio e al pericolo di discriminazione algoritmica*, in A. PAJNO - F. DONATI - A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, cit., pp. 165 ss. V. inoltre il punto 5 della relazione su "*Tutela dei diritti fondamentali nell'era digitale – Relazione annuale 2021 sull'applicazione della Carta dei diritti fondamentali dell'Unione europea*", cit., p. 18.

[38] A. ADINOLFI, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, cit., pp. 29 s.; EAD., *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, cit., p. 146. Cfr. il punto 5 della relazione su "*Tutela dei diritti fondamentali nell'era digitale – Relazione annuale 2021 sull'applicazione della Carta dei diritti fondamentali dell'Unione europea*", cit., p. 18.

[39] Punto 5 della relazione su "*Tutela dei diritti fondamentali nell'era digitale – Relazione annuale 2021 sull'applicazione della Carta dei diritti fondamentali dell'Unione europea*", cit., p. 18.

© Wolters Kluwer Italia

umano non sia mai l'esecutore della macchina" e per lasciare che "*(...) determinate decisioni rimangano prerogativa degli esseri umani, [...] [quando] hanno una componente morale e implicazioni giuridiche o un impatto sociale (...)*" [40].

La tripartizione dei sistemi di IA a seconda del rischio che questi comportano permette di verificare quali diritti fondamentali sono oggetto di tutela e di desumere quindi quale sia il grado di violazione ritenuta tollerabile o meno [41]. L'identificazione del rischio, effettuata in astratto e in via preventiva, potrebbe peraltro rivelarsi inidonea, all'atto pratico. Né il potere della Commissione di cui all'art. 7, di intervenire sull'All. III per aggiungere o modificare i casi di uso dei sistemi di IA ad alto rischio o per rimuoverli dalla lista, né il potere di valutazione e di riesame alla stessa affidato dall'art. 112, appaiono risolutivi: l'uno, perché si tratta pur sempre di modifiche che non possono derogare dai settori predefiniti nell'All. III; l'altro, a causa della rapidità del progresso tecnologico e "*(...) del modo con cui si possono manifestare nuove minacce ai diritti della persona e ai principi di democrazia*" [42].

Peculiare è il riverbero che i sistemi di IA hanno sulla protezione dei dati personali, prevista dall'art. 16 TFUE, dall'art. 8 della Carta dei diritti fondamentali e dall'art. 8 CEDU [43].

All'infuori (quando è permessa) dell'identificazione biometrica remota "in tempo reale" di persone fisiche in spazi accessibili al pubblico a fini di attività di contrasto, a termini del 38° "considerando" e dell'art. 5, par. 1, lett. h), il regolamento (UE) 2024/1689 non invoca il principio di specialità, ma dispone l'applicazione cumulativa tra esso e le fonti di diritto derivato pertinenti: il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati

---

[40] Così il punto 1.8. del parere del Comitato economico e sociale europeo del 19 settembre 2018 su "*L'intelligenza artificiale: anticipare i suoi effetti sul lavoro per assicurare una transizione equa*", reperibile in G.U.U.E. C440 del 6 dicembre 2018, pp. 1 ss.; e il punto 1.9. del parere del Comitato economico e sociale europeo del 22 settembre 2021 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*", in G.U.U.E. C517 del 22 dicembre 2021, pp. 61 ss. Sulla percepibilità di "nuovi" diritti, cfr. A. Adinolfi, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, cit., pp. 150 ss.

[41] V. A. Adinolfi, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, cit., p. 153 ss.

[42] Cfr. F. Donati, *Op. cit*., p. 120.

[43] Lo ha analizzato, tra gli altri, G. Contaldi, *Op. cit*., pp. 207 ss.

© Wolters Kluwer Italia

personali, nonché alla libera circolazione di tali dati [44]; la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte, rispettivamente, delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, ovvero delle istituzioni, degli organi e degli organismi dell'Unione, e alla libera circolazione di tali dati [45].

Il rinvio non scongiura del tutto alcuni problemi di coordinamento sui quali la dottrina, commentando la proposta del 2021, si era opportunamente soffermata. I colegislatori hanno chiarito adesso, nel 10° "considerando" del regolamento (UE) 2024/1689, che titolari e responsabili del trattamento sono i fornitori e i *deployer* dei sistemi di IA, dovendosi logicamente escludere l'attribuzione di queste qualifiche al sistema di IA vero e proprio, vista l'obbligatorietà dell'intervento umano ai sensi dell'art. 22 del regolamento (UE) 2016/679, dell'art. 11 della direttiva (UE) 2016/680 e dell'art. 24 del regolamento (UE) 2018/1725 [46]; e hanno espresso la volontà di mantenere varie definizioni contenute nei medesimi atti normativi per evitare irragionevoli e pericolose discrepanze [47]. Non sembrano però fugate le perplessità, per citarne due, sulla congruenza tra il concreto funzionamento dei sistemi di IA e i princìpi di minimizzazione e dell'espresso consenso di cui al regolamento (UE) 2016/679, alla direttiva (UE) 2016/680 e al regolamento (UE) 2018/1725; e riguardo all'aderenza dell'art. 10 del regolamento (UE) 2024/1689 ai casi di discriminazione indiretta, pur dopo

---

[44] In G.U.U.E. L119 del 4 maggio 2016, pp. 1 ss.

[45] Pubblicati in G.U.U.E. L119 del 4 maggio 2016, pp. 89 ss., e in G.U.U.E. L295 del 21 novembre 2018, pp. 39 ss.

[46] A. ADINOLFI, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, cit., pp. 22 s.; EAD., *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, cit., p. 149; G. CONTALDI, *Op. cit*., pp. 219 ss.; G. FINOCCHIARO - L. GRECO, *Il ruolo di titolare, responsabile e contitolare del trattamento nei trattamenti di dati personali mediante intelligenza artificiale*, in A. PAJNO - F. DONATI - A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, cit., pp. 313 ss.; T.E. FROSINI, *L'orizzonte giuridico dell'intelligenza artificiale*, in *Dir. inform*., 1/2022, p. 11; A. SIMONCINI, *Op. cit*., pp. 19 ss.

[47] È il caso dei "dati biometrici": cfr. l'art. 4, n. 14, del regolamento (UE) 2016/679; l'art. 3, n. 13, della direttiva (UE) 2016/680; l'art. 3, n. 18, del regolamento (UE) 2018/1725; il 14° "considerando" e l'art. 3, n. 34, del regolamento (UE) 2024/1689. V. anche A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, cit., p. 142.

© Wolters Kluwer Italia

l'intervento esplicativo sul par. 5 frutto della procedura legislativa ordinaria [48].

Ci si potrebbe interrogare sulla adeguatezza, tanto della trama di regolamentazione a vocazione generale scelta dalla Commissione, quanto delle altre fonti attualmente vigenti, a garantire la salvaguardia efficace dei diritti connessi all'intelligenza artificiale. Questo perché specifici sottoinsiemi di applicazioni di IA possono subire, anche durante l'uso, continui adattamenti non facilmente monitorabili che le cambiano e le fanno evolvere in modo imprevisto [49]. Il tenore del Preambolo e delle disposizioni della Carta dei diritti fondamentali, nonché delle norme della CEDU, consente in realtà interpretazioni tali da permettere "*(...) di estenderne la portata in relazione alle problematiche poste dai nuovi strumenti tecnologici*" [50]. La convenienza di esprimere princìpi e valori con fisionomia propria, più specifica rispetto a quanto si possa cogliere dagli strumenti esistenti, non è comunque da scartare e andrebbe valutata in riferimento ai "nuovi" diritti sopra menzionati, ogniqualvolta si dimostrasse la impossibilità di ricondurre agevolmente questi ultimi a diritti già protetti. La redazione di codici etici innovativi, flessibili e non vincolanti può essere di aiuto nella misura in cui essi riescano ad acquisire rilevanza interpretativa rispetto ai diritti fondamentali enunciati da atti vincolanti e a consentire la formulazione di regole tecniche sulla progettazione e sulla produzione dei sistemi di IA [51].

L'iniziativa culminata nelle "*Ethics Guidelines for Trustworthy*

---

[48] G. Contaldi, *Op. cit*., pp. 222 s. e 225 s.; G. Resta, *Op. cit*., pp. 336 s. Sulla compatibilità, riguardo al primo tema, dell'art. 20 della direttiva (UE) 2016/680 con il meccanismo operativo dei sistemi di IA e sulle ricadute che si possono manifestare per la sicurezza informatica, v. J. Andraško - M. Mesarčík - O. Hamulák, *The Regulatory Intersections between Artificial Intelligence, Data Protection and Cyber Security: Challenges and Opportunities for the EU Legal Framework*, in *AI & Soc*., 2/2021, pp. 623 ss.

[49] Punto 5 della relazione su "*Tutela dei diritti fondamentali nell'era digitale – Relazione annuale 2021 sull'applicazione della Carta dei diritti fondamentali dell'Unione europea*", cit., p. 19.

[50] Cfr. A. Adinolfi, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, cit., p. 32; Ead., *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, cit., p. 145. Il Preambolo della Carta dei diritti fondamentali dell'Unione europea codifica, del resto, l'obiettivo di rafforzare la tutela di tali diritti anche "*(...) alla luce [...] degli sviluppi scientifici e tecnologici (...)*".

[51] A. Adinolfi, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, cit., pp. 32 ss.; Ead., *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, cit., pp. 129 s. e 152 s.

© Wolters Kluwer Italia

AI" che il Gruppo di esperti di alto livello sull'intelligenza artificiale incaricato dalla Commissione ha emanato l'8 aprile 2019 [52], pare abbia avuto un risultato nei codici di buone pratiche e nei codici di condotta di cui agli art. 56 e 95 del regolamento (UE) 2024/1689, laddove questi si concentrano su canoni specifici di valutazione e di attenuazione dei rischi [53].

4. Il regolamento (UE) 2024/1689 come mezzo per migliorare il funzionamento del mercato interno

L'art. 114 TFUE, in combinato disposto con l'art. 26 dello stesso Trattato, affida all'Unione europea la competenza ad adottare misure di ravvicinamento destinate all'instaurazione e al funzionamento del mercato interno. Il regolamento (UE) 2024/1689, come dichiara anche la proposta del 2021, è strumentale a questo obiettivo, poiché, attraverso un quadro giuridico uniforme (teso a evitare un pregiudizio dovuto a interventi normativi isolati degli Stati membri), favorisce e sostiene le applicazioni di intelligenza artificiale per quanto concerne lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso, valorizzando il nesso che esse hanno con la realizzazione del mercato suddetto (nella specie, del mercato unico digitale) [54]. La garanzia della libera circolazione transfrontaliera di beni e servizi basati sull'IA impedisce agli Stati membri di imporre restrizioni alla commercializzazione e all'utilizzo dei relativi sistemi (se non espressamente autorizzate dal regolamento), a conferma degli aspetti positivi e strategici che l'IA esprime per vari settori dell'economia europea [55].

Rapide osservazioni si rendono opportune a proposito di pochi punti rilevanti.

L'art. 114, par. 1, TFUE lascia libere le istituzioni dell'Unione di

---

[52] HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, *Ethics Guidelines for Trustworthy AI*, Brussels, 2019. Ne danno notizia A. ADINOLFI, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, cit., p. 31; EAD., *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, cit., p. 153; G. SARTOR, *Artificial Intelligence and Human Rights: Between Law and Ethics*, in *MJECL*, 6/2020, pp. 705 ss.; G. CONTALDI, *Op. cit*., pp. 210 s. e 225 s.; G. RESTA, *Op. cit*., p. 328; N.T. NIKOLINAKOS, *Op. cit*., pp. 101 ss. e 119 ss.

[53] A. SIMONCINI, *Op. cit*., pp. 14 ss.; N.T. NIKOLINAKOS, *Op. cit*., pp. 600 ss.

[54] V. M. CARTA, *Op. cit*., p. 196; M. INGLESE, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?*, in *Quad. AISDUE*, 2/2024, pp. 12 s.

[55] V. il 1° "considerando" del regolamento (UE) 2024/1689.

© Wolters Kluwer Italia

optare tra l'adozione di regolamenti o di direttive (con salvezza delle procedure applicabili e del principio di proporzionalità, criteri dettati dall'art. 296, 1° co., TFUE). In proposito, la dottrina ha valutato con favore la scelta della Commissione (da taluni definita "coraggiosa") di proporre un regolamento. Questo pare, infatti, più appropriato a ridurre la frammentazione giuridica; a realizzare un'azione di armonizzazione preventiva, tale da "intercettare" l'esigenza di colmare un vuoto normativo prima che si "stabilizzino" negli Stati membri disposizioni differenziate sulla classificazione e sulla certificazione inclini a determinare una segmentazione dannosa; e a facilitare lo sviluppo di un mercato di sistemi di IA, come già detto, "leciti, sicuri e affidabili" [56].

Le condizioni e gli obblighi imposti agli operatori permettono di ottenere gli *standard* comuni che consentono di garantire l'armonizzazione delle regole nazionali necessarie ai fini del funzionamento del mercato interno. Il valore commerciale dei dati personali e il conseguente vantaggio derivante da una diffusione e da un trattamento non conformi al principio della tutela della vita privata, inducono d'altro canto ad affermare che risponde alle esigenze correlate al mercato e alle regole di concorrenza la regolamentazione sia degli aspetti più squisitamente tecnici dei prodotti e dei servizi fondati sull'IA (necessari, per l'appunto, a garantire le libertà del mercato stesso), sia di quelli connessi al rispetto rigoroso dei diritti fondamentali (per evitare il vantaggio competitivo di imprese non tenute a osservare parametri altrettanto stringenti) [57].

L'aver concepito i sistemi di IA come prodotti (potenzialmente pericolosi), ha peraltro portato la Commissione e i colegislatori a ricorrere al procedimento, ben conosciuto nel diritto dell'Unione europea da circa quaranta anni (e abbastanza criticato, in verità), del c.d. Nuovo Approccio, o *New Legislative Framework*, il quale, per la definizione di aspetti tecnici e complessi della regolazione dei prodotti industriali e dei servizi nel mercato interno, fa leva su strumenti non vincolanti, volontari e di provenienza privata [58]. Nel regolamento sull'intelligenza

---

[56] Cfr. A. Adinolfi, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, cit., pp. 136 s. e 140 s.; F. Donati, *Op. cit*., p. 120; A. Simoncini, *Op. cit.*, p. 10; M. Carta, *Op. cit*., pp. 196 s. e 198; M. Inglese, *Op. cit*., pp. 8 ss.

[57] Cfr. A. Adinolfi, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, cit., p. 34; M. Inglese, *Op. cit*., pp. 13 s.

[58] V. in argomento M. Eliantonio - C. Cauffman (eds.), *The Legitimacy of Standardisation as a Regulatory Technique. A Cross-disciplinary and Multi-level Analysis*, Cheltenham, 2020; A. Simoncini, *Op. cit.*, p. 26; M. Carta, *Op. cit*., p. 197; A. Volpa-

© Wolters Kluwer Italia

artificiale, quindi, sono state inserite solamente le caratteristiche essenziali di interesse generale, mentre la definizione dettagliata delle regole tecniche (denominate "norme armonizzate") viene demandata alle organizzazioni europee di normazione riconosciute nell'All. I del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, chiamate a pronunciarsi su richiesta della Commissione [59]. Per i sistemi di IA ad alto rischio, sottoposti ai requisiti di affidabilità, l'applicazione delle norme armonizzate facilita l'ottenimento della certificazione ai fini della dichiarazione di conformità UE, della marcatura CE e dell'immissione sul mercato. L'art. 40, par. 1, del regolamento (UE) 2024/1689 stabilisce pertanto che "*I sistemi di IA ad alto rischio [...] che sono conformi alle norme armonizzate o a parti di esse i cui riferimenti sono stati pubblicati nella* Gazzetta ufficiale dell'Unione europea *[...] si presumono conformi ai requisiti di cui [agli art. 10-15] (...)*" del medesimo regolamento. Tale meccanismo e la supposizione di conformità vengono altresì estesi alla categoria dei modelli di IA per finalità generali [60].

È inutile nascondere che quanto sopra delineato non è esente da difficoltà, risolte solo parzialmente dal regolamento (UE) n. 1025/2012. Non pochi commentatori hanno fatto risaltare i problemi, sotto il profilo democratico, posti da queste norme armonizzate dettate da aziende private il cui *expertise* è lontano dalla scienza giuridica [61]. Formalmente non sono vincolanti, ma hanno notevoli effetti giuridici e pratici per gli operatori economici (soprattutto quando sussistono esigenze di certificazione), tanto da essere ormai ritenute delle "misure di attuazione necessaria" di requisiti essenziali definiti dal diritto derivato, paragonabili a un atto di esecuzione, componenti proprie del di-

---

TO, *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale*, in *Quad. AISDUE*, 2/2024, pp. 3 ss.

[59] Sul regolamento (UE) n. 1025/2012 v. G.U.U.E. L316 del 14 novembre 2012, pp. 12 ss. Con la decisione di esecuzione C/2023/3215 del 22 maggio 2023 [precedente, perciò, al regolamento (UE) 2024/1689], la Commissione ha selezionato, tra le organizzazioni, il Comitato europeo di normazione (CEN) e il Comitato europeo di normazione elettrotecnica (CENELEC), e ha dato loro il mandato di elaborare norme armonizzate a supporto della politica europea sull'intelligenza artificiale. Cfr. S. DE VRIES - O. KANEVSKAIA - R. DE JAGER, *Internal Market 3.0: The Old "New Approach" for Harmonising AI Regulation*, in *Eur. P.*, 2/2023, pp. 583 ss.; A. VOLPATO, *Op. cit.*, pp. 9 ss.

[60] A. VOLPATO, *Op. cit.*, p. 10. V. anche il 121° "considerando" del regolamento (UE) 2024/1689.

[61] Per i dettagli si rinvia ad A. VOLPATO, *Op. cit.*, pp. 7 s. V. anche M. VEALE - F. ZUIDERWEEN BORGESIUS, *Demystifying the Draft EU Artificial Intelligence Act*, in *Comp. LRI*, 4/2021, p. 105; G. RESTA, *Op. cit.*, pp. 341 s.

© Wolters Kluwer Italia

ritto dell'Unione europea soggette all'interpretazione pregiudiziale della Corte di giustizia ai sensi dell'art. 267 TFUE [62]. Di qui alcuni correttivi specifici pensati per l'IA, introdotti dal regolamento (UE) 2024/1689 a garanzia dell'interesse pubblico e dei diritti fondamentali: la maggiore enfasi sull'inclusività e sulla partecipazione al processo di normazione tecnica; il rafforzamento del ruolo di controllo della Commissione, fino a poter impedire la pubblicazione del riferimento alla norma armonizzata sulla G.U.U.E.; l'induzione delle organizzazioni europee di normazione ad agire in ossequio alle indicazioni delle istituzioni dell'Unione [63]. Un certo scetticismo, tuttavia, permane. Non sembra che il largo potere decisionale delegato alle organizzazioni suddette dall'art. 40 precedentemente citato (perché non è chiaro quali diritti fondamentali vadano salvaguardati, né se siano garantite le competenze opportune per valutazioni così complesse) metta al riparo da possibili incompatibilità con la giurisprudenza della Corte di giustizia protettiva dei princìpi generali del diritto dell'Unione [64].

5. Rilievi sulla conformazione della *governance* e sull'attività di vigilanza nazionale

Un accenno merita, infine, l'architettura di *governance* ideata dal regolamento sull'intelligenza artificiale per gli ordinamenti dell'Unione europea e degli Stati membri.

Nell'Unione si contempla, in primo luogo, la creazione di un Ufficio per l'IA costituito presso la Commissione e da questa formalizzato con la decisione C/2024/1459 del 24 gennaio 2024 [65]. La sua configurazione originaria, suggerita non dalla proposta del 2021, ma dal Parlamento europeo nel corso del procedimento legislativo, immaginava un organismo con funzioni e poteri rilevanti, totalmente indipendente, dotato di personalità giuridica, controllato e diretto dagli Stati membri, dalla Commissione, dal Garante europeo della protezione dei dati (GEPD), dall'Agenzia dell'Unione europea per i diritti fondamentali e dall'Agenzia dell'Unione europea per la cibersicurezza, responsabile nei confronti dello stesso Parlamento europeo e

[62] C. giust. UE, 27 ottobre 2016, C-613/14, *James Elliott Construction Ltd*, punto 43. Su questa sentenza e sulla giurisprudenza della Corte in merito v. A. Volpato, *Op. cit*., pp. 8 s.

[63] Art. 40, par. 2 e 3, e 41, par. 1 e 4, del regolamento (UE) 2024/1689.

[64] Cfr. in tal senso A. Volpato, *Op. cit*., pp. 12 ss.

[65] In G.U.U.E. C/2024/1459 del 14 febbraio 2024, pp. 1 ss.

© Wolters Kluwer Italia

del Consiglio [66]. Il regolamento (UE) 2024/1689, agli art. 3, n. 47, e 64, par. 1, delinea invece una struttura centralizzata, parte integrante della Commissione, soggetta al suo piano di gestione annuale, volta all'attuazione, al monitoraggio e alla supervisione sia dei sistemi di IA e dei modelli di IA per finalità generali, sia della *governance* dell'IA [67]. È evidente l'abbondante stravolgimento a vantaggio di un maggiore condizionamento della Commissione, senza più riferimenti alla responsabilità verso altre istituzioni e al controllo statale. La stessa decisione C/2024/1459 è un provvedimento *sui generis*: emessa quando il regolamento (UE) 2024/1689 era ancora "di prossima adozione", ha anticipato così diverse sue disposizioni e non è un atto delegato o esecutivo, quanto piuttosto "*(...) un atto «a schema libero» e sintomatico del margine di manovra che la Commissione si è riservata nell'attività di supervisione di una materia altamente sensibile*" [68].

È prevista altresì l'istituzione del Consiglio europeo per l'intelligenza artificiale ("Consiglio per l'IA"), formato dai rappresentanti degli Stati membri e al quale il GEPD partecipa come osservatore. Il Consiglio per l'IA funge da organo di coordinamento, consultivo e di assistenza per la Commissione e per gli Stati membri. Tra le varie funzioni enunciate dall'art. 66 (in un elenco non "chiuso"), preme segnalare quelle concernenti la raccolta e la condivisione tra gli Stati membri delle conoscenze e delle migliori pratiche tecniche e normative; la formulazione, su richiesta della Commissione o di propria iniziativa, di raccomandazioni e pareri scritti su qualsiasi questione pertinente relativa all'attuazione del regolamento; il sostegno alla Commissione nella promozione dell'alfabetizzazione in materia di IA, della sensibilizzazione del pubblico e della comprensione dei benefici, dei rischi, delle garanzie, dei diritti e degli obblighi in relazione all'uso dei sistemi di IA; il contributo alla efficace cooperazione con le auto-

---

[66] V. gli emendamenti 523-530 (art. 56-56 *quater*) illustrati nella relazione del 22 maggio 2023 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, doc. A9-0188/2023, pp. 280 ss. Cfr. inoltre F. FERRI, *Il giorno dopo la rivoluzione: prospettive di attuazione del regolamento sull'intelligenza artificiale e poteri della Commissione europea*, in *Quad. AISDUE*, 2/2024, pp. 13 ss.

[67] L'art. 112, par. 5, del regolamento (UE) 2024/1689 attribuisce alla Commissione il compito di valutare, entro il 2 agosto 2028, il funzionamento dell'Ufficio per l'IA, al fine di verificare se sia necessario potenziarne le competenze di esecuzione e aumentarne le risorse, trasmettendo poi una relazione al Parlamento europeo e al Consiglio.

[68] F. FERRI, *Op. cit.*, p. 15.

© Wolters Kluwer Italia

rità competenti degli Stati terzi e con le organizzazioni internazionali [69]. Rispetto alla proposta del 2021 e alle interlocuzioni successive con il Parlamento europeo (nelle quali si menzionava un "Comitato europeo per l'intelligenza artificiale"), occorre rilevare nel regolamento (UE) 2024/1689 alcune differenze, orientate in questo caso a "depotenziare" la Commissione: questa non presiede più il Consiglio per l'IA, non convoca più le sue riunioni e non prepara più il relativo ordine del giorno [70]. Il minor peso specifico di tale Consiglio in relazione all'Ufficio per l'IA sembra inoppugnabile, malgrado l'estensione delle mansioni affidategli [71].

Se l'Ufficio e il Consiglio per l'IA consolidano la "centralizzazione" "*(...) che [...] sta innervando le riforme UE intese a limitare la libertà di azione di attori economici ritenuti capaci di alterare sin dalle fondamenta le basi comuni su cui si innesta il processo di integrazione europea*" [72], il *Forum* consultivo, con membri permanenti e temporanei, rappresenta la selezione equilibrata dei portatori di interessi commerciali e non commerciali (industria, *start-up*, PMI, società civile, mondo accademico) [73]. C'è poi il Gruppo di esperti scientifici indipendenti, selezionati dalla Commissione, il cui compito consiste soprattutto nell'avvisare l'Ufficio per l'IA dei possibili rischi sistemici nell'Unione dei modelli di IA per finalità generali e nell'offrire consulenza sulla classificazione e sperimentazione dei modelli suddetti [74]. Va da sé che l'effettiva idoneità del *Forum* e del Gruppo di esperti a realizzare i rispettivi mandati, soprattutto a valutare correttamente i problemi etici e giuridici legati all'impiego dell'IA, dipenderà dalla qualità e dalla competenza tecnica delle persone chiamate a farne parte, nonché dalla loro abilità a rendersi autonome da pressioni esterne di tipo politico ed economico [75].

---

[69] V. l'art. 66, lett. b), e), f) e i), del regolamento (UE) 2024/1689. Cfr. N.T. Nikolinakos, *Op. cit*., pp. 605 ss.

[70] Cfr. l'art. 57, par. 3, della proposta di regolamento del 2021, cit., p. 77, nonché F. Ferri, *Op. cit*., p. 16.

[71] F. Ferri, *Op. cit*., p. 17.

[72] *Ibid*.

[73] V. l'art. 67 del regolamento (UE) 2024/1689. I membri permanenti del *Forum* consultivo sono "*(...) l'Agenzia per i diritti fondamentali, l'ENISA, il Comitato europeo di normazione (CEN), il Comitato europeo di normazione elettrotecnica (CENELEC) e l'Istituto europeo per le norme di telecomunicazione (ETSI) (...)*" (par. 5); i membri temporanei (il mandato è biennale, prorogabile fino al massimo di quattro anni) li nomina la Commissione "*(...) tra i portatori di interessi con competenze riconosciute nel settore dell'IA*" (par. 3).

[74] Art. 68 del regolamento (UE) 2024/1689.

[75] F. Donati, *Op. cit*., pp. 124 s.

© Wolters Kluwer Italia

Relativamente agli Stati membri, l'art. 70 del regolamento (UE) 2024/1689 dispone che ciascuno di essi debba designare le autorità competenti (almeno un'autorità di notifica e un'autorità di vigilanza del mercato, che opera nello Stato come punto di contatto unico) le quali, agendo "*(...) in modo indipendente, imparziale e senza pregiudizi (...)*" e salvaguardando i "*(...) principi di obiettività delle loro attività e dei loro compiti (...)*", assicurino l'applicazione e l'attuazione del regolamento medesimo, in condizioni adeguate di cibersicurezza e nel rispetto degli obblighi di riservatezza dettati dall'art. 78 [76]. Le autorità di vigilanza del mercato, nell'ambito degli obblighi di segnalazione di cui al regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti [77], contribuiscono al monitoraggio successivo all'immissione sul mercato mediante *audit* e danno ai fornitori la possibilità di rendere noti incidenti o violazioni gravi dei diritti fondamentali di cui sono venuti a conoscenza. Qualsiasi autorità di vigilanza, inoltre, può, per motivi eccezionali, autorizzare l'immissione sul mercato di uno specifico sistema di IA ad alto rischio [78]. Nel complesso, la struttura di vigilanza concisamente descritta appare frammentata e potenzialmente incline a privilegiare interventi limitati al territorio dei singoli Stati membri. L'orientamento a tutelare le esigenze di controllo di questi ultimi sull'IA viene confermato dall'ampia discrezionalità che gli Stati stessi hanno nel designare le rispettive autorità preposte, creandone di nuove o utilizzando quelle già esistenti [79]. Manca un soggetto indipendente che sia in grado di garantire un coordinamento effettivo non solo tra le autorità nazionali, ma anche tra queste e il GEPD (competente per la vigilanza sulle istituzioni, sugli organi e sugli organismi dell'Unione, a termini dell'art. 70, par. 9) [80]. Ne risulta una orga-

---

[76] Così l'art. 70, par. 1, 2, 4 e 5, del regolamento (UE) 2024/1689. Il par. 3 precisa inoltre che il personale preposto deve possedere una comprensione approfondita delle tecnologie, dei dati e del calcolo dei dati di IA, della protezione dei dati personali, della cibersicurezza, dei diritti fondamentali, dei rischi per la salute e la sicurezza, e una conoscenza delle norme e dei requisiti giuridici esistenti.

[77] In G.U.U.E. L169 del 25 giugno 2019, pp. 1 ss. V. l'art. 34, par. 4, del regolamento (UE) 2019/1020.

[78] Art. 74 del regolamento (UE) 2024/1689. V. N.T. NIKOLINAKOS, *Op. cit.*, pp. 617 ss.

[79] M. INGLESE, *Op. cit*., p. 15; S. VILLANI, *Il sistema di vigilanza sull'applicazione dell'*AI Act*: ognun per sé?*, in *Quad. AISDUE*, 2/2024, pp. 10 e 17.

[80] S. VILLANI, *Op. cit*., p. 18, nota al riguardo che "*(...) in assenza di un sistema di raccordo indipendente a livello sovranazionale, sarà la Commissione europea, e dunque un'istituzione politica [...], ad assumere il ruolo di «super controllore» del sistema*

© Wolters Kluwer Italia

nizzazione non del tutto sufficiente ad assicurare una applicazione efficace del regolamento in esame, troppo affidata, nella sostanza, all'azione esecutiva delle autorità nazionali, con il conseguente pericolo di difformità, anche nei criteri di valutazione degli *standard* tecnici, dovute a risorse e a prassi di intervento variabili da Stato a Stato [81].

6. I sistemi di intelligenza artificiale tra efficienza competitiva e promozione di diritti, libertà e valori. Conclusioni

John McCarthy, l'antesignano dell'intelligenza artificiale menzionato nel paragrafo introduttivo, era solito affermare che l'IA fosse "the science and engineering of making intelligent machines, especially intelligent computer programs" [82]. Una definizione forse riduttiva, vista l'inimmaginabile, travolgente (e inarrestabile) ascesa a cui stiamo assistendo, verosimilmente concepita in origine più per fare colpo, ammaliandoli, sugli addetti ai lavori, quale pungolo alla creazione e alla sperimentazione di macchine che fossero in grado, prima o poi, di esibire capacità di ragionamento paragonabili a quelle umane [83].

L'intelligenza artificiale, in effetti, sta trasformando il mondo, la società e l'industria esattamente come hanno fatto in passato il motore a vapore o l'elettricità. È destinata ad avere un impatto enorme sugli stili di vita e di lavoro delle persone nei prossimi decenni. L'aumento della velocità di calcolo e della disponibilità dei dati, e il progresso negli algoritmi, la rendono una delle tecnologie più strategiche del XXI secolo [84].

In questo scenario, il regolamento (UE) 2024/1689, malgrado rifletta una prospettiva prevalentemente rivolta agli aspetti commerciali

---

di vigilanza, potendo valutare, in caso di dubbi, se le misure adottate dalle autorità nazionali rispetto ai sistemi di IA immessi nel mercato siano giustificate".

[81] *Ibid*.

[82] Come riportato da P. Wang, *On Defining Artificial Intelligence*, in *J. Art. Gen. Int*., 2/2019, pp. 1 ss., e da R.S. Sutton, *John McCarthy's Definition of Intelligence*, ivi, 2/2020, pp. 66 s.

[83] La stessa espressione "intelligenza artificiale", d'altronde, era stata accuratamente scelta per motivare le nuove generazioni di scienziati, ingegneri e ricercatori impegnati nella cibernetica e nell'informatica, e per attrarre i finanziamenti necessari: lo dice con franchezza F. Cabitza, Deus in machina? *L'uso umano delle nuove macchine, tra dipendenza e responsabilità*, in L. Floridi - F. Cabitza (a cura di), *Intelligenza artificiale. L'uso delle nuove macchine*, Firenze, 2021, pp. 9 s.

[84] Punto 1 della comunicazione su "*L'intelligenza artificiale per l'Europa*", cit., p. 2; punto 1 della comunicazione sul "*Piano coordinato sull'intelligenza artificiale*", cit., p. 1.

© Wolters Kluwer Italia

dell'IA, cerca di intraprendere una applicazione umana ed etica di questa nuova tecnologia attraverso una struttura normativa proporzionata e a "geometria variabile" per mezzo della quale, ponendo l'accento sulla necessità di preservare la salute, la sicurezza e i diritti fondamentali, statuisce una serie di requisiti che devono essere rispettati soltanto dagli operatori di sistemi di IA ad alto rischio [85]. Il regolamento in parola diventa così il veicolo per il cui tramite si prova a realizzare una sintesi, un bilanciamento accettabile tra elementi concorrenti: la sperimentazione innovativa e la crescita economica, con il rafforzamento della capacità industriale e tecnologica dell'Unione allo scopo di diffondere l'IA in tutto il mercato interno e di potersi misurare con altri attori internazionali; e la protezione di diritti, libertà e valori sanciti dai Trattati istitutivi, dalla Carta dei diritti fondamentali dell'Unione europea, dalla CEDU e dalla giurisprudenza della Corte di giustizia, avvertiti come intangibili e rispetto ai quali l'Unione stessa, rifacendosi anche alle affermazioni del Comitato economico e sociale contenute in un parere reso il 19 settembre 2018, non è affatto disposta a retrocedere [86].

Tanto il regolamento (UE) 2024/1689, quanto la proposta del 2021 che lo ha precorso, appaiono significativamente influenzati dalla tensione dialettica tra le suddette finalità contrapposte. Dal loro testo emerge un atteggiamento ambivalente. Da un lato, ci sono gli interessi economici dell'Unione collegati al funzionamento del mercato interno e alla competitività dell'industria europea in ambito globale, con la conseguente promozione dello sviluppo delle applicazioni di IA ai fini di accrescere la capacità innovativa delle imprese europee nelle tecno-

---

[85] V. G. CONTALDI, *Op. cit*., pp. 214 ss.; A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, cit., pp. 153 ss.; F. DONATI, *Op. cit*., pp. 117 ss.; G. FINOCCHIARO, *Op. cit*., pp. 311 ss.; G. RESTA, *Op. cit*., pp. 338 ss. Sulla opportunità di dispositivi di IA umani ed etici, cfr. anche A.C. AMATO MANGIAMELI, *Intelligenza artificiale, big data e nuovi diritti*, in *Riv. it. inform. dir.*, 1/2022, pp. 93 ss.

[86] Così L. FLORIDI, *Op. cit*., p. 218; A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, cit., pp. 128 e 133; e G. RESTA, *Op. cit*., p. 328. Nel punto 4.1. del parere del Comitato economico e sociale europeo del 19 settembre 2018 sulla "*Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni — L'intelligenza artificiale per l'Europa*", pubblicato in G.U.U.E. C440 del 6 dicembre 2018, pp. 51 ss., si osserva infatti che "*(...) i valori e i principi dell'UE non dovrebbero essere sacrificati sull'altare della competitività globale*". Cfr. altresì il 2° "considerando" del regolamento (UE) 2024/1689.

© Wolters Kluwer Italia

logie evolute. Dall'altro, insistono le preoccupazioni relative alla tutela delle attività commerciali tradizionali e al rispetto dei valori dell'Unione sui quali l'art. 2 TUE fonda l'integrazione tra gli Stati membri, con la conseguente manifestazione di cautela nei confronti di fenomeni che "*(...) incidono fortemente sugli schemi di regolazione – in particolare quelli relativi alle libertà economiche e alla concorrenza – consolidati nell'ordinamento dell'Unione*", nonché di una problematica teorico-pratica riguardante i limiti che "*(...) le libertà di mercato – in questo caso, quelle del mercato digitale – devono trovare alla luce della protezione dei diritti fondamentali e dei valori dell'Unione*" [87].

Nello sfruttamento dell'intelligenza artificiale appare decisiva la chiara volontà dell'Unione europea di colmare il divario economico, sociale e giuridico accumulato finora rispetto agli Stati Uniti d'America (detentori di un antico primato tecnologico) e alla Cina (potenza emergente nel settore), "recuperando" nei loro confronti un protagonismo messo a dura prova dal recesso del Regno Unito [88]. Gli orientamenti politici per la Commissione 2024-2029 "*Europe's Choice*", una volta confermato che "(...) Europe is already leading the way on making AI safer and more trustworthy, and on tackling the risks stemming from its misuse", hanno ribadito la necessità di concentrare gli sforzi "(...) on becoming a global leader in AI innovation" [89]. Quello adottato dall'Unione, dunque, è un modello di regolamentazione "rigido" a carattere "orizzontale", non incentrato sulla *ballot-box democracy* o sulla *rule by law*, bensì mirato alla sorveglianza umana, nonché alla gestione ottimale dei rischi insiti nell'uso dei dispositivi di IA, a difesa dei diritti e delle libertà individuali. In quanto tale, si contrappone al modello "auto-regolatorio" statunitense (fondato sull'*antitrust*) e al modello "dirigistico" cinese (ispirato al capitalismo di Stato) [90]. Nel

---

[87] Cfr. A. Adinolfi, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, cit., p. 15.

[88] A. Adinolfi, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, cit., p. 17; G. Contaldi, *Op. cit*., p. 208; G. Resta, *Op. cit*., pp. 325 ss.; A. Simoncini, *Op. cit*., pp. 27 s.; M. Carta, *Op. cit*., p. 190; M. Inglese, *Op. cit*., p. 3.

[89] European Commission, *Europe's Choice*, *Political Guidelines for the Next European Commission 2024-2029*, Brussels, 2024, p. 10.

[90] Cfr. in merito E. Brattberg - R. Csernatoni - V. Rugova, *Europe and AI: Leading, Lagging Behind, or Carving Its Own Way?*, Carnegie Endowment for International Peace Working Paper, Washington, D.C., 2020, pp. 5 ss.; H. Roberts - J. Cowls - F. Mazzi - A. Tsamados - M. Taddeo - L. Floridi, *Achieving a "Good AI Society": Comparing the Aims and Progress of the EU and US*, in *Sc. Eng. Ethics*, 27/2021, pp. 1 ss.; F. Donati, *Op. cit*., pp. 121 s.; G. Finocchiaro, *Op. cit*., p. 304; H. Roberts - J. Cowls - E. Hine - J. Morley - V. Wang - M. Taddeo - L. Floridi, *Governing Artificial Intelli-*

© Wolters Kluwer Italia

governare le nuove tecnologie, esso intende proteggere i diritti fondamentali e i valori europei. Desideroso di concretizzare il c.d. *Brussels effect* (ossia, l'attitudine dell'Unione di adottare discipline che diventino poi *standard* accettati su scala globale), persegue con determinazione l'obiettivo dell'esportazione in altre regioni geopolitiche del proprio schema di riferimento: uno schema sì giuridico, ma anche, e soprattutto, culturale [91]. Non è un caso che il regolamento (UE) 2024/1689 abbia all'art. 2, par. 1, come già accennato, una clausola di applicazione molto ampia, idonea a manifestare forme di estensione extraterritoriale non discriminatoria della normativa di diritto derivato nei riguardi di soggetti (fornitori, *deployer*, rappresentanti autorizzati di fornitori) stabiliti in Stati terzi [92].

La vera sfida per il futuro, che il regolamento (UE) 2024/1689 e diversi altri provvedimenti cui si accompagna sembrano destinati a raccogliere, nell'ambito del mercato unico digitale e di una "via europea" allo sviluppo tecnologico da questo prospettata, è pertanto quella dell'"innovazione responsabile" nella quale, in relazione all'intelligenza artificiale, senza essere di ostacolo alla transizione in corso si raggiunga una ponderazione adeguata tra i benefici recati dall'utilizzo dell'IA e i diritti fondamentali delle persone, venendosi a saldare l'approccio basato sul rischio con la visione antropocentrica [93]. L'Unione europea può assumere un ruolo guida e sfruttare al massimo le opportunità offerte dall'IA, avvalendosi in ciò non solo di ricercatori, laboratori e imprese *start-up* di elevato livello, ma anche del mercato unico digitale, le cui norme comuni in materia di protezione e libera circolazione dei dati, di sicurezza informatica e di connettività aiutano le società a operare e a crescere perché incoraggiano gli investimenti [94].

Può il regolamento (UE) 2024/1689, pienamente valido solo nel

---

gence in China and the European Union: Comparing Aims and Promoting Ethical Outcomes, in *Inform. Soc.*, 2/2023, pp. 79 ss.

[91] A. ADINOLFI, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, cit., p. 34; EAD., *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, cit., pp. 161 s.; F. DONATI, *Op. cit*., p. 122; G. FINOCCHIARO, *Op. cit*., p. 304; G. RESTA, *Op. cit*., p. 334; M. CARTA, *Op. cit*., p. 190. Per approfondimenti sul *Brussels effect* si rinvia ad A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, New York, 2020.

[92] V. L. FLORIDI, *Op. cit*., pp. 216 s.; G. RESTA, *Op. cit*., pp. 330 ss. Cfr. altresì il 21°, 22° e 82° "considerando" del regolamento (UE) 2024/1689.

[93] Cfr. F. DONATI, *Op. cit*., p. 115; A. ODDENINO, *Op. cit*., p. 198.

[94] Punto 1 della comunicazione su "*L'intelligenza artificiale per l'Europa*", cit., p. 2. Sul mercato unico digitale e sui vari aspetti a esso collegati, v. F. ROSSI DAL POZZO (a cura di), *Mercato unico digitale, dati personali e diritti fondamentali*, *Eurojus*, numero speciale, 2020.

© Wolters Kluwer Italia

2027, essere concretamente funzionale a questo obiettivo? Bisognerà verificarlo nella pratica, e dipenderà anche dall'autonomia, dall'indipendenza e dalla preparazione tecnica di chi dovrà applicarlo e assicurarne l'osservanza. Accanto a indiscutibili punti di forza, permangono zone d'ombra che lo rendono al momento (sia permessa l'espressione figurata) un atto ancora "in chiaroscuro". Oltre alla mancata definizione di un modello di responsabilità civile per i danni provocati da sistemi di IA [95], è, in particolare, nell'identificazione astratta, preventiva e "in bianco" delle soglie di rischio che si annidano le maggiori esitazioni. La classificazione rigida dei dispositivi di IA, fatta seguendo logiche di discrezionalità politica che non lasciano spazio alcuno all'apprezzamento individuale dei destinatari della norma, è abituale nei sistemi tecnologici né vietati, né leciti in assoluto, ma potrebbe rivelarsi inadeguata di fronte al pericolo di discriminazione algoritmica e non sufficientemente elastica per stare al passo con una intelligenza artificiale "strutturalmente mobile" [96].

[95] M. Carta, *Op. cit*., pp. 192 s.

[96] Il termine è di A. Oddenino, *Op. cit*., pp. 198 ss., il quale aggiunge che, per questo motivo, "*(...) si sarebbe potuto ricorrere ad una qualche formulazione del principio precauzionale, che è tipicamente evocato in ambiti caratterizzati dalla impossibilità di una piena conoscibilità e conseguente gestione del rischio (...)*". V. altresì F. Donati, *Op. cit*., pp. 119 e 125; G. Finocchiaro, *Op. cit*., pp. 321 s.; G. Resta, *Op. cit*., p. 339; A. Simoncini, *Op. cit*., pp. 8 e 12; M. Carta, *Op. cit*., pp. 193 ss.

© Wolters Kluwer Italia

THE FRAMEWORK CONVENTION ON ARTIFICIAL INTELLIGENCE AND HUMAN RIGHTS, DEMOCRACY AND THE RULE OF LAW PROMOTED BY THE COUNCIL OF EUROPE: SOME CRITICAL ISSUES *

CHIARA VENTURINI

SUMMARY: 1. Introductory remarks. – 2. The Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. – 3. The potential critical aspects of the Framework Convention. – 3.1. An AI definition. – 3.2. The scope of application and exceptions. – 3.3. The complementary nature of the Convention. – 3.4. The general principles of the Convention. – 3.5. The monitoring system of the Convention. – 3.6. Territorial application. – 4. Concluding remarks.

Abstract: The year 2024 marked the adoption of the first international and European regulatory instruments on artificial intelligence: the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law; the AI Act; and the UN General Assembly resolution entitled "*Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*". This paper focuses on the first of these instruments. Although it is a regional instrument, the Convention has a clear universal aspiration. While innovative in many respects, the treaty is complementary in nature to the obligations laid down in the European Convention on Human Rights, yet appears to confer considerable discretion to the States Parties. Accordingly, this paper will analyse its most critical provisions, bearing in mind that the Convention's actual effectiveness can only be assessed once it enters into force.

* Contribution subjected to double-blind peer review.

© Wolters Kluwer Italia

1. Introductory remarks

The first treaty on artificial intelligence, the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law [1] (hereinafter Convention), was recently approved [2] within the Council of Europe. [3] It was opened for ratification not only by the organisation's Member States, but also by non-Members as of 5 September 2024. At the time of writing [4], Andorra, Georgia, Iceland, Norway, the Republic of Moldova, San Marino, the United Kingdom, Israel, the United States of America, and the European Union have signed the Convention, which will enter into force on the first day of the month following the expiration date of a three-months period from the date of ratification by five Signatories, including at least three Council of Europe Member States. Therefore, it is reasonable to assume that the time is ripe for a rapid entry into force of the agreement, resulting in obligations for the Parties.

However, this is not the only binding source about artificial intelligence, at least for some States: Regulation (EU) 2024/1689 of the European Parliament and of the Council, of 13 June 2024, which establishes harmonised rules on artificial intelligence [5], was approved by the Council of the European Union on 21 May 2024 (hereinafter also the AI Act). The Regulation, as well as the Convention under review, aims to protect the fundamental rights of individuals under the Charter of Fundamental Rights of the European Union and their safety, as well

---

[1] Text available online: *www.rm.coe.int.*

[2] 17 May 2024.

[3] For a comment on the work of the Council of Europe on this topic C. CASTETS-RENARD - J. EYNARD, *Artificial intelligence law: between sectoral rules and comprehensive regime: comparative law*, Brussels, 2023, pp. 134 ff.

[4] This text was last updated as of August 2024.

[5] 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 Regulation), OJEU L/2024/1689, 12 July 2024, pp. 1 ff. On the Regulation see A. ANDREANGELI, *Algoritmi di prezzo e legge sull'intelligenza artificiale: navigare in acque inesplorate tra il diritto della concorrenza e la regolamentazione tradizionale delle tecnologie autonome*, in this volume, pp. 63 ff.; P. SIMONE, *Verso l'individuazione di una "via europea" allo sviluppo tecnologico. Alcune riflessioni sul regolamento (UE) 2024/1689 che stabilisce norme armonizzate sull'intelligenza artificiale*, in this volume, pp. 15 ff.; R.J. NEUWIRTH, *The EU Artificial Intelligence Act: regulating subliminal AI systems,* Abingdon, Oxon, 2023.

© Wolters Kluwer Italia

as the founding values of the legal order such as democracy, the rule of law and the protection of the environment, from the possible negative impact of the use of artificial intelligence. The complementarity of the provisions of the two acts is evident and justified the proposal for a Council Decision [6]. The purpose of the latter was to initiate the process leading to the European Union's signature of the Convention, with the intention of subsequently proceeding to its ratification in accordance with Article 218, para. 5, TFEU. [7]

Indeed, it is only fair to recall that if, on the one hand, the Convention is the first international treaty on AI, on the other hand, the European Union Regulation is the first of its kind on the subject with direct applicability. [8] The latter constitutes the fulfilment of the obligations of the former. [9] Not only the Council sees the two sources as aligned in their approach to artificial intelligence systems, but, given its strictly risk-based character, [10] it requires risk assessment and mitigation measures. [11] The Convention includes principles and obligations already covered by the Regulation, such as measures for the protection of human rights, safety and reliability, responsibility and accountability, data

---

[6] Proposal for a Council Decision on the signing, on behalf of the European Union, of the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, 26 June 2024. The latter was followed by the Council Decision (EU) 2024/2218 of 28 August 2024 on the signing, on behalf of the European Union, of the Council of Europe Framework Convention on Artificial ntelligence and Human Rights, Democracy and the Rule of Law that lead to the signature by the EU.

[7] Since the subject matter of the Convention is also largely regulated by European Union law, in the Council's view it should be ratified by reason of Article 3, para. 2, TFEU. The exercise of legislative power to regulate the use of artificial intelligence internally means that the European Union can exercise the same competence in its external relations (limited to the portion of competence it holds); indeed, the Council states that "*the Convention should be signed on behalf of the Union as an «EU only» agreement*".

[8] In this respect, the proposed Decision says: "*The Convention should be exclusively implemented in the EU through the AI Act, which fully harmonizes the rules for the placing on the market, putting into service and use of AI systems, and other relevant Union acquis, where applicable*"; Proposal for a Council Decision on the signing, on behalf of the European Union, of the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, Brussels, 26 June 2024, COM(2024)264 final, p. 2.

[9] *Ibid*.

[10] G. De Gregorio - P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law Review*, 2/2022, pp. 473-500.

[11] G.M. Ruotolo, *Spirits in the material world: artificial intelligence act e responsabilità per la diffusione online di informazioni*, in *SIDI Blog*, 26 October 2023.

© Wolters Kluwer Italia

governance and data protection, transparency and oversight, equality and non-discrimination, digital skills and literacy. According to the Council, control mechanisms would also be compatible with EU law thanks to the creation of an enforcement system on a national level. To put it bluntly, it seems more likely that the States Parties will have more effective mechanisms because of the Regulation rather than because of the Convention itself. In summary, according to the Council "*Both the Convention and the AI Act are integral components of a regulatory approach to AI, with consistent and mutually reinforcing commitments at multiple international levels and sharing the common objective to ensure trustworthy AI*". [12]

It is also worth mentioning the UN General Assembly resolution "*Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*". [13] The latter is not a binding act, that shows the difficulty of States in finding a common ground for the regulation of artificial intelligence on a global level. It is part of a context of repeated resolutions on new technologies, indicating the need for an internationalist approach to the issue. [14]

The referred texts seem, on the one hand, to demonstrate the need for universal regulation on artificial intelligence, [15] but, on the other, they show how easier it is to achieve an agreement on particularly sensitive issues with instruments of regional nature, such as the Framework Convention. In fact, although the Member States of the Council of Europe have indeed passed a final text, prognosis on the actual scope of the treaty must be reserved until the text comes into force. For this reason, the considerations held here can only be provisional and subject to possible future revision. This does not detract from the fact that it is nonetheless necessary to account for the existence of a (not yet) binding source aimed at regulating the use of artificial intelligence, compatible with human rights, the rule of law and democracy.

In this brief paper, however, we will just provide an overview of the treaty and highlight its most seemingly critical aspects.

---

[12] COM(2024)264 final, cit., p. 4.

[13] UN. Doc. n. A/78/L.49.

[14] A. KNAUER, *The First United Nations General Assembly Resolution on Artificial Intelligence*, in *EJIL:Talk!*, 2 April 2024 (see *www.ejiltalk.org*).

[15] N. RÉBÉ, *Artificial Intelligence: Robot Law, Policy and Ethics*, Leiden, 2021.

© Wolters Kluwer Italia

2. The Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law

The Convention is the outcome of work that began in 2019, when the CAHI was established within the Council of Europe, later to become the CAI in 2022, which was responsible for drafting the text. [16] The negotiations lasted only two years and also involved many non-Member States of the Council of Europe (Australia, Canada, Costa Rica, Israel, the United States; just to name a few), [17] various representatives of civil society [18] and international organisations (European Union, UNESCO, OSCE, OECD).

The first noticeable aspect is the complementary nature of the Convention. [19] According to the chairman of the Committee on Artificial Intelligence, the aim of the negotiations would not be to enshrine new and additional individual substantial rights, but rather to ensure that already existing systems for the protection of human rights, democracy and the rule of law are adapted to artificial intelligence challenges. In other words, the willingness of States would be to bring in this area the same standards of protection provided outside the cyber context, especially for all those actions involving the use of artificial intelligence systems which are known to be potentially risky for the individual. [20]

The Convention enshrines general principles and rules that should not only safeguard human rights but, at the same time, should enable and not hinder technological development. [21] In fact, the treaty refers to the entire life cycle of an artificial intelligence system, so as not to

---

[16] C. Castets-Renard - J. Eynard, *Artificial intelligence law: between sectoral rules and comprehensive regime: comparative law*, cit., pp. 139 ff.

[17] Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CM(2024)52-addprov2, para. 3, p. 1.

[18] Explanatory Report to the Council of Europe Framework Convention, cit., par. 4, p. 1. The same happened with the General Assembly's resolution "*Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*" (78/L.49), which was strongly supported by the US-based Open AI, Anthropic, Google and Microsoft.

[19] Explanatory Report to the Council of Europe Framework Convention, cit., para. 13, p. 4.

[20] It is just worth mentioning the potential dangers posed by the creation and dissemination of false images, rather than fake news, the circulation of data and information without consent, or altered, or not corresponding to the truth.

[21] Explanatory Report to the Council of Europe Framework Convention, cit., para. 10, p. 3.

© Wolters Kluwer Italia

exclude any aspect of its use; [22] it follows that conventional obligations must be respected from the design phase to the withdrawal of the system from the market. It should be noted that no type of technology is explicitly mentioned, precisely to avoid an overly restrictive approach that would exclude the implementation of obligations to anticipate and mitigate risks associated with the use of artificial intelligence. [23]

According to the Convention, the latter should take place in compliance with the principles of fairness and non-discrimination; respect for human dignity; transparency; privacy and sharing of personal data; accountability and safe innovation. [24] In this sense, States should constantly carry out a risk assessment with respect to each system on the basis of the collection of documents defining the types of artificial intelligence; guaranteeing the possibility of lodging a complaint against decisions taken by means of artificial intelligence as well as suitable instruments against violations of human rights and fundamental freedoms caused by the use of algorithms or machines; the obligation to notify the users that they are having an interaction with artificial intelligence and not a human being. [25]

Compliance with the obligations imposed by the Convention also includes a monitoring system. [26] The treaty establishes a Conference of the Parties that assesses the actual implementation of measures and their suitability to mitigate AI-related risks by issuing recommendations to guide the action of States as well as to foster cooperation between Parties and stakeholders in the adoption of measures.

3. The potential critical aspects of the Framework Convention

3.1. *An AI definition*

As stressed, there are many aspects that deserve further investigation. First, the fact that the Convention provides a definition of artificial intelligence in Article 2 "*artificial intelligence system means a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, con-*

[22] Art. 1, para. 1, Convention.

[23] Explanatory Report to the Council of Europe Framework Convention, cit., paras. 13-14, p. 4.

[24] Arts. 6-13 Convention.

[25] See *infra*.

[26] Arts. 1, para. 3, and 23 Convention.

© Wolters Kluwer Italia

tent, recommendations or decisions that may influence physical or virtual environments". This definition is shared and accepted in many contexts. It is the same as the one adopted by the OECD in a recommendation of November 2023, [27] and was therefore chosen by the Parties, with the aim of achieving harmonised *governance* of artificial intelligence. The adoption of an unambiguous definition should also allow for a consistent national implementation of the obligations imposed by the Convention itself. It is a flexible definition that can encompass as many systems/algorithms as possible, and it is also open to the possibility of further specification by different national legislatures. The definition of artificial intelligence provided for by Article 3 (1) of the AI Act, the Regulation on artificial intelligence, is only at first glance different in content. The Article does not refer to an inference mechanism used to generate predictions or outputs resulting from machine processing, but rather to various techniques employed by the machine itself, including, however, inference (e.g. statistical inference). [28] Upon closer analysis, the two definitions appear to be aligned, and it can be noticed by the Regulation recitals. [29]

The Convention, in line with the will of the Parties, provides for a broad and flexible definition, capable of encompassing future developments of artificial intelligence systems operating techniques, which are expressly provided for by Annex I of the AI Act (which is also subject to amendments and updates). [30]

---

[27] Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449.

[28] Annex 1 to the Proposal for a Regulation of the European Parliament and of the Council, Brussels, 21 April 2021 COM(2021)206 final, available online: *www.eur-lex.europa.eu,* says: "*(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods*".

[29] "*The notion of an «AI system» as referred to in this Regulation should be clearly defined and should be closely aligned with the work of international organizations dealing with AI to ensure legal certainty, facilitate international convergence and wide acceptance, while providing for the necessary flexibility to facilitate rapid technological developments in this area*": Regulation (EU) 2024/1689, recital 12. See also COM(2024)264 final, cit., pp. 2-3.

[30] On the other hand, it is not surprising that the General Assembly's definition of artificial intelligence is even less precise and specific: UN Doc. A/78/L.49, cit., p. 2: "*artificial intelligence systems – which, for the purpose of this resolution, refers to artificial intelligence systems in the non-military domain, whose life cycle includes the*

© Wolters Kluwer Italia

3.2. *The scope of application and exceptions*

The stated objective of the Convention is to cover all activities concerning the life cycle of an algorithmic system, imposing an obligation on State authorities to assess and mitigate risks to human rights, democracy and the rule of law also with measures that directly address private parties. [31] This means that the onus is on the Parties to monitor the activities of the private party to whom they have theoretically delegated the potential risky activity. In essence, it is important that there is no deviation from the level of protection of fundamental rights provided for activities not performed with algorithmic systems or machines. To this end, the Parties are required to specify, at the time of ratification or accession, how they intend to fulfil their obligations, a declaration that can be modified at any time. According to the commentary to the Convention, [32] the declaration would be in accordance with the principle of transparency and cooperation and offers the possibility for the Parties either to apply the conventional principles or to adopt other measures that are in any case respectful of the obligations. Given that the system will be confirmed or disproved by future practice, it seems from the outset to be excessively flexible and, for this reason, scarcely effective.

Despite the high risk of affecting the entitlement of individual rights, Article 3 provides exceptions to the Parties' obligations. Firstly, artificial intelligence systems used in the national security sector are excluded from the Convention, on the assumption that such activities are, regardless of their scope, carried out with respect for human rights, democracy and the rule of law. [33] Secondly, the national defence sector is also excluded from the scope of the Convention. Thirdly, the re-

---

stages: pre-design, design, development, evaluation, testing, deployment, use, sale, procurement, operation and decommissioning, are such that they are human-centric, reliable, explainable, ethical, inclusive, in full respect, promotion and protection of human rights and international law, privacy preserving, sustainable development oriented, and responsible – have the potential to accelerate and enable progress towards the achievement of all 17 Sustainable Development Goals and sustainable development in its three dimensions – economic, social and environmental – in a balanced and integrated manner; promote digital transformation; promote peace; overcome digital divides between and within countries; and promote and protect the enjoyment of human rights and fundamental freedoms for all, while keeping the human person at the center".

[31] Art. 3 Convention.

[32] Explanatory Report to the Council of Europe Framework Convention, cit., para. 30, p. 7.

[33] Art. 3, paras. 2 and 4, Convention; see Explanatory Report to the Council of Europe Framework Convention, cit., para. 32, p. 7.

© Wolters Kluwer Italia

search sector is excluded from the scope of the Convention as well. Although both the treaty and its commentary ensure that the exceptions are not a contradiction to the principle of safe innovation, doubts about effective respect for human rights and the rule of law may remain. The exceptions specifically concern areas where the risk of subversion of the democratic regime, rather than the rule of law, is more pronounced, not to mention the violation of human rights. [34] However, it is worth remembering that even if the Framework Convention does not apply, States continue to be bound by other conventional and customary obligations that prevent the violation of individual rights or the threat to the rule of law. In contrast to the Framework Convention, the EU Artificial Intelligence Regulation does not allow for any exceptions in its application. It classifies all forms of artificial intelligence based on the risks they pose and entrusts public authorities to deal with particularly complex systems involving *cybersecurity* and public safety matters. [35]

3.3. *The complementary nature of the Convention*

A further problematic aspect of the Framework Convention concerns the obligations laid down and their wording. Chapter 2 of the Framework Convention text explicitly defines the obligations binding on the Parties: protect human rights and respect the integrity of the democratic order and the rule of law. Beyond the undoubtedly valuable content, it is worth emphasising how the norm is formulated as the agreement seems to make a mere reference to standards outside the Convention to define States' conduct. [36] Again, this approach seems to undermine the effectiveness of the agreement, which appears to be nothing more than a mere reconnaissance of the existing one. Article 4 states, in fact, that the State is obliged to respect human rights throughout the life cycle of an artificial intelligence system, due to rules of international and national law. The latter must be brought into line with the obligations imposed by the former and this also applies to

[34] Widely commented on by the doctrine is the use of autonomous weapons, with all the consequences in terms of human rights violations that this entails; on this D. Mauri, *Autonomous Weapons Systems and the Protection of the Human Person: An International Law Analysis*, Cheltenham-Northampton, Massachusetts, 2022; D. Amoroso, *Autonomous Weapons Systems and International Law*, Naples, 2020.

[35] *Passim*, an example could be Art. 65 of the Regulation.

[36] Explanatory Report to the Council of Europe Framework Convention, cit., paras. 12-13, p. 4.

© Wolters Kluwer Italia

the use of algorithms. The Convention does not create new obligations, but it reaffirms the need to uphold those already assumed elsewhere. It is no coincidence that the commentary to the agreement provides a list of all the international instruments to which States are already Parties, [37] with respect to which coordination is required. This *modus operandi* seems merely to extend existing obligations to an area where they have not yet been designed. It is therefore unconvincing, also in the light of the peculiar subject matter regulated. In other words, given the example of the right to life, it seems necessary that the same obligation dropped into the context of the cyber and algorithmic world must be appropriately specified in its limits and content. [38] On the one hand, the more flexible approach could be endorsed, considering both the difficulties of negotiation and the overly restrictive effect of applying a detailed regulation. Article 5, on the other hand, provides for the obligation to take measures to prevent the use of systems that risk subverting the "*integrity, independence and effectiveness of democratic institutions and processes, including the principle of the separation of powers, respect for judicial independence and access to justice*". The vagueness of the provision opens it up to abuse and different interpretations.

The Parties are also required to guarantee individuals' access to information and public debate, as well as the opportunity to form their own opinions. In this case, the wording of the obligation is more precise about the purpose, i.e. a non-distorting use of artificial intelligence in politics but leaves wide discretion to the Parties as to how to implement the prescribed result. States understand that the possibility of disseminating false information, with the consequent likelihood of influencing the outcome of an election or the conviction of a citizen, is the main problem associated with the use of technologies taken into consideration. However, the provision only extends the application of already existing obligations. Therefore, there remain doubts about the appropriateness of the provision, despite the greater detail compared

[37] *Id*., pp. 9-10.

[38] Against the above background, the general obligation in Article 4 of the Framework Convention requires Parties to take stock of their existing human rights obligations, frameworks and mechanisms in their domestic legal system and, in line with the approach described in Art. 1, para. 2, ensure that the existing frameworks, rules and mechanisms continue to protect and promote human rights, consistent with international human rights obligations, and are sufficient and effective to respond to the evolving artificial intelligence landscape. Explanatory Report to the Council of Europe Framework Convention, cit., p. 10.

© Wolters Kluwer Italia

to the previous article. [39] It should be noted that the AI Act adopted a different approach with respect to artificial intelligence systems applied to the management of electoral processes or for the administration of justice: they are classified as high-risk activities. [40]

3.4. *The general principles of the Convention*

The Convention goes on to list the already mentioned general principles that must govern the use of artificial intelligence. [41] The principles are followed by the remedies that must be granted to the individuals in the event of a violation of their rights. Article 14 provides not only for the obligation to guarantee free information, but also for the possibility of a remedy, again according to the rules laid down in the national law of the contracting Party. The Convention does not provide any other way by which individuals may be protected in the event of a violation of their fundamental rights, other than by lodging a complaint to the competent authorities (Article 14 Convention). On this point, it seems that the complementarity of the Convention with other existing systems of protection should have been better specified. [42] A further observation that arises here is the potential unequal treatment of individuals subjected to the jurisdiction of States with different systems, where the independence of the judiciary could be questioned: imagine the potential different outcomes between a legal challenge in France and one filed in Bulgaria or Poland. Even though these States are Members of the European Union and Members of the European Convention for the Protection of Human Rights and Fundamental Freedoms, the outcome of application could differ considerably due to the well known problems of independence of the Polish judiciary or the weak democratic system in Bulgaria. In drafting the provision, the Par-

[39] Explanatory Report to the Council of Europe Framework Convention, cit., para. 48, p. 12.

[40] The requirements for high-risk systems are listed in Art. 6 of the Regulation and are subject to strict rules of control and verification.

[41] The commentary specifies that the principles set out in the Convention must be implemented directly by the national legislator. Explanatory Report to the Council of Europe Framework Convention, cit., paras. 49-52, p. 12.

[42] On the co-existence of several mechanisms of protection, as well as on the principle of the primacy of the norm most favorable to the individual, A.A. Cançado Trinidade, *Co-Existence and Co-Ordination of Mechanisms of International Protection of Human Rights: At Global and Regional Levels*, in *Recueil des cours*, *The Hague Academy of International Law*, Dordrecht-Boston-London, 1987, pp. 114 ff.

© Wolters Kluwer Italia

ties chose to adopt the same terminology used in other human rights treaties, including Article 13 of the European Convention and Article 2 of the 1966 Covenant on Civil and Political Rights, again with the aim of emphasising the complementary nature of the Convention. The system does not seem particularly innovative, and perhaps ill-suited to countering the risks posed by artificial intelligence use. In fact, it merely ensures that fundamental rights violations caused by artificial intelligence systems follow the same course as any other human rights violation, leaving the definition of the procedures for redress and protection to national law. If the use of algorithms is indeed as problematic as it seems, then perhaps it would have been appropriate to provide for a well-defined procedure of redress that also guarantees sound expertise of the judges. It also seems to differ with the universal vocation which the Convention would appear to have since, as drafted, individuals subject to the jurisdiction of EU Member States will have a wider range of remedies available compared with a person under the jurisdiction of a non-Memeber State. Added to this the Convention provides for a *threshold*[43] that the violation must exceed; below this threshold the remedy does not seem to be guaranteed (Article 14, para. 2, Convention). The definition of the threshold is left to the discretion of the Parties, which seem to confer too much flexibility to the system.

3.5. *The monitoring system of the Convention*

Chapters 5 and 6 are devoted to risk assessment and to the implementation of Convention obligations, respectively. Article 16, which addresses the assessment of risks arising from the use of artificial intelligence, is closely connected to the principles outlined in Chapter 3 and establishes the criteria that national measures must meet in order to be considered adequate. They include the context and intended use

[43] On this point, the commentary to the Convention clarifies "*which means that (1) the relevant requirements of Articles 14 and 15 do not apply automatically to all artificial intelligence systems falling within the scope of Article 3 of the Framework Convention; (2) that the artificial intelligence systems which have no significant effect or impact on human rights do not fall within the scope of the specific new obligations in this Article; and (3) it is up to the parties of the Framework Convention to examine whether, in view of their existing international and domestic human rights law and the context and other relevant circumstances in relation to a given artificial intelligence system, such system can be said to have «significant effect» or «significant impact» on human rights*"; Explanatory Report to the Council of Europe Framework Convention, cit., para. 101, p. 22.

© Wolters Kluwer Italia

of artificial intelligence, whether preliminary tests are carried out, monitoring risks to human rights, democracy and the rule of law, and assessment of the measures impact on individuals and stakeholders. The risk assessment should also consider compliance with the principle of sustainable development, environmental protection and the benefits for society. [44] The principle of the provision is to ensure a uniform approach among all Parties, which will be required to amend their domestic legislation in accordance with the provisions of the treaty. After all, the risk assessment carried out at the design stage of a system/algorithm is fundamental for the development of the entire product in compliance with the obligations imposed by the Convention, and it will have to be followed by monitoring procedures. Article 16, para. 4, then provides that the Parties can ban any AI system "*where it considers such uses incompatible with the respect for human rights, the functioning of democracy or the rule of law*". The determination of what may be banned is reserved to each Party, with the risk of differential application from State to State. Moreover, this is a very vague criteria, which lends itself to abuse and makes the provision scarcely enforceable. Chapter 6, on the other hand, imposes further obligations on the Parties. The articles deal with the prohibition of discrimination, disability and minors and the promotion of digital knowledge. [45] It goes on to specify that what is provided for in the Convention does not compress already existing human rights and that States have the possibility of guaranteeing broader protection than that stipulated in the treaty. [46]

The follow-up mechanism established by the Convention raises several concerns, which leads one to doubt the very effectiveness of the system, especially when one considers that it is implemented in States that are not EU Members or not Party to other international law instruments for human rights protection. Article 23 provides for the establishment of a body, the Conference of the Parties (composed of the representatives of the Contracting States), responsible for monitoring the appropriateness of the measures adopted by States in the implementation of convention obligations. It would also have the function of exchanging information between the Parties, with the aim of

[44] Explanatory Report to the Council of Europe Framework Convention, cit., para. 108, p. 23.

[45] Arts. 17-20 Convention.

[46] Arts. 21-22 Convention.

© Wolters Kluwer Italia

fostering cooperation between them, and of resolving disputes.[47] The most problematic aspect concerning this body appears to be the procedure for its convocation, as it still requires a decision to be adopted by a majority of States within the Committee of Ministers, and subsequently implemented by the Secretary.[48] This excludes the possibility of influencing decisions taken by the body for States that are Parties to the agreement but not Members of the Council of Europe. The same can be said for international organisations that have ratified the Framework Convention. These Parties, however, are required to contribute[49] in a fair manner[50] to the activities of the Conference of the Parties, without clarifying its meaning or how they will financially contribute. There is also an obligation to report to the Conference within two years of its establishment, and periodically thereafter. The body itself will determine the procedures for reports submission. Even with respect to this point, this is an obligation that runs the risk of turning into a mere formality: the Convention's supervisory body, which is composed of the Member States themselves, could be scarcely independent of them, and thus be endowed with limited discretion in assessing both the fulfilment of obligations and the settlement of disputes. At the same time, the Convention does not provide for any sanctioning or coercive mechanism.

In addition to the Conference of the Parties, Article 26 envisages the obligation to establish a national monitoring mechanism that is independent and impartial of the executive and legislative branches and is responsible for monitoring compliance with the Convention obligations. The provision seems to be based on the idea that, since it is necessary to assess the measures taken under domestic law, a national body is the best solution. However, the Convention does not define its powers; it merely stipulates that it must have the necessary supervision, expertise and resources to be able to perform its function. Again, there is no mention of coercive or sanctioning instruments, which, if at all, will have to be decided by the State Party.

The provision defining the disputes settlement also raises doubts. Article 29, in fact, provides for the use of peaceful procedures, including the Conference of the Parties. There is no provision for referral to

[47] Art. 29 Convention.

[48] Art. 23, para. 3, Convention.

[49] Art. 23, para. 7, Convention.

[50] Explanatory Report to the Council of Europe Framework Convention, cit., para. 134, p. 28.

© Wolters Kluwer Italia

any previously identified court or arbitral tribunal. This leads, inter alia, to the question whether the Court of Justice of the European Union could have jurisdiction in the event of a dispute between EU Member States. The answer would seem to be affirmative, especially considering the coordination clause in Article 27 of the Convention. It provides that the Member States of the Union may continue to apply EU law in their mutual relations without prejudice to the object and purpose of the Framework Convention. Again, this is a confirmation of the idea that the Convention and the AI Act are two harmonised sources from their design.

3.6. *Territorial application*

At the end of the treaty, Article 32 permits the Parties to limit the territorial scope of the Convention, allowing States – as well as the European Union – to specify, at the time of ratification, by means of a declaration, the territories to which the Convention shall apply. The provision is part of a long tradition of similar clauses inserted in the various conventions of the Council of Europe [51] and, in part, follows Article 56 of the European Convention on Human Rights, as well as Article 52 TEU and Article 355 TFEU, [52] which specify the territo-

[51] Art. 29, Council of Europe Convention against Trafficking in Human Organs, Santiago de Compostela; Art. 12, Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, Riga; Art. 21, Council of Europe Convention on Cinematographic Co-production (revised), Rotterdam; Art. 29, Council of Europe Convention on Offences relating to Cultural Property, Nicosia; Art. 34, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg; Art. 18, Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, Strasbourg.

[52] The territory of the Faroe Islands, the United Kingdom Sovereign Base Areas of Akrotiri and Dhekelia in Cyprus are excluded ("*except to the extent necessary to ensure the implementation of the arrangements set out in the Protocol on the Sovereign Base Areas of the United Kingdom of Great Britain and Northern Ireland in Cyprus annexed to the Act concerning the conditions of accession of the Czech Republic, the Republic of Estonia, the Republic of Cyprus, the Republic of Latvia, the Republic of Lithuania, the Republic of Hungary, the Republic of Malta, the Republic of Poland, the Republic of Slovenia and the Slovak Republic to the European Union and in accordance with the terms of that Protocol;*"), as well as overseas territories that have a special relationship with the Union. While the provisions of the Treaties apply to Guadeloupe, French Guiana, Martinique, Réunion, Saint Barthélemy, Saint Martin, the Azores, Madeira and the Canary Islands. However, the regime is subject to change due to decisions taken by the European Council.

© Wolters Kluwer Italia

rial application of EU law. Given the subject matter regulated, such clarifications are of little relevance, since it is very difficult to geo-restrict an artificial intelligence system, with the consequence that it is very easy to circumvent the regime. However, it should be noted that declarations by States to territorially limit the application of a Council of Europe Convention are not a particularly large number. [53]

4. Concluding remarks

Only after the conclusion of the ratification process and the subsequent entry into force of the agreement will it be possible to make more comprehensive assessments of the actual role of the Convention with respect to the use of artificial intelligence systems and their potential risks to fundamental rights, the rule of law and democracy. As repeatedly mentioned, the treaty is distinct from the system of the European Convention, yet it recalls its principles and, above all, extends its obligations to the use of artificial intelligence.

It seems safe to say that the Convention expresses the need of some States to regulate a matter that is potentially dangerous to human rights. It contains provisions that codify principles aimed at guiding the activities of States in regulating the life cycles of artificial intelligence systems. The most interesting aspect is that it is a regional instrument with a universal vocation: it will also be open to ratification by States that are not Part of the Council of Europe, some of which were actively involved in the negotiations. This means that the obligations imposed by the Convention's rules could potentially lead to a harmonisation of the regulation of the subject matter in all the legal systems of the Parties. As regards the EU Member States, the harmonisation process has already started.

[53] The declaration to extend the application of Convention 108 to Gibraltar made in 2019 by the United Kingdom, available online: *www.coe.int*; Azerbaijan's declaration of 30 October 2023 to also apply the Council of Europe Convention against Trafficking in Human Organs (CETS No. 216) to Armenia, available online: *www.coe.int.* The same cannot be said for the *colonial clause* of Art. 56 of the European Convention, on account of which especially the United Kingdom, France and the Netherlands have made declarations, available online: *www.coe.int*; see also W.A. SCHABAS, *The European Convention on Human Rights: A Commentary*, 2015, Oxford, pp. 916 ff.

© Wolters Kluwer Italia

In conclusion, the critical issues mentioned above could undermine the effectiveness of the Convention, even though there is an obvious relationship with the AI Act.[54] However, the question remains open as to how the Convention will be implemented in the legal systems of States other than Members of the European Union. In this case, the not particularly detailed provisions and the ineffective means of control and dispute resolution raise some concerns.

[54] The Regulation, however valuable, is still lacking in some respects, for instance the Regulation of deepfake, see M. J. Block, *A Critical Evaluation of Deepfake Regulation through the AI Act in the European Union*, in *Journal of European Consumer and Market Law*, 4/2024, pp. 184-192.

© Wolters Kluwer Italia

Sezione Seconda

LEZIONI

ALGORITMI DI PREZZO E LEGGE SULL'INTELLIGENZA ARTIFICIALE: NAVIGARE IN ACQUE INESPLORATE TRA IL DIRITTO DELLA CONCORRENZA E LA REGOLAMENTAZIONE TRADIZIONALE DELLE TECNOLOGIE AUTONOME * **

ARIANNA ANDREANGELI

SOMMARIO: 1. Introduzione. – 2. Le ragioni e l'approccio alla regolamentazione dell'intelligenza artificiale: dall'intervento frammentario alla legge europea sull'intelligenza artificiale. – 2.1. Regolamentare il progresso: come affrontare l'impatto delle tecnologie autonome sull'interesse pubblico? – 2.2. Un approccio basato sul rischio alla regolamentazione dell'IA: l'idea di "IA affidabile" nell'*EU AI Act*: alcune osservazioni. – 3. Algoritmi per la determinazione dei prezzi e *AI Act*: a cavallo tra diritto della concorrenza e regolamentazione del progresso tecnologico? – 3.1. Dal prezzo discriminatorio alla determinazione dei prezzi algoritmica, dinamica e personalizzata: alcune riflessioni. – 3.2. Prezzi algoritmici, concorrenza ed equità nel mercato interno. – 3.3. Algoritmi di determinazione dei prezzi e regolamentazione dell'IA: dalla regolamentazione *ex post* a quella *ex ante* per progettazione? – 3.4. Algoritmi di determinazione dei prezzi e il concetto di intelligenza artificiale "affidabile": prospettive circa la possibile applicazione dell'*AI Act*. – 4. Prezzi algoritmici, regolamentazione dell'intelligenza artificiale e concorrenza: alcune conclusioni.

Abstract: This paper seeks to address the possible implications arising from the interaction between the EU Artificial Intelligence Act and existing legal approaches to algorithmic pricing. It will argue that while competition law remains well-placed in targeting cer-

* Contributo sottoposto a doppio referaggio in forma anonima.

** Testo rielaborato dall'Autrice a seguito della *lectio magistralis* tenutasi il 24 maggio 2024. Sentiti ringraziamenti vanno al Prof. Luigi Daniele, alla Dott.ssa Luisa Lodevole dell'Università degli Studi di Roma "Tor Vergata", al Prof. Roberto Cisotta dell'Università degli Studi di Roma "La Sapienza" e a tutti gli studenti che hanno partecipato.

© Wolters Kluwer Italia

tain forms of algorithmic collusion, its scope might reach its limits when it comes to *prima facie* collusive outcomes that can arise from the deployment of pricing algorithms which, due to their reliance on reinforcement learning, can determine prices that are increasing divorced from any "collusive plan". It will be queried whether pricing algorithms should be subjected to the generally applicable rules enacted to govern artificial intelligence more broadly. The paper will discuss the nature of algorithmic pricing in light of the "risk-based" approach at the basis of the AI Act and argue that, as pricing algorithms become increasingly autonomous and complex, especially given the nature of the data which they process, it might be necessary to consider subjecting them to *ex ante* scrutiny and to the authorisation regime enshrined in the AI Act itself.

1. Introduzione

L'intelligenza artificiale è diventata parte della vita quotidiana grazie all'espansione del commercio digitale, all'importanza dei *social media* e alla dipendenza dalle tecnologie *online*. Sono necessarie norme giuridicamente vincolanti su misura, emanate per affrontare specificamente le implicazioni dell'uso di queste tecnologie? Questo dibattito ha portato al regolamento UE 2024/1689 che stabilisce norme uniformi sull'intelligenza artificiale (noto anche come *EU AI Act*) [1]. Tuttavia, non è chiaro fino a che punto e in che modo gli algoritmi di determinazione dei prezzi rientrino nel suo campo di applicazione. Poiché grazie al commercio digitale i venditori *online* hanno accumulato quantità significative di dati sul comportamento, le preferenze e i dati demografici degli acquirenti, "*(...) applicando algoritmi a questi dati,* [essi] *possono determinare prezzi personalizzati su larga scala*" [2]. Fi-

[1] 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), in G.U.U.E. L/2024/1689 del 12 luglio 2024.

[2] V. H.S.E. ROBERTSON, *Algorithmic pricing: a competition law perspective on personalised prices*, Graz Law Working Paper, 8/2023, pp. 3-4, disponibile su: *www.papers.ssrn.com*.

© Wolters Kluwer Italia

nora, il diritto della concorrenza è stato considerato idoneo ad affrontare l'impatto degli algoritmi di prezzo, come i rischi di segmentazione dei mercati e marginalizzazione dei rivali. Tuttavia, l'emergere di sistemi più complessi e più autonomi sembra aver messo in dubbio l'idoneità di queste regole generali ad affrontare le sfide della collusione nei mercati digitali. Di conseguenza, è il momento di valutare se e in che misura sia necessaria una diversa regolamentazione.

Questo contributo cerca di affrontare le possibili implicazioni dell'interazione tra la legge europea sull'intelligenza artificiale e gli approcci giuridici alla determinazione dei prezzi algoritmici. Partendo dai pro e i contro della regolamentazione dell'intelligenza artificiale (da qui in avanti anche IA), il contributo prenderà poi in considerazione gli aspetti essenziali della legge europea sull'intelligenza artificiale. Si concentrerà poi sulla determinazione dei prezzi algoritmica e le sue conseguenze.

Sosterrà che, sebbene il diritto della concorrenza resti ben posizionato nel prendere di mira alcune forme di collusione algoritmica, la sua portata potrebbe mostrare i suoi limiti quando si tratta di risultati collusivi *prima facie* che possono derivare dal funzionamento di algoritmi. Questi ultimi, a causa della loro natura, possono determinare prezzi indipendentemente da ogni "piano collusivo". Il contributo permetterà di concludere che, poiché gli algoritmi di tariffazione diventano sempre più autonomi e complessi, soprattutto data la natura dei dati che elaborano, potrebbe essere necessario prendere in considerazione la possibilità di sottoporli ad un controllo *ex ante* e al regime di autorizzazione sancito dalla stessa legge sull'IA.

2. Le ragioni e l'approccio alla regolamentazione dell'intelligenza artificiale: dall'intervento frammentario alla legge europea sull'intelligenza artificiale

2.1. *Regolamentare il progresso: come affrontare l'impatto delle tecnologie autonome sull'interesse pubblico?*

Nei limiti di questo contributo, può dirsi che l'intelligenza artificiale sia un termine "pigliatutto"; esso indica una varietà di sviluppi tecnologici che cercano di "far fare ai *computer* il tipo di cose che le menti possono fare" [3]. Progettando algoritmi sempre più complessi,

[3] M.A. Boden, *Artificial Intelligence. A Very Short Introduction*, Oxford, 2020, p. 3.

© Wolters Kluwer Italia

i *computer* possono imitare funzioni tipicamente umane, come l'apprendimento e l'elaborazione delle informazioni raccolte dall'ambiente attraverso interfacce "*user-friendly*", che consentono agli individui di visualizzare, inserire e derivare grandi quantità di informazioni che vengono elaborate a velocità sempre più elevate da potenti unità di elaborazione e spesso senza supervisione umana [4].

È indubbio che gli agenti autonomi possano influenzare l'ambiente con cui interagiscono e possono persino incidere sui diritti degli individui, ad esempio di quegli individui di cui gli agenti elaborano i dati e le informazioni [5]. In quanto tali, quindi, essi generano rischi [6]. La regolamentazione dell'intelligenza artificiale può essere quindi giustificata da ragioni quali la certezza del diritto, le esigenze di giustizia e la necessità di responsabilità di coloro che traggono vantaggio dal suo utilizzo [7]. La domanda da porsi è come regolamentarla. Si è sostenuto che la legge conservi un certo grado di "flessibilità" che le consente, attraverso l'interpretazione, di adattarsi a nuovi fenomeni [8]. Tuttavia, la complessità dei sistemi di IA può complicare l'applicazione delle regole generali, con ricadute negative per il diritto delle vittime ad accedere alla giustizia [9].

Regolamentare una tecnologia in rapida evoluzione, la cui gamma completa di implicazioni non è facilmente comprensibile, è, però, complesso [10]. Ciò per una serie di ragioni, tra cui, l'asimmetria informativa, l'incertezza che spesso sorge in merito all'impatto delle nuove tecnologie sulla società e la necessità di bilanciare il legittimo interesse degli inventori a perseguire la loro "ricerca" per far avanzare le frontiere della conoscenza, rispetto a quelli degli individui che potrebbero essere influenzati, a volte negativamente, dall'impatto di queste innovazioni [11].

Quanto al contenuto di tale legislazione, si è sostenuto che essa si

---

[4] V., *ex multis*, T.J. SEJNOVSKI, *The unreasonable effectiveness of deep learning in artificial intelligence*, in *PNAS*, 48/2020, pp. 30033-34.

[5] G. FINOCCHIARO, *Intelligenza Artificiale: quali regole?*, Bologna, 2024, p. 32.

[6] *Id*., pp. 61-63.

[7] Cfr., *inter alia*, G. FINOCCHIARO, *Op. cit*., pp. 1-20; v. anche M. DAVIES - M. BIRTWISTLE, *Regulating AI in the UK Strengthening the UK's proposals for the benefit of people and society*, Report of the Ada Lovelace Institute, July 2023, disponibile su: *www.adalovelaceinstitute.org*, pp. 12 ss.

[8] V., *inter alia*, G. FINOCCHIARO, *Op. cit*., p. 18.

[9] *Id*., p. 2.

[10] A. TAEIHAGH - M. RAMESH - M. HOWLETT, *Assessing the regulatory challenges of emerging disruptive technologies*, in *Regulation & Governance*, 15/2021, p. 1010.

[11] G.E. MARCHANT, *The growing gap between emerging technologies and the law*,

© Wolters Kluwer Italia

debba articolare in regole sostanziali. Queste ultime sono spesso elaborate in concerto con attori non statali, come gli organismi di definizione degli *standard* tecnici [12] e procedure applicative [13]. Determinare tale regime normativo pone diversi interrogativi circa lo scopo, generale o limitato ad alcuni aspetti, e circa la necessità di assicurare la "longevità" di tali regole [14].

Alla luce di quanto sopra, si può concludere che l'emergere dell'IA ha sollevato importanti domande per i decisori politici. Nella prossima sezione verrà riassunto l'approccio adottato dall'Unione europea.

2.2. *Un approccio basato sul rischio alla regolamentazione dell'IA: l'idea di "IA affidabile" nell'*EU AI Act*: alcune osservazioni*

Va notato che l'Unione europea ha affrontato la questione della regolamentazione dell'IA con un progetto geopolitico molto chiaro, cioè, diventare la giurisdizione *leader* per lo sviluppo dell'IA che deve essere "*sicura, affidabile ed etica*" [15] e stabilire una "*sovranità digitale europea*" [16]. L'Unione ha perseguito tale piano diventando non un *leader* industriale, dato che la produzione di IA si svolge molto maggiormente in altre giurisdizioni [17], ma il capofila nell'emanazione di un "modello Europeo" di norme che diventino un punto di riferimento per altri sistemi giuridici [18].

Secondo la Strategia IA dell'Unione, le tecnologie autonome possono offrire vantaggi chiave per cittadini, aziende ed enti del settore

---

in G.E. Marchant - B.R. Allenby - J.R. Herket (eds.), *The Growing Gap between emerging technologies and ethical and legal oversight*, Berlin, 2011, pp. 19 ss.

[12] L.E. Blais - W.E. Wagner, *Emerging science, adaptive regulation and the problem of rulemaking ruts*, in *Texas Law Review*, 1701/2008, pp. 1707-1708. V. anche S. Feldstein, *Evaluating Europe's push to enact AI's regulations: how will this influence global norms?*, in *Democratization*, 5/2023, p. 24.

[13] A. Taeihagh - M. Ramesh - M. Howlett, *Op. cit*., p. 1013.

[14] H. Ruschemeier, *AI as challenge for legal regulation-The scope of application of the artificial intelligence act proposal*, in *ERA Forum*, 2023, pp. 361-363 e 366-367.

[15] Cfr. *European approach to artificial intelligence*, disponibile su: *www.digital-strategy.ec.europa.eu*; per un commento, v. G. Finocchiaro, *Op. cit*., pp. 113-114.

[16] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "*Revisione intermedia dell'attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti*", Bruxelles, 10 maggio 2017, COM(2017)228 final, p. 6, disponibile su: *www.eur-lex.europa.eu.*

[17] G. Finocchiaro, *Op. cit*., pp. 108-109.

[18] *Id*., p. 109.

© Wolters Kluwer Italia

pubblico [19]. Tuttavia, esse generano rischi. Di conseguenza, "*se le tecnologie autonome devono operare all'interno della società, dobbiamo essere in grado di fidarci che il loro comportamento*" sia conforme alle regole e alle aspettative che caratterizzano la società stessa [20]. "L'IA affidabile", quindi, deve rispettare le norme giuridiche ed etiche applicabili in una particolare società o giurisdizione, oltre che conformarsi a canoni di robustezza e affidabilità tecnica e statistica [21]. Inoltre, deve essere "spiegabile", cioè, atta ad essere accessibile agli utenti, che devono essere in grado di comprenderne lo scopo e l'impatto con i propri interessi [22] e conforme con regole sulla riservatezza dei dati personali e di non-discriminazione [23].

L'*AI Act* dell'Unione europea "traduce" questi valori in un quadro normativo applicabile in tutto il mercato interno [24] e mirante a garantire la sicurezza e la conformità di queste tecnologie con i diritti fondamentali, aumentare la certezza del diritto per gli investimenti e l'innovazione e migliorare la *governance* e l'efficacia di tali sistemi [25]. Esso stabilisce un quadro giuridico flessibile e proporzionato, basato sulla valutazione del rischio associato alle tecnologie di IA rispetto ai diritti delle persone interessate [26] e articolato in tre livelli. Il primo comprende le "tecnologie proibite", vale a dire gli usi dell'IA che sono considerati come portatori di un livello di rischio "inaccettabile" in quanto incompatibili con i "valori dell'Unione" – per esempio, sistemi che "*hanno un potenziale significativo di manipolare le persone attraverso tecniche subliminali al di là della loro coscienza*" o che possono sfruttare le vulnerabilità dei membri di gruppi già deboli [27].

---

[19] "*Libro bianco sull'intelligenza artificiale-Un approccio europeo all'eccellenza e alla fiducia*", Bruxelles, 19 febbraio 2020, COM(2020)65 final, pp. 2-3, disponibile su: *www.commission.europa.eu.*

[20] L. DENNIS - M. FISHER - M. SLAVKOVIK - M. WEBSTER, *Formal verification of ethical choices in autonomous systems*, in *Robotics and Autonomous Systems*, 2017, p. 1.

[21] *Id*., pp. 2-3.

[22] COM(2017)228 final, ult. cit.

[23] HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, *Ethics guidelines for trustworthy AI*, 8 April 2019, pp. 3-5 e 14-15, disponibile su: *www.ec.europa.eu.*

[24] V. *Excellence and trust in artificial intelligence*, disponibile su: *www.commission.europa.eu*. V. anche la proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, Bruxelles, 21 aprile 2021, COM(2021)206 final, disponibile su: *www.eur-lex.europa.eu*; cfr. anche *Memorandum*, p. 1.

[25] *Memorandum*, cit., p. 3.

[26] *Id*., pp. 3-5.

[27] *Id*., pp. 12-13.

© Wolters Kluwer Italia

Il secondo livello identifica invece gli usi dell'IA che sono considerati, sulla base di uno *screening ex ante* basato sul rischio, come portatori di un "rischio elevato" per i valori dell'Unione europea e la protezione dei diritti fondamentali. Secondo il Titolo III, essi devono essere sottoposti a una valutazione *ex ante* per quanto riguarda la loro conformità a specifici requisiti obbligatori, prima di poter essere immessi sul mercato interno. Questa valutazione si concentra sia sulla funzione del sistema autonomo sia sugli "*scopi e sulle modalità specifici*" a cui il suo adottante intende sottoporlo [28]. Una volta concessa un'autorizzazione, gli adottanti sono soggetti a obblighi iterativi per garantire la sicurezza continua del sistema, mediante l'istituzione e l'esecuzione di un sistema di gestione del rischio incentrato sull'identificazione dei rischi noti e prevedibili associati al sistema, la valutazione dei rischi associati al suo uso, processi di valutazione del rischio post-lancio e il rispetto di regole di gestione e *governance* dei dati utilizzati per l'addestramento dei sistemi. Coloro che adottano sistemi di IA sono anche responsabili per la produzione di informazioni relative a tutti questi processi e a conservarle ai fini di *audit* e supervisione umana.

Infine, il regolamento identifica "sistemi a rischi limitati", stabilendo un requisito di "trasparenza", in base al quale gli individui interessati dall'uso di questi sistemi hanno il diritto di essere informati di ciò. Inoltre, se il contenuto è generato autonomamente, deve essere chiaramente identificato come tale dal sistema [29]. Altri agenti autonomi che non presentano rischi significativi possono essere utilizzati liberamente, in quanto si è ritenuto che essi abbiano una "connessione più debole" con i diritti fondamentali [30]. L'UE, tramite l'Ufficio IA, si è impegnata nello sviluppo di Codici di condotta, contenenti regole tecniche e non vincolanti [31].

Dall'analisi precedente emerge che il nuovo regolamento disciplina tutto il ciclo di creazione di IA, dalla fase di raccolta dei dati al filtraggio e all'addestramento, alla progettazione e all'esecuzione dei sistemi. Esso è "incentrato sull'uomo" e cioè fortemente attento al rispetto dei diritti fondamentali, alla salvaguardia della dignità umana e allo scopo di ricercare il bene comune [32]. È stato però criticato per le scelte generali fatte dal legislatore europeo. È stato osservato che,

---

[28] *Ibid*.

[29] Reg. (UE) 2024/1689, cit., art. 50.

[30] L. Edwards, *Expert opinion: Regulating AI in Europe*, Report of the Ada Lovelace Institute, March 2022, p. 13-14, disponibile su: *www.adalovelaceinstitute.org*.

[31] Reg. (UE) 2024/1689, cit., 27° "considerando".

[32] S. Feldstein, *Op. cit*., pp. 5-6.

© Wolters Kluwer Italia

mentre la nozione di "intelligenza artificiale" è ampia, l'effettiva classificazione di sistemi specifici nelle diverse categorie di rischio appare rigida, sollevando così la questione se potrebbe adattarsi all'emergere di nuovi sistemi di IA [33].

Inoltre, poiché l'onere di conformità al regolamento incide su un'ampia categoria di entità, tra cui, potenzialmente, piccole e medie imprese, potrebbe esserci un rischio di sovraccaricarle e mettere così a rischio il loro incentivo a investire [34]. È stato, inoltre, osservato che l'*AI Act* non è il primo atto legislativo basato sul principio secondo cui spetta a coloro a cui sono rivolte le sue disposizioni garantire la conformità agli obblighi ivi contenuti [35]. Tuttavia, il loro contenuto sostanziale è lasciato alle norme tecniche stabilite da organizzazioni tecniche di settore [36]. Sorgono anche questioni sistemiche circa la collocazione del nuovo regolamento rispetto ad altri importanti strumenti che sono rilevanti per la disciplina dei mercati digitali, come il regolamento generale sulla protezione dei dati (GDPR), il *Digital Services Act* e il *Digital Markets Act* [37].

Si può quindi concludere che l'*AI Act* rappresenta un significativo cambiamento nel dibattito su come dovremmo regolamentare gli agenti autonomi. Tuttavia, permangono aree di preoccupazione, come l'assenza di norme esplicite per la protezione dei diritti individuali e il rischio che, poiché il quadro sancito dal regolamento è "pesante di burocrazia", potrebbe scoraggiare l'emergere dell'industria dell'IA, che l'Unione stessa vuole attrarre.

3. Algoritmi per la determinazione dei prezzi e *AI Act*: a cavallo tra diritto della concorrenza e regolamentazione del progresso tecnologico?

3.1. *Dal prezzo discriminatorio alla determinazione dei prezzi algoritmica, dinamica e personalizzata: alcune riflessioni*

Le sezioni precedenti hanno delineato le principali implicazioni

[33] G. FINOCCHIARO, *Op. cit.*, p. 120.
[34] *Id.*, pp. 121-122.
[35] *Id.*, p. 120.
[36] *Id.*, pp. 123-124.
[37] *Id.*, p. 123. V., tra gli altri, M. PATHAK, *Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act*, in *European Data Protection Law Review (EDPL)*, 1/2024, disponibile su: *www.doi.org/10.21552/edpl/2024/1/8*.

© Wolters Kluwer Italia

dell'impatto dell'IA nella società e nell'economia e hanno esplorato alcune delle sfide associate alla regolamentazione di queste nuove tecnologie. Questa sezione considera le implicazioni del regolamento sull'IA per gli algoritmi di determinazione dei prezzi. In uno studio pubblicato nel 2018, la *Competition and Markets Authority* ha mostrato che dal 2013 grandi piattaforme *online* come Amazon avevano sistematicamente implementato sistemi di determinazione dei prezzi autonomi in tutte le loro operazioni [38]. Quindi, i rivenditori *online* non solo possono eseguire fino a 2,5 milioni (secondo lo studio *CMA*, in riferimento alle operazioni di Amazon) di modifiche dei prezzi al giorno, ma anche di raccogliere volumi considerevoli di informazioni sui loro clienti [39]. Inoltre, poiché la scala e la frequenza di tali variazioni di prezzo non possono essere ottenute dagli individui, gli algoritmi di prezzo sono indispensabili per consentire ai concorrenti di "tenere il passo" [40].

Questi sistemi di IA hanno avuto un impatto pervasivo sui mercati e sulle aziende digitali, poiché sfruttano i dati basati sulle transazioni e sulle preferenze generati tramite l'interazione con consumatori *online* per reagire rapidamente alle fluttuazioni del mercato e determinare i prezzi in modo dinamico alla luce delle variazioni di domanda e offerta [41]. Inoltre, possono consentire ai singoli fornitori di ottimizzare i processi interni, fornendo efficaci meccanismi di monitoraggio dei costi [42]. La "discriminazione di prezzo", cioè lo stabilire prezzi diversi per la medesima transazione commerciale, è di varie forme. Quella "di primo grado" si verifica quando un prezzo viene determinato per ciascun acquirente sulla base del suo prezzo di riserva individuale, in altre parole, in correlazione diretta con la sua disponibilità a pagare; la discriminazione di "secondo grado" si verifica invece quando i prez-

---

[38] CMA-Competition and Markets Authority, *Pricing algorithms. Economic working paper on the use of algorithms to facilitate collusion and personalised pricing*, October 2018, pp. 17-18, disponibile su: *www.assets.publishing.service.gov.uk.*

[39] *Id*., p. 17.

[40] *Id*., p. 18. V. anche Q. Wang - Y. Huang - P. Vir Singh - K. Srinivasan, *Algorithms, artificial intelligence and simple rule-based pricing*, 14 April 2023, pp. 5-6, disponibile su: *www.ssrn.com.*

[41] P. Van Cleynenbruegel, *Pricing algorithms and antitrust enforcement: sandboxes to the rescue?*, CPI Antitrust Chronicle, February 2024, p. 3, disponibile su: *https://orbi.uliege.be.* V. anche CMA-Competition and Markets Authority, *Pricing algorithms*, cit., p. 20.

[42] V. tra gli altri, Organisation for Economic Co-operation and Development (OECD), *Executive Summary of the Roundtable on Algorithmic Competition*, 8 November 2023, p. 3, disponibile su: *www.one.oecd.org*.

© Wolters Kluwer Italia

zi vengono determinati sulla base della quantità di prodotti acquistati [43]. La discriminazione di "terzo grado", forse la più comune, comporta la definizione di prezzi diversi per ogni categoria di consumatori, raggruppati in base a "caratteristiche osservabili" [44].

Da una prospettiva etica, si è sostenuto che la pratica suddetta sarebbe intrinsecamente "ingiusta", in quanto consente al venditore di "selezionare i propri clienti" sulla base di variabili spesso non economiche, incompatibilmente con i principi di parità di trattamento [45]. Per quanto riguarda le implicazioni economiche, queste pratiche possono verosimilmente determinare prezzi sovra-competitivi in mercati con caratteristiche specifiche, come l'esistenza di una posizione di potere di mercato, sia a causa dell'elevata concentrazione o della differenziazione molto significativa del prodotto che della limitata trasparenza per quanto riguarda le informazioni a disposizione dei consumatori, che si traducono in inerzia e incapacità di adottare comportamenti in grado di controbilanciare l'impatto negativo della tariffazione personalizzata [46]. Inoltre, è stato osservato che la combinazione di dati riguardanti le caratteristiche di gruppi di consumatori e il loro comportamento di consumo aggregato sono rilevanti nella valutazione dell'impatto dei prezzi [47].

La determinazione dei prezzi personalizzata nei mercati competitivi rispetto a quelli monopolistici pare che abbia implicazioni meno chiare. Nei mercati in cui esiste concorrenza, i prezzi sembrano inferiori al prezzo di riserva massimo degli acquirenti interessati, anche con una discriminazione di prezzo in atto [48], probabilmente a causa del

---

[43] Cfr., *ex multis*, I. GRAEF, *Algorithms and Fairness: What Role for Competition Law in Targeting Price Discrimination towards Ends Consumers*, in *Columbia Journal of European Law*, 3/2018, p. 543; v. anche W. SAUTER - H. VEDDER, *Anti-competitive discrimination by digital platforms*, in *European Competition Law Review*, 3/2023, p. 89.

[44] W. SAUTER - H. VEDDER, *Op. cit*., p. 89.

[45] J.M. ELEGIDO, *The Ethics of Price Discrimination*, in *Business Ethics Quarterly*, 4/2011, pp. 634-636.

[46] H. VARIAN, *Price discrimination*, in R. SCHMALENSEE - R. WILLIG (eds.), *Handbook of Industrial Organisation*, vol. I, Amsterdam, 1989, pp. 597-600.

[47] J.P. DUBÉ - S. MISRA, *Personalised pricing and consumer welfare*, in *Journal of Political Economy*, 1/2023, pp. 135-136. V. anche D. BERGEMANN - B. BROOKS - S. MORRIS, *The limits of price discrimination*, in *American Economics Review*, 3/2015, pp. 924-925; S. COWAN, *Third-degree price discrimination and consumer surplus*, in *Journal of Industrial Economics*, 2/2012, pp. 342-343.

[48] D. ULPH - N. VULKAN, *Electronic Commerce and Competitive First-Degree Price Discrimination*, Discussion Papers, University of Bristol, Department of Economics, 2000, pp. 11-12, disponibile su: *www.citeseerx.ist.psu.edu.*

© Wolters Kluwer Italia

comportamento di consumatori più informati, che sono pertanto capaci di "contrastare" l'azione dei venditori cercando un prodotto concorrente [49].

Alla luce del diritto della concorrenza, in particolare l'art. 101 TFUE, accordi, decisioni di associazioni di imprese o pratiche concordate che hanno come oggetto o effetto l'applicazione di "*condizioni dissimili per prestazioni equivalenti con altre parti, ponendole così in una situazione di svantaggio concorrenziale*" sono incompatibili con i principi del mercato interno [50]. Analogamente, l'art. 102 TFUE mette al bando la stessa pratica se adottata da un'impresa dominante, a condizione che la differenziazione comporti uno "*svantaggio concorrenziale*" subito da "*altre parti*" [51]. La giurisprudenza della Corte di giustizia suggerisce che l'esistenza di uno svantaggio concorrenziale è fondamentale per valutare la legalità di prezzi discriminatori [52].

È indispensabile valutare l'impatto della differenziazione dei prezzi sugli "*interessi dell'operatore a cui sono state applicate tariffe più elevate rispetto ai suoi concorrenti*" e la probabilità che la società dominante possa perseguire una "*strategia volta a escludere dal mercato a valle uno dei suoi partner commerciali*". La pratica della discriminazione dei prezzi è stata inoltre ritenuta incompatibile con l'art. 101 TFUE, in quanto può comportare la segmentazione del mercato interno dell'Unione e l'esclusione di gruppi specifici di clienti. È stato rilevato che limitare l'applicazione di prezzi specifici solo alle vendite effettuate in uno specifico Stato membro renderebbe probabilmente meno attraenti per i grossisti le importazioni da e per altre parti del mercato interno, determinando così la sua segmentazione sui confini nazionali [53].

Si può concludere che l'applicazione di prezzi diversi a transazio-

---

[49] *Id*., p. 11.

[50] Decisione della Commissione 2001/791/CE, dell'8 maggio 2001, relativa ad un procedimento a norma dell'articolo 81 del trattato CE, sui casi: IV/36.957/F3 *Glaxo Wellcome* (notifica), IV/36.997/F3 *Aseprofar e Fedifar* (denuncia), IV/37.121/F3 *Spain Pharma* (denuncia), IV/37.138/F3 *BAI* (denuncia) e IV/37.380/F3 *EAEPC* (denuncia), in G.U.C.E. L302 del 17 novembre 2001, pp. 1-43, par. 115 e 118-119.

[51] C. giust. UE, 19 aprile 2018, C-525/16, *MEO-Serviços de Comunicações e Multimédia SA*, par. 29-31.

[52] C. giust. UE, *MEO-Serviços de Comunicações e Multimédia SA*, cit., par. 31-32. V. C. giust. CE, 5 dicembre 1996, C-267/95 e C-268/95, *Merck e altri*, par. 45-47 e 49; Trib. CE, 6 luglio 2000, T-62/98, *Volkswagen* c. *Commissione*, par. 8, 16, 17 e 176-179.

[53] V. C. giust. CE, *Merck e altri*, cit., par. 45-47 e 49; Trib. CE, *Volkswagen* c. *Commissione*, cit., par. 8, 16, 17 e 176-179.

© Wolters Kluwer Italia

ni simili solleva importanti questioni. In termini economici, questa pratica ha effetti ambigui sui mercati e sui consumatori. Dal punto di vista legale, è stato dimostrato che è improbabile che queste pratiche siano compatibili con gli artt. 101 e 102 TFUE, in quanto possono portare alla segmentazione del mercato interno e distorcere la concorrenza tra il cliente interessato e i rivali di quest'ultimo [54].

3.2. *Prezzi algoritmici, concorrenza ed equità nel mercato interno*

La sezione precedente ha delineato alcune delle implicazioni della discriminazione dei prezzi e in particolare dei prezzi personalizzati. Questa sezione considera l'impatto dei prezzi algoritmici sui mercati digitali. L'espansione dell'*e-commerce* e l'interazione con fattori tecnologici consentono ai rivenditori di accedere a un tesoro di informazioni sul comportamento degli acquirenti che possono essere codificate ed elaborate in tempo reale [55]. La determinazione dei prezzi algoritmica "*utilizza l'impronta digitale elettronica di un potenziale acquirente [...] per valutare la probabilità che si tiri indietro se il prezzo è alto. Se il cliente sembra sensibile al prezzo, ottiene un affare; se non lo è, paga un premio*" [56].

Gli algoritmi basati su metodi di apprendimento rinforzato sono adatti alla personalizzazione, poiché possono determinare e adattare in modo iterativo il processo di determinazione dei prezzi, alla luce degli stimoli che ricevono dal mercato in cui vengono lanciati [57]. Se il loro obiettivo è ottenere il massimo profitto possibile, l'algoritmo osserverà il risultato della sua interazione con l'ambiente esterno (ad esempio adottando un prezzo più alto di quello originariamente determinato) e invertirà la sua azione o la ripeterà se il risultato raggiunto, ovvero il raggiungimento di uno *status* diverso, rispettivamente si traduce in una perdita o in un aumento dei ricavi [58].

---

[54] Cfr., *inter alia*, W. SAUTER, *Discrimination of consumers in EU competition law*, *in European Competition Law Review*, 11/2019, pp. 514-515.

[55] Cfr., *inter alia*, CMA-COMPETITION AND MARKETS AUTHORITY, *Pricing algorithms* cit., p. 14-15. V. anche P. SEELE - C. DIERKSMEIER - R. HOFSTETTER - M.D. SCHULTZ., *Mapping the Ethicality of Algorithmic Pricing: A Review of Dynamic and Personalized Pricing*, in *Journal Business Ethics*, 2021, p. 698.

[56] P. KRUGMAN, *Reckonings; Why price fairness?*, in *New York Times*, 4 October 2000, p. 35.

[57] *Ibid*.

[58] CMA-COMPETITION AND MARKETS AUTHORITY, *Pricing algorithms*, cit., pp. 11-12.

© Wolters Kluwer Italia

Si è suggerito che tali algoritmi possano aumentare i rischi di collusione in mercati concentrati e relativamente trasparenti, con prodotti omogenei e clienti incapaci di esercitare pressione sui fornitori [59]. L'algoritmo può essere utilizzato come strumento per eseguire un piano collusivo concordato in precedenza [60]. In questo caso, esso è irrilevante per la valutazione giuridica della pratica in questione, che sarà giudicata alla luce delle norme sulla concorrenza applicabili (nell'Unione l'art. 101 TFUE), sebbene sia molto probabile che abbia reso la sua esecuzione molto più rapida [61].

Tuttavia, più complessi diventano gli algoritmi, più complessa diventa questa indagine [62]. Nel caso *Eturas* la Corte di giustizia dell'Unione europea ha dovuto occuparsi di una cospirazione *hub and spoke*, cioè un accordo in base al quale un "centro nevralgico" determinava un comportamento uniforme a cui due o più aziende dovevano attenersi, senza necessariamente che vi fosse un contatto diretto tra ciascuna di esse [63]. L'*hub* era, tuttavia, un sistema autonomo che gli utenti di una piattaforma digitale alberghiera avevano accettato di utilizzare e il cui compito era determinare i prezzi, la disponibilità e l'entità degli sconti [64].

Il fatto che un sistema centralizzato utilizzato da diversi *tour operators* avesse inviato un messaggio che limitava gli sconti che potevano essere offerti da ciascun utente che aveva poi provveduto a implementare tale messaggio o almeno non vi aveva sollevato obiezioni è stato ritenuto sufficiente a costituire una violazione dell'art. 101 TFUE [65]. Pertanto, il caso *E-Turas* dimostra come, anche in assenza

---

[59] Cfr., *inter alia*, M. Gal, *Algorithmic facilitated coordination*, Roundtable on Algorithms and Collusion, OECD Competition Committee, 21-23 June 2017, pp. 3-4, disponibile su: *www.one.oecd.org.* V. anche G. Stigler, *A Theory of Oligopoly*, in *Journal of Political Economy*, 1964, pp. 46-48.

[60] M. Ezrachi - A. Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-driven Economy*, Cambridge, Massachusetts, 2018, pp. 29-31.

[61] *Ibid*.; v. anche, *mutatis mutandis*, United States District Court for the Northern District of California, 6 April 2015, *US v. David Topkins*; patteggiamento approvato il 30 aprile 2015, disponibile su: *www.justice.gov.*

[62] M. Ezrachi - A. Stucke, *Algorithmic collusion: problems and countermeasures*, Roundtable on Algorithms and Collusion, OECD Competition Committee, 21-23 June 2017, pp. 4 e 23-24, disponibile su: *www.one.oecd.org.*

[63] C. giust. UE, 21 gennaio 2016, C-74/14, *Eturas*; v. M. Ezrachi - A. Stucke, *Virtual Competition*, cit., p. 28-29. V. anche la decisione della Commissione 86/399/CEE, del 10 luglio 1986, relativa ad una procedura d'applicazione dell'articolo 85 del trattato CEE (IV/31.371 - *Rivestimenti bitumati*), in G.U.C.E. L232 del 19 agosto 1986, pp. 15-33.

[64] C. giust. UE, *Eturas*, cit., par. 26.

[65] *Id*., par. 28-29 e 49-50.

© Wolters Kluwer Italia

di un accordo preventivo sull'adozione di singole forme di comportamento anticoncorrenziale, il fatto che quest'ultimo sia determinato in un modo che ciascuna parte accetta come "matrice" per il proprio comportamento tariffario sarebbe sufficiente a comportare l'applicazione delle norme sulla concorrenza [66].

Mentre non tutti i mercati *online* sono suscettibili di collusione algoritmica [67], l'abbondanza di dati digitalizzati riguardanti prezzi, condizioni commerciali e, dal lato della domanda, il comportamento di acquisto dei consumatori facilita gli operatori storici nel tentativo di monitorarsi a vicenda [68], replicare il proprio comportamento e sanzionare qualsiasi deviazione [69]. Questi sistemi consentono quindi alle imprese di reprimere qualsiasi incentivo a competere per la quota di mercato [70]. Va anche osservato che nelle industrie digitali, dove il controllo sui dati è centrale per le dinamiche di mercato, è probabile che i potenziali entranti affrontino ulteriori barriere all'ingresso poiché non hanno accesso alle informazioni di mercato su cui si basano gli algoritmi [71].

Come è stato brevemente ricordato, gli algoritmi di prezzo stanno diventando sempre più autonomi. Secondo Ezrachi e Stucke, uno scenario potrebbe essere caratterizzato dal fatto che ogni concorrente abbia adottato un algoritmo per stabilire i prezzi senza necessariamente aver accettato di utilizzarlo al pari di concorrenti (o forse senza saperlo) e che tale algoritmo apprenda il comportamento "andando per tentativi" [72], cioè sulla base dell'osservazione del proprio impatto su un ambiente dinamico, basandosi su "*tecniche statistiche e metodi di programmazione dinamica per stimare l'utilità di intraprendere azioni*" in circostanze mutevoli [73]. È quindi legittimo chiedersi se l'uso ripetuto di questi algoritmi da parte di una varietà di imprese concorrenti tra loro potrebbe facilitare la determinazione di prezzi apparentemente collusivi [74].

È stato dimostrato che in un mercato simmetricamente duopolisti-

---

[66] M. EZRACHI - A. STUCKE, *Virtual Competition*, cit., pp. 73-74.

[67] V., *inter alia*, G. STIGLER, *Op. cit*., loc. ult. cit.

[68] M. EZRACHI - A. STUCKE, *Virtual Competition*, cit., p. 52.

[69] *Id*., pp. 13 e 122-123.

[70] *Ibid*.; v. anche, *inter alia*, L.P. KAELBLING - M.L. LITTMAN - A.W. MOORE, *Reinforcement learning: a survey*, in *Journal of Artificial Intelligence*, 4/1996, pp. 237-238.

[71] M. GAL, *Op. cit*., pp. 4-7.

[72] Cfr., *inter alia*, L.P. KAELBLING - M.L. LITTMAN - A.W. MOORE, *Op. cit.*, pp. 237-238.

[73] *Ibid*.

[74] V., *ex multis*, M. GAL, *Op. cit*., p. 8.

© Wolters Kluwer Italia

co, in cui i membri del duopolio utilizzano algoritmi di determinazione dei prezzi relativamente semplici, questi ultimi impareranno nel tempo a colludere, fissando prezzi al di sopra dei livelli competitivi [75]. Mentre la probabilità di collusione diminuisce con l'aumentare del numero di imprese concorrenti, può rimanere particolarmente "ostinata" se ci sono tre o quattro concorrenti, in quanto questi ultimi possono rilevare le deviazioni e punire coloro che ne sono responsabili [76].

È quindi legittimo chiedersi come il diritto della concorrenza possa affrontare tali quesiti. Poiché non vi è alcuna prova di "contatto" tra rivali, la scelta di utilizzare questi tipi di algoritmi è molto probabile che risponda a una "strategia egoistica" [77]. Tuttavia, ciò non sembra escludere che, soprattutto quando si progetta l'algoritmo, un'impresa potrebbe aver tenuto conto del fatto che altri rivali potrebbero fare lo stesso e che la strategia vincente sarebbe quella di garantire la massimizzazione del profitto [78]. Di conseguenza, è stato sostenuto che a causa dell'implementazione di algoritmi di apprendimento per rinforzo, "*il parallelismo consapevole avviene [...] a livello di sistema*", senza che vi sia alcuna interazione tra rivali, la responsabilità non può essere esclusa. È stato suggerito che, se si potesse dimostrare che le imprese interessate erano a conoscenza dell'uso diffuso di algoritmi di determinazione dei prezzi sul mercato interessato e quindi avrebbero potuto prevedere che ciò avrebbe potuto aumentare la trasparenza, non avrebbero dovuto evitare la responsabilità per violazione dell'art. 101 [79]. Su quale base, però, non è del tutto chiaro.

Secondo la Corte di giustizia, una pratica concordata, ad esempio, si verifica quando due o più imprese rinunciano ai vantaggi della concorrenza per la tranquillità dell'adozione di prezzi uniformi, anche se il mercato è così caratterizzato da portare a livelli di prezzo più bassi, in assenza di tale comportamento [80]. È stato affermato che ciascuna im-

---

[75] E. Calvano - G. Calzolari - V. De Nicolò - S. Pastorello, *Artificial Intelligence, algorithms and collusion*, in *American Economic Review*, 10/2020, pp. 3268-3269.

[76] *Id*., p. 3268. Per un esame della questione relativamente a mercati non digitali, v., tra gli altri, S. Assad - R. Clark - D. Ershov - L. Xu, *Algorithmic pricing and competition: empirical evidence from the German retail gasoline market*, in *Journal of Political Economy*, 3/2024, pp. 727-728; cfr. anche M. Gal, *Op. cit*., pp. 5-7.

[77] M. Ezrachi - A. Stucke, *Virtual Competition*, cit., pp. 64-65.

[78] *Ibid*.

[79] *Ibid*.

[80] Cfr., *ex multis*, F. Ghezzi - M. Maggiolino, *Bridging EU concerted practices with US concerted action*, in *Journal of Competition Law & Economics*, 3/2014, pp. 653 ss.

© Wolters Kluwer Italia

presa può tenere conto di come gli altri stiano agendo e determinare di conseguenza la propria condotta, anche tenendo conto di ciò che un concorrente ha deciso di fare [81]. Tuttavia, questa deve essere una scelta indipendente, in assenza di qualsiasi scambio di informazioni, anche se non in segreto [82].

È riconosciuto che in alcuni mercati l'adozione di prezzi uniformi nel tempo è quasi un risultato scontato quando i mercati sono intrinsecamente oligopolistici e l'ampia circolazione di informazioni relative alla domanda e all'offerta è inevitabile a causa di fattori indipendenti dai rivali [83]. È dunque legittimo chiedersi se l'uso diffuso di prezzi autonomi abbia trasformato ogni rivale in un "agente prevedibile" e possa giustificare la conclusione che è stata commessa un'infrazione dell'art. 101 TFUE [84].

Alla luce di quanto sopra, si può concludere che ci si possa aspettare un crescente grado di trasparenza sui mercati digitali. Tuttavia, questo risultato solleva problemi rilevanti, in quanto lascia ben poco spazio per considerazioni di tutela dei consumatori e della concorrenza.

3.3. *Algoritmi di determinazione dei prezzi e regolamentazione dell'IA: dalla regolamentazione* ex post *a quella* ex ante *per progettazione?*

La sezione precedente ha delineato alcuni dei problemi derivanti dall'impatto dell'IA sui mercati e si è concentrata sulle implicazioni degli algoritmi di determinazione dei prezzi per la continua competitività delle industrie digitali. È stato osservato che l'art. 101 TFUE potrebbe rivelarsi efficace nell'affrontare i prezzi collusivi derivanti dall'uso di agenti autonomi come "strumento" per l'esecuzione di un piano di cooperazione precedentemente concordato o come "centro nevralgico" di una struttura di uso comune, come una piattaforma.

---

[81] C. giust. CE, 14 luglio 1972, 48/69, *ICI* c. *Commissione*, par. 118.

[82] *Ibid*., par. 116.

[83] C. giust. CE, 31 marzo 1993, C-89/85, C-104/85, C-114/85, C-116/85, C-117/85 e C-125/85-C-129/85, *Ahlstrom e altri* c. *Commissione*, par. 64, 101 e 126. V. C. giust. CE, *ICI* c. *Commissione*, cit., par. 118, e F. GHEZZI - M. MAGGIOLINO, *Op. cit*., pp. 652-654.

[84] M. EZRACHI - A. STUCKE, *Virtual Competition*, cit., pp. 61-62. V. anche G. COLANGELO, *Artificial Intelligence and Anticompetitive Collusion: From the "Meeting of Minds" Towards the "Meeting of Algorithms"?*, TTLF Stanford Law School Working Paper No. 74, in M. EBERS - C. PONCIBÒ - M. ZOU (eds.), *Contracting and Contract Law in the Age of Artificial Intelligence*, Oxford, 2022, p. 10, disponibile su: *www.ssrn.com.*

© Wolters Kluwer Italia

Come si può difendere la concorrenza sui mercati digitali quando l'impatto combinato della continua accumulazione di dati e degli algoritmi di determinazione dei prezzi accresca la trasparenza sui mercati e il rischio di collusione? Come si è già detto, tale scenario mette in crisi le strutture regolamentari e di *enforcement*, che sono state pensate per mercati non digitali [85]. È lecito chiedersi se sia venuto il momento di riconsiderare i concetti giuridici delle regole della concorrenza. In alternativa, si potrebbe pensare a cambiare totalmente metodo di regolamentazione dei mercati digitali, passando da un approccio *ex-post* a uno *ex-ante* [86].

È stato suggerito che, se sussistono sospetti di collusione algoritmica, il codice dell'algoritmo di determinazione dei prezzi dovrebbe essere esaminato nella sua progettazione e nel suo funzionamento. Se questo esame rivelasse che l'algoritmo ha determinato un prezzo "*condizionato [...] sui prezzi passati di un'azienda rivale*" in modo da "*premiare o punire*" uno dei concorrenti per l'essersi, rispettivamente, allineato o discostato dal prezzo determinato dagli altri rivali, allora l'algoritmo porterebbe probabilmente a un livello di prezzi che approssima un esito collusivo [87]. Tuttavia, un metodo di "*analisi che identificherà sempre correttamente la cattiva condotta*" di un agente autonomo esclusivamente sulla base del codice sorgente e dei dati di *input* non è disponibile [88].

Per far fronte a tale difficoltà, è stato suggerito che i progettisti di algoritmi di prezzo debbano essere obbligati a ideare un sistema che permetta la supervisione *ex post* del processo che ha portato a un *output* specifico da un *set* di dati di *input* noti [89]. Questo requisito, pur non richiedendo la piena trasparenza, fornirebbe un metodo sufficientemente affidabile per verificare che i prezzi non siano stati determinati in un modo che imitasse dinamiche collusive [90].

In base a quanto detto finora, appare evidente che vi siano forti argomenti in favore dell'introduzione di una regolamentazione *ex ante*

---

[85] B. Ong, *The applicability of Article 101 TFEU to algorithmic horizontal pricing practices: two conceptual frontiers*, in *International Review of Intellectual Property and Competition Law (ICC)*, 2021, pp. 209-210.

[86] *Id*., p. 210.

[87] J.E. Harrington, *Developing competition law for collusion by artificial agents*, in *Journal of Competition Law and Economics*, 3/2018, pp. 350-351.

[88] D.R. Desai - J.A. Kroll, *Trust but verify: a guide to algorithms and the law*, in *Harvard J of Law and Technology*, April 2017, p. 34.

[89] *Id*., pp. 35-36.

[90] *Id*., pp. 38 e 40-42.

© Wolters Kluwer Italia

per i sistemi autonomi destinati alla determinazione dei prezzi. Tale regolamentazione dovrebbe imporre requisiti di progettazione che consentano uno scrutinio *ex post* degli algoritmi [91] tramite la raccolta delle "*prove necessarie per [...] la [...] valutazione*" del funzionamento di tali sistemi [92], cosicché sia possibile controllare che essi "*funzionino correttamente ed entro i limiti stabiliti dalla legge*" [93].

Si può quindi concludere che, con l'espansione dell'uso degli algoritmi di determinazione dei prezzi e la loro crescente complessità, diventa necessario considerare meccanismi alternativi al tradizionale controllo *ex post* che il diritto della concorrenza permette [94]. Tuttavia, tali requisiti possono essere stabiliti solo grazie a una nuova regolamentazione *ex ante*, incentrata sulla progettazione del sistema.

3.4. *Algoritmi di determinazione dei prezzi e il concetto di intelligenza artificiale "affidabile": prospettive circa la possibile applicazione dell'*AI Act

Le sezioni precedenti hanno illustrato alcuni dei problemi derivanti dall'impiego degli algoritmi di determinazione dei prezzi sui mercati digitali, sostenendo che, a causa dell'espansione del ruolo di queste tecnologie e della loro crescente complessità e autonomia, potrebbe essere necessario considerare l'imposizione di norme generali afferenti al *design* di tali algoritmi per consentirne uno scrutinio *ex post*.

Come discusso in precedenza, l'*AI Act* dell'Unione stabilisce un approccio basato sul rischio applicabile ai sistemi di IA, al fine di, da un lato, garantire che queste nuove tecnologie possano essere considerate affidabili da coloro la cui posizione giuridica sia interessata dal loro utilizzo e, dall'altro, incoraggiare gli investimenti nel loro sviluppo. A uno sguardo più attento, tuttavia, seppur con un'eccezione molto limitata, gli algoritmi di determinazione dei prezzi, non sono considerati come portatori di un "rischio elevato" per i valori dell'Unione. Deve riconoscersi che, sebbene molti algoritmi di determinazione dei prezzi non influenzino in maniera apprezzabile l'osservanza di tali garanzie per l'individuo, in alcuni casi tali sistemi autonomi sono impiegati in contesti "rivolti all'acquirente" [95] e possono quindi in-

[91] *Id*., pp. 42-43 e 48-49.
[92] *Id*., pp. 50-51.
[93] *Id*., p. 64.
[94] J.E. HARRINGTON, *Op. cit*., p. 351.
[95] V., *inter alia*, M. GAL, *Op. cit*., pp. 6-7.

© Wolters Kluwer Italia

fluenzare il rispetto dei suoi diritti, ad esempio il diritto alla *privacy* [96]. È dunque legittimo chiedersi se la determinazione dei prezzi algoritmica possa essere considerata una forma di "IA affidabile" [97].

Si può sostenere che l'IA possa avvantaggiare gli acquirenti, riducendo i costi di ricerca e facilitando il confronto dei prezzi [98]. Inoltre, è stato già osservato che alcune forme di collusione algoritmica possono essere efficacemente affrontate tramite l'applicazione delle norme sulla concorrenza [99]. Tuttavia, quando la probabilità di prezzi paralleli o collusivi *prima facie* diventa quasi una "caratteristica" insita nel sistema di IA, ogni impresa che adotta algoritmi di prezzo diventa "prevedibile" nel proprio comportamento sul mercato agli occhi dei propri rivali che si affidano a sistemi simili [100].

È dunque lecito domandarsi se l'*AI Act* possa colmare questa apparente "lacuna" delle norme sulla concorrenza. È stato osservato che gli algoritmi per la determinazione dei prezzi sono considerati in genere come aventi un rischio basso o minimo [101]. Tuttavia, la discussione precedente ha indicato che l'impatto degli algoritmi di determinazione dei prezzi nei mercati digitali può essere estremamente significativo e potenzialmente avverso alla concorrenza e alla protezione dei dati personali. È, inoltre, molto difficile identificare una categoria uniforme di algoritmi di determinazione dei prezzi [102].

Va ricordato che l'affidabilità dell'IA richiede che le tecnologie autonome siano "lecite", cioè conformi a tutte le leggi e i regolamenti applicabili; etiche, cioè coerenti con i principi e i valori morali su cui si basa l'Unione; e infine, "robuste", nel senso che queste tecnologie devono essere progettate in modo solido e operativamente resilienti [103].

---

[96] Ipsos - London Economics - Deloitte consortium, *Consumer market study on online segmentation through personalised pricing/offers in the European Union*, Final report commissioned by the European Commission, June 2018, p. 255, disponibile su: *www.commission.europa.eu.*

[97] Reg. (UE) 2024/1689, cit., 58° "considerando"; v. anche Protocollo n. 3, punto 5(c).

[98] Dec. 86/399/CEE, cit., par. 154. V. anche Ipsos - London Economics - Deloitte consortium, cit., pp. 124-125.

[99] C. giust. UE, *Eturas*, cit.; v. M. Ezrachi - A. Stucke, *Virtual Competition*, cit., pp. 28-29.

[100] M. Ezrachi - A. Stucke, *Virtual Competition*, ult. cit.

[101] Reg. (UE) 2024/1689, cit., 58° "considerando".

[102] Z. Li, *Affinity-based algorithmic pricing: a dilemma for EU data protection law*, in *Computer Law and Security Review*, 2022, pp. 6-7.

[103] High-Level Expert Group on Artificial Intelligence, *Ethics guidelines for trustworthy AI*, cit., p. 5.

© Wolters Kluwer Italia

In questo contesto, si sostiene che la nozione di "IA lecita" possa essere interpretata in modo ampio e alla luce di una chiara distinzione tra "*standard legali [...], requisiti etici e* [standards] *tecnici volontari*" [104]. Mentre questi ultimi non sono vincolanti, la loro osservanza è in gran parte guidata dal mercato, i requisiti afferenti più propriamente alla "legalità" di sistema sono "obbligatori" e possono essere applicati "nel contesto di un sistema di istituzioni e norme" [105]. Su tale base, può ritenersi, che il requisito che l'IA sia "legale" dia "forza" al concetto di IA affidabile [106]. Gli *standard* di protezione del diritto alla *privacy* forniscono un importante parametro rispetto al quale dovrebbe essere testata la liceità delle tecnologie autonome [107]. Tuttavia, non sono le uniche norme di diritto sostanziale rilevanti. Si ritiene che il diritto della concorrenza debba essere considerato come ugualmente applicabile [108], data la sua centralità nei Trattati e della sua importanza come valore costituzionale della UE [109].

Se però la nozione di "legalità" dell'IA può e deve essere interpretata conformemente ai principi di concorrenza [110], bisogna chiedersi se l'*EU AI Act* possa affrontare l'impatto negativo che gli algoritmi di determinazione dei prezzi potrebbero avere sull'apertura e la rivalità dei mercati digitali. Si sostiene che l'uso sempre più pervasivo di questi sistemi, la loro crescente complessità e autonomia potrebbero creare rischi per la concorrenza nei mercati digitali che l'applicazione *ex post*

---

[104] A. JABŁONOWSKA - M. KUZIEMSKI - A.M. NOWAK - H.W. MICKLITZ - P. PAŁKA - G. SARTOR, *Consumer Law and Artificial Intelligence: Challenges to the EU Consumer Law and Policy Stemming from the Business' Use of Artificial Intelligence - Final report of the ARTSY project*, EUI Department of Law Research Paper No. 2018/11, p. 10, disponibile su: *www.ssrn.com*.

[105] *Ibid*.

[106] A. JABŁONOWSKA - M. KUZIEMSKI - A.M. NOWAK - H.W. MICKLITZ - P. PAŁKA - G. SARTOR, ult. cit.

[107] G. MALGIERI - F. PASQUALE, *Licensing high-risk artificial intelligence: Toward ex ante justification for a disruptive technology*, in *Computer Law & Security Review*, 2024, pp. 2, 7-8 e 11-12.

[108] *Inter alia*, C. WENDERHORST - J. HIRTELNEHMER, *Outlook on the future regulatory requirements for Artificial Intelligence in Europe*, 2022, pp. 2 e 28-29, disponibile su: *www.papers.ssrn.com.*

[109] Protocollo n. 27 sul mercato interno e sulla concorrenza, in G.U.U.E. C115 del 9 maggio 2008, pp. 309 ss.; v. anche l'art. 3 TUE. Cfr., *ex multis*, N.A. SMUHA - E. AHMED-RENGERS - A. HARKENS - W. LI - J. MACLAREN - R. PISELLI - K. YEUNG, *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, 5 August 2021, p. 8, disponibile su: *www.ssrn.com.*

[110] V. N.A. SMUHA - E. AHMED-RENGERS - A. HARKENS - W. LI - J. MACLAREN - R. PISELLI - K. YEUNG, *Op. cit*., p. 5.

© Wolters Kluwer Italia

degli artt. 101 e 102 TFUE non può sempre affrontare [111]. Deve riconoscersi che il complesso regime di gestione del rischio stabilito nel Titolo III del regolamento UE sull'IA potrebbe non fornire una piena soluzione a tali problemi. Tuttavia, si sostiene che potrebbe affrontare almeno alcune delle preoccupazioni derivanti dall'impatto degli algoritmi di prezzo nei mercati digitali e in particolare offrire gli strumenti necessari al rilevamento di prezzi collusivi *prima facie* come "malfunzionamento" del sistema [112].

Si può quindi concludere che, mentre la nozione di "IA affidabile" è sufficientemente ampia da comprendere una varietà di valori, principi e obiettivi politici dell'Unione, il nuovo regolamento sull'IA lascia alcune incertezze quando si tratta di regolamentare le tecnologie autonome nei contesti di mercato. Richiedere a coloro che utilizzano e traggono vantaggio dall'IA di valutare e gestire il rischio di esiti collusivi sarebbe coerente con l'obiettivo del regolamento di creare un "ecosistema di fiducia" per l'IA.

4. Prezzi algoritmici, regolamentazione dell'intelligenza artificiale e concorrenza: alcune conclusioni

Le tecnologie di IA hanno avuto un impatto significativo sulla società e sull'economia. Tuttavia, sollevano domande importanti per la continua osservanza di principi chiave, come la tutela della *privacy*, della concorrenza e della non-discriminazione. L'*AI Act* ha l'obiettivo estremamente rilevante di regolamentare questa tecnologia. Tuttavia, esso non sembra affrontare direttamente i rischi che gli algoritmi di determinazione dei prezzi creano per i diritti degli individui interessati dal loro utilizzo e per l'osservanza di importanti regole alla base del mercato unico, cioè i principi di concorrenza. È stato suggerito che poiché l'uso diffuso dell'IA sui mercati digitali porta la trasparenza a un livello che nessun altro approccio alla determinazione dei prezzi e al monitoraggio dei prezzi può raggiungere, può creare rischi per l'integrità del processo concorrenziale.

L'approccio adottato dall'*EU AI Act* nei confronti dei sistemi di determinazione dei prezzi autonomi sembra quindi porre notevoli in-

---

[111] V., *inter alia*, J.E. Harrington, *Op. cit*., pp. 351-352; D.R. Desai - J.A. Kroll, *Op. cit*., pp. 34-36.

[112] J.E. Harrington, *Op. cit*., p. 351; v. anche, *mutatis mutandis*, B. Ong, *Op. cit.,* pp. 209-210.

© Wolters Kluwer Italia

terrogativi sul se il regolamento possa raggiungere il suo obiettivo di garantire che l'IA sia "affidabile". In questo contesto, il requisito di "legalità" dell'IA punta a garantire che le tecnologie di IA siano tanto coerenti con la legge quanto soggette a strutture procedurali che possano assicurare la piena conformità con gli *standard* giuridici applicabili all'implementazione di questi sistemi.

Su questa base, si sostiene che gli algoritmi di determinazione dei prezzi non possono essere considerati "a basso rischio" quasi *a priori*, ma dovrebbero essere sottoposti a un attento esame cosicché la natura e l'intensità del rischio di ciascun sistema siano identificate e che ad esso vengano applicate le appropriate regole di gestione del rischio e di responsabilità [113]. Si può concludere che, sebbene sia presto per dire se l'*AI Act* possa raggiungere efficacemente i propri obiettivi, esso pone importanti interrogativi sul fatto che il trattamento di uno degli esempi più comuni di utilizzo dell'IA sia al di fuori dell'ambito del regime predisposto dal regolamento per le tecnologie ad "alto rischio" per i valori dell'Unione.

[113] B. SAREEN, *Explainable AI and pricing algorithms: a case for accountability in practice*, June 2023, p. 15, disponibile su: *www.ssrn.com*.

© Wolters Kluwer Italia

LA COSTRUZIONE DI UN MERCATO ANTROPOCENTRICO DELL'INTELLIGENZA ARTIFICIALE TRA DIRITTO DELL'UNIONE E DIRITTO NAZIONALE *

VINCENZO RICCIUTO

SOMMARIO: 1. La circolazione dell'IA nel territorio dell'Unione. Tra innovazione e tutela dei diritti. – 2. La disciplina del rischio come punto di contemperamento. – 3. Il rapporto tra persona e mercato: soluzioni a confronto. – 4. Gli organismi di vigilanza del mercato. – 5. Ambito e perimetro delle regolazioni europea e nazionale sull'IA. Considerazioni conclusive sul ruolo delle autorità indipendenti.

Abstract: The contribution revolves around the consideration of AI as a product, for which a safe, ethical and reliable market must be built, and of the individual as a mere user-consumer of this asset, to be protected only indirectly, i.e. through the correct regulation of commercial operations, and no longer according to an absolutist vision of the rights of the person. It is no coincidence that the AI Act, while affirming the anthropocentric nature of the European approach to regulating the technological phenomenon, is concerned with circumscribing the acts of private autonomy that concretise the circulation of AI on the market, finding a point of equilibrium between fundamental rights and business activities in the regulation of risk, which in some cases can go so far as to prohibit certain practices carried out with intelligent systems. A confirmation of this mercantilist structure is in the provision of market surveillance authorities, of its requirements and functioning, on whose altar the individual's subjective profiles and situations seem to have to be sacrificed.

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

1. La circolazione dell'IA nel territorio dell'Unione. Tra innovazione e tutela dei diritti

Il dibattito intorno al fenomeno dell'intelligenza artificiale si è, ad oggi, soprattutto sviluppato, nella prospettiva del diritto civile, intorno alla questione dei diritti fondamentali. E tuttavia, una tale prospettiva non può che essere posta sempre in relazione alla questione dello sviluppo e del funzionamento del mercato. In altri termini, siamo passati – basti vedere la direttiva 95/46/CE in tema di dati personali e poi la l. 31 dicembre 1996, n. 675 – da una visione di tipo assolutistico dei diritti della persona ad una che potremmo definire "relativistica".

Ne offrono un'indubbia testimonianza gli stessi "considerando" del regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679, o GDPR), costantemente richiamato dal regolamento (UE) 2024/1689 (regolamento sull'IA o *AI Act*).

Il 4° "considerando", infatti, pur ponendo l'individuo al centro della questione del trattamento dei dati personali (e dunque riconoscendo la centralità del tema dei diritti fondamentali), afferma che "*il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità*". E così, esso va contemperato con altri diritti fondamentali (libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, ecc.); tra essi, dunque, anche con la libertà d'impresa, che è carattere ed aspetto del diritto fondamentale di libera iniziativa economica (art. 41 Cost.).

Lo stesso art. 1 del GDPR, in particolare il par. 3, sancisce che: "*la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*".

A sua volta, il regolamento sull'IA intende affermare il carattere antropocentrico dell'approccio europeo alla regolazione del fenomeno, procedendo, però, alla disciplina della circolazione dell'IA nel territorio dell'Unione. Infatti, l'8° "considerando" ritiene necessario un quadro giuridico dell'Unione armonizzato in materia di IA, tale da consentirne lo sviluppo, l'uso e l'adozione nel mercato interno, garantendo "nel contempo" un elevato livello di protezione degli interessi pubblici (in questo senso si esprime anche l'art. 1 del regolamento sull'IA).

Si coglie, nel legislatore europeo, la consapevolezza che tali obiettivi siano raggiungibili attraverso la regolazione del mercato dell'IA, e così disciplinando la sua "*immissione sul mercato, la messa in servizio e l'uso di determinati sistemi di IA, garantendo in tal modo il buon fun-*

© Wolters Kluwer Italia

zionamento del mercato interno e consentendo a tali sistemi di beneficiare del principio della libera circolazione di beni e servizi" e favorendo l'innovazione.

La visione politica di questo approccio europeo è quella che aspira a fare dell'Unione europea "*un leader mondiale nello sviluppo di un'IA sicura, affidabile ed etica*" che "*garantisce la tutela dei principi etici*" (8° "considerando").

2. La disciplina del rischio come punto di contemperamento

Dalle norme di apertura e dai "considerando" si evince quindi che l'interesse dell'UE è disciplinare un'attività e la circolazione di un prodotto e inserire profili di conformazione dei loro presupposti e delle loro modalità.

Se volessimo leggerlo con le nostre categorie tradizionali, e segnatamente quella del diritto soggettivo, qui la situazione soggettiva disciplinata (nei suoi presupposti e nei limiti) è il diritto di attività di impresa (nella nostra Costituzione garantito all'art. 41) più che i diritti della persona (e qui il richiamo va all'art. 2 Cost.).

Semmai, qui, il tentativo è quello di un contemperamento tra il fenomeno economico dell'intelligenza artificiale (come si deve produrre, come può circolare, come può essere utilizzata, ecc.) e i diritti della persona che da quel fenomeno economico possono essere interessati (salute, riservatezza, dignità personale, ecc.).

Il punto di contemperamento sta nella disciplina del rischio nell'uso dell'IA in relazione ai diritti fondamentali della persona: aspetto che diventa una "qualità" del "prodotto" intelligenza artificiale. A ben vedere, l'articolazione dell'intelligenza artificiale si sostanzia in diverse "categorie merceologiche", come l'art. 6 dell'*AI Act* ci prospetta, dettando regole di "classificazione" in relazione al grado di "rischio" per la persona.

È proprio in relazione alla categoria corrispondente ad un livello di rischio più o meno alto, in grado di attentare alla vulnerabilità dell'individuo, che l'*AI Act* disciplina se e come può circolare quel prodotto, giungendo sino al punto che, in alcuni casi la sua stessa circolazione è vietata, come nel caso del "rischio inaccettabile" (art. 5: tecniche manipolative, subliminali, ingannevoli, ecc.).

Così, la ricaduta di questo impianto si percepisce in sede di valutazione circa la liceità degli atti di autonomia privata che realizzano la circolazione di un tal bene.

© Wolters Kluwer Italia

3. Il rapporto tra persona e mercato: soluzioni a confronto

Da quanto sinora detto si evince come il tema della persona si integra nella questione contrattuale e del mercato perché va a colorarne la causa e a connotare la meritevolezza o meno del rapporto contrattuale. Insomma, il tema del "rischio inaccettabile" entra, in sostanza, come profilo, come elemento che connota la causa del contratto: occorrerà poi riflettere se ciò sia riconducibile alla violazione espressa di norme imperative (ad esempio l'art. 5 *AI Act*, ossia le "pratiche di IA vietate") oppure se sia derivante dalla violazione di principi di ordine pubblico, anche economico.

Deve segnalarsi, in questa prospettiva, che il rapporto tra persona e mercato trova soluzioni talvolta diverse ove si confronti il GDPR e l'*AI Act*.

È il caso dell'art. 22 GDPR, che configura il diritto soggettivo dell'individuo a non essere sottoposto a decisioni interamente automatizzate (quindi delle macchine) che incidano sulla sua persona (compresa la profilazione). In questo caso, "*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*".

E tuttavia, prodotti (intesi anche come programmi, sistemi di intelligenza artificiale) in questa ipotesi possono circolare, ma è il diritto soggettivo dell'interessato che può impedire una tale pratica.

Di contro, nell'impianto della disciplina del mercato dell'*AI Act*, l'illiceità colpisce a monte alcuni tipi di prodotti impedendo che essi possano essere anche solo immessi nel mercato.

Qui il legislatore europeo sembra voler recuperare l'assolutezza dei diritti della persona, sottraendo alla stessa sua autonomia ogni profilo di disponibilità rispetto all'utilizzazione di quei prodotti.

In realtà, a ben vedere, ben prima che entri nel novero delle situazioni disponibili per il soggetto, rispetto al fenomeno dell'intelligenza artificiale, la disciplina agisce *ab origine*, impedendo che talune pratiche possano essere realizzate con quei sistemi. E ciò, appunto, senza nemmeno concedere potenzialmente che gli stessi possano incontrare la volontà e disponibilità dell'utente. È una scelta che attiene ad una esclusiva conformazione del mercato, ne delinea il perimetro e l'ambito, finendo per circoscrivere l'attività di impresa (la produzione, la commercializzazione, ecc.).

© Wolters Kluwer Italia

4. Gli organismi di vigilanza del mercato

La prospettiva del mercato, che costituisce il centro e la ragione dell'intervento normativo europeo, e rispetto al quale il tema della persona costituisce "solo" un limite all'attività di impresa in senso lato, trova conferma nella previsione di organismi di "vigilanza del mercato" che gli Stati membri sono chiamati ad individuare a norma degli artt. 70 ss. dell'*AI Act*.

Ed infatti, l'art. 70, al par. 1, prevede che "*ciascuno Stato membro istituisce o designa come autorità nazionali competenti ai fini del presente regolamento almeno un'autorità di notifica e almeno un'autorità di vigilanza del mercato. Tali autorità nazionali competenti esercitano i loro poteri in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti e garantire l'applicazione e l'attuazione del presente regolamento [...] a condizione che siano rispettati detti principi, tali compiti e attività possono essere svolti da una o più autorità designate, conformemente alle esigenze organizzative dello Stato membro*".

E al par. 2, dopo aver ancora parlato di "*autorità di vigilanza del mercato*", il legislatore europeo qualifica tale organismo come "*punto di contatto unico per il presente regolamento*".

E così, di nuovo, nei termini indicati titola l'art. 74 "*Vigilanza del mercato e controllo dei sistemi di IA nel mercato dell'Unione*".

Ancora una volta credo sia utile un raffronto tra la previsione del GDPR e quella dell'*AI Act*. Nel primo caso, al di là della più recente riflessione sui dati personali come bene economico che circola nel mercato, l'autorità preposta al fenomeno ha una tipica connotazione in termini di autorità di tutela del soggetto interessato con riguardo ai profili della personalità ecc., prova ne sia che la sua tutela è alternativa a quella offerta dal giudice civile ordinario secondo lo schema della c.d. tutela binaria.

Nel caso della regolazione europea dell'IA, di contro, la designazione dell'autorità preposta indica esplicitamente, se non esclusivamente, la prospettiva del mercato e della sua vigilanza e regolazione.

Così, al di là del fatto che non può attribuirsi alla stessa la tutela di diritti (e configurare dunque una tutela di tipo binario rispetto all'IA), consegue a questo impianto una diversa articolazione della funzione e dei poteri dei due organismi. È evidente che per poter correttamente operare, l'autorità di vigilanza del mercato dell'IA dovrà essere inevitabilmente dotata di poteri di conformazione dei contratti, laddove il Garante ha poteri minimi su questo fronte.

In questo quadro da ultimo delineato, il rapporto tra persona e

© Wolters Kluwer Italia

mercato nel fenomeno dell'IA rimane sostanzialmente irrisolto, laddove, se è vero – e lo è – che il tema della persona si integra nella questione contrattuale e del mercato, rimane tuttavia carente e ambiguo l'approccio nazionale sul tema della *governance* del fenomeno.

Nelle ipotesi nazionali di designazione delle autorità competenti non si coglie, evidentemente, la necessità di prevedere una *governance* istituzionale capace di gestire l'unitarietà del fenomeno (persona e mercato) e di costituire riferimento esclusivo di un fenomeno all'interno del quale i due termini continuano ad essere visti come antitetici e che invece sono sempre più entrambi costitutivi di una stessa vicenda.

5. Ambito e perimetro delle regolazioni europea e nazionale sull'IA. Considerazioni conclusive sul ruolo delle autorità indipendenti

A ben vedere, tutti i profili che si impongono alla riflessione del giurista del diritto civile e, segnatamente, quello della tutela dell'individuo e quello della tutela della libertà di iniziativa economica e del mercato, portano a dover affrontare la più ampia e pregiudiziale tematica del rapporto tra il diritto dell'Unione ed il diritto nazionale, soprattutto considerando l'approccio normativo (europeo) al fenomeno dell'intelligenza artificiale: un approccio puramente normativo, squisitamente europeo (che nasce in contesto sovranazionale e condiziona e limita la possibilità degli Stati di immaginare modelli di disciplina alternativi), frammentato (basti ricordare che temi centrali, come quello della responsabilità civile, si troveranno in provvedimenti diversi rispetto al regolamento sull'IA).

L'intervento normativo in tema di IA è stato realizzato senza che la corrispondente realtà economico-sociale fosse pienamente penetrata nella società, nelle relazioni sociali, nell'economia e nel sistema produttivo europeo. Di norma il diritto regola una realtà socio-economica già esistente ed in buona misura già acquisita da quei punti di vista.

Si pensi proprio alla vicenda dei dati personali: quando interviene il legislatore europeo (direttiva 95/46/CE) e poi quello italiano (l. n. 675/1996), il fenomeno del loro trattamento era già una vicenda reale, che aveva portato all'attenzione, prima ancora che del legislatore, delle istituzioni e delle imprese, il tema delle banche dati, del loro valore economico, dei rischi legati alla schedatura dei soggetti.

Ora l'Unione europea sembra procedere inversamente da una prospettiva quasi opposta. L'intelligenza artificiale come tecnologia non è ancora penetrata in maniera diffusa e stabile in tutti i processi di cui

© Wolters Kluwer Italia

abbiamo sopra parlato. Prova ne sia che la stessa Unione europea nel suo programma "*Europa Digitale*" ha stanziato un cospicuo finanziamento di 67.5 milioni per investire in progetti volti ad accelerare e rafforzare l'adozione delle tecnologie di intelligenza artificiale in Europa.

Premesso questo, l'interprete deve porsi la domanda relativa alla definizione degli ambiti e del perimetro intorno alla regolazione da un lato europea e dall'altro nazionale. Mi riferisco qui al disegno di legge italiano "*Disposizioni e delega al Governo in materia di intelligenza artificiale*" presentato il 20 maggio 2024.

La questione diventa comprendere fino a che punto una normativa statale può porsi su un piano di autonomia, se non in alternativa, rispetto alle disposizioni di fonte regolamentare europea, a partire dall'idea stessa che l'Unione europea ha dell'IA, che, come si è detto, è quella di un prodotto del quale va garantito e costruito il mercato.

Il 3° "considerando" dell'*AI Act* esprime tutta la preoccupazione del legislatore europeo che "*normative nazionali divergenti possono determinare una frammentazione del mercato interno e diminuire la certezza del diritto per gli operatori che sviluppano, importano o utilizzano sistemi di IA. È pertanto opportuno garantire un livello di protezione costante ed elevato in tutta l'Unione al fine di conseguire un'IA affidabile, mentre dovrebbero essere evitate le divergenze che ostacolano la libera circolazione, l'innovazione, la diffusione e l'adozione dei sistemi di IA e dei relativi prodotti e servizi nel mercato interno, stabilendo obblighi uniformi per gli operatori e garantendo la tutela uniforme dei motivi imperativi di interesse pubblico e dei diritti delle persone in tutto il mercato interno, sulla base dell'articolo 114 del trattato sul funzionamento dell'Unione europea*".

La preoccupazione del legislatore europeo è quella del mercato con il timore che i singoli Stati impongano la loro visione dell'IA, magari impedendone od ostacolandone la circolazione (in ipotesi anche per motivi astrattamente o vagamente riconducibili alla tutela della persona) e così ponendosi in contrasto con l'esigenza del mercato dell'IA.

La tecnica utilizzata è quella che afferma quale principio generale della materia quello di libera circolazione e vieta agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione da parte dell'*AI Act* (v. il 1° "considerando").

Del resto, ci conferma questo atteggiamento l'esperienza dell'Unione europea in tema di dati personali. Già con la direttiva 95/46/CE l'idea dell'Unione in tema di dati personali era che questi ultimi dovessero circolare all'interno di un mercato unico. Lo strumento della

© Wolters Kluwer Italia

direttiva, però, lasciava in questa cornice significativi spazi agli Stati, alcuni dei quali (ad esempio l'Italia), avevano limitato tale circolazione in relazione ai rischi possibili rispetto alla persona. Pertanto, il GDPR del 2016 ha dovuto esplicitare i limiti possibili per gli interventi statali, introducendo, come già visto, la disposizione di cui all'art. 1, par. 3.

Nel quadro regolatorio posto dall'*AI Act* la persona sembrerebbe venire in considerazione soprattutto come "utente" del prodotto di IA, e quindi come soggetto, a sua volta, del mercato, in quanto consumatore. La tutela dell'individuo sembrerebbe così proporsi soltanto in via indiretta, attraverso la disciplina del bene e delle operazioni commerciali meritevoli di tutela giuridica o no (in questo si traduce il discrimine tra pratiche vietate e pratiche pericolose).

E tuttavia, lo spazio di tutela della persona che residua da un governo del prodotto interamente gestito a livello europeo, consegna agli Stati un'area di possibile, quanto difficile, intervento proprio in relazione alla tutela dell'individuo, in coerenza con l'approccio antropocentrico europeo all'IA. Questo pare essere l'intento dell'art. 3 del progetto di legge italiano e ancor prima della relazione di accompagnamento.

Dicevo prima: "difficile" intervento normativo nazionale. Difficile in quanto nella ideazione e predisposizione degli strumenti di tutela della persona gli Stati sono vincolati al rapporto con la prospettiva mercantilistica che caratterizza il fenomeno e il regolamento europeo, sul cui altare sembrano doversi sacrificare profili e situazioni soggettive dell'individuo.

Eppure, il regolamento non mira a pregiudicare l'applicazione della normativa in tema di trattamento dei dati personali (in relazione alla quale si pone in posizione di complementarità). Né l'effetto ricercato è quello di una modifica o compromissione dei compiti e dei poteri delle autorità di controllo indipendenti in materia di protezione dei dati personali, competenti a monitorare la conformità di un'attività con il GDPR (v. il 10° "considerando").

Al di là dell'individuazione di una competenza diretta ed esclusiva in tema di regolazione e vigilanza dell'IA posta in capo alle autorità di cui all'art. 70 del medesimo regolamento, pertanto, le autorità nazionali per la protezione dei dati personali non possono non avere un ruolo decisivo e trasversale sui profili di regolazione dell'IA, perché la loro competenza esclusiva sul tema dei dati dell'individuo-persona sicuramente incide sulla stessa circolazione dei prodotti di intelligenza artificiale, condizionandone e plasmandone la stessa diffusione e la stessa utilizzazione. L'illiceità di un trattamento su cui si basa un certo prodotto di intelligenza artificiale, individuata ed accertata dal Garante

© Wolters Kluwer Italia

per la protezione dei dati personali, insomma, non potrà che rilevare in termini di impedimento del trattamento, ed in definitiva dell'utilizzo e della circolazione del prodotto di IA che su esso si basa.

Sicché, in sostanza, il diritto e la prassi nazionali, che sul prodotto non hanno grandi margini di operatività, recuperano spazio di manovra attraverso la possibilità di regolare i processi che alimentano il fenomeno IA, secondo la propria impostazione giuridico-sistematica, nonché la propria sensibilità attenta alla realtà sociale e "naturale" della dimensione umana.

Nel nostro quadro normativo nazionale, settori e materie che riguardano diritti fondamentali sono stati affidati tradizionalmente a modelli di vigilanza svolta da autorità amministrative indipendenti in ragione del principio di neutralità e indipendenza delle stesse. D'altra parte, una tale caratteristica è avvertita come necessaria dallo stesso legislatore europeo, che all'art. 70 configura le autorità nazionali competenti in tema di intelligenza artificiale come soggetti "indipendenti, imparziali". Possiamo dire, da quanto detto, che vi è più di una perplessità su quelle che sembrano essere le scelte contenute nell'attuale disegno di legge italiano.

© Wolters Kluwer Italia

L'ESERCIZIO DELLA FUNZIONE AMMINISTRATIVA ATTRAVERSO L'INTELLIGENZA ARTIFICIALE: POTENZIALITÀ E LIMITI DEL SUO UTILIZZO DA PARTE DELLE PUBBLICHE AMMINISTRAZIONI * **

ALBERTO ZITO

SOMMARIO: 1. La potenziale pervasività dell'uso dell'IA rispetto all'insieme delle attività amministrative: nuove problematiche e nuovi approcci di studio. – 2. Il regolamento UE 2024/1689 e l'impatto sull'uso dell'intelligenza artificiale da parte delle pubbliche amministrazioni. – 3. IA e suo uso da parte delle pubbliche amministrazioni: problemi teorici e di metodo. – 4. La decisione amministrativa affidata all'IA: la questione dei provvedimenti discrezionali.

Abstract: The use of artificial intelligence by public administration presents some challenges for legal experts. However, it cannot be denied that the application of AI produces positive effects for the recipients of administrative actions. From a legal point of view, it could be said that it represents a necessary implementation of the principle of good administration. However, the issue becomes more complex when AI is used in decision-making processes. Legal scholars have mainly focused on decisions that have the nature and form of administrative acts and that represent the exercise of power, questioning the use of AI in relation to mandatory and discretionary decisions. However, the problem has wider implications because it affects all decisions made by public administration.

* Contributo sottoposto a doppio referaggio in forma anonima.

** Testo rielaborato dall'Autore a seguito della *lectio magistralis* tenutasi il 26 marzo 2024.

© Wolters Kluwer Italia

1. La potenziale pervasività dell'uso dell'IA rispetto all'insieme delle attività amministrative: nuove problematiche e nuovi approcci di studio

L'utilizzo da parte della pubblica amministrazione della intelligenza artificiale (d'ora in avanti anche IA) pone molti problemi al giurista.

Prima di esaminare quelli più rilevanti, è utile ricordare come l'IA si presti ad essere utilizzata dalla pubblica amministrazione rispetto al complesso delle sue funzioni e dunque tanto in relazione all'attività da cui scaturisce una decisione destinata a realizzare effetti nella sfera giuridica dei destinatario quanto in relazione all'attività da cui scaturisce un'utilità sia essa a fruizione individuale (come nel caso della messa a disposizione della prestazione sanitaria) o a fruizione collettiva (come nel caso della vigilanza e della sicurezza di un parco pubblico).

Gli esempi appena fatti confermano, per un verso, la pervasività della tecnologia digitale rispetto all'agire della pubblica amministrazione e, per altro verso, consentono di fare una prima distinzione rispetto ai diversi problemi che il suo utilizzo pone. Non si può negare infatti come, allorquando la pubblica amministrazione ricorra all'IA per rendere prestazioni più efficienti nei confronti della collettività e dei suoi membri (ad esempio una diagnosi precoce e più attendibile di una patologia o l'esecuzione più accurata di un intervento chirurgico), si realizzino effetti positivi per i destinatari di tale azione che non sarebbe stato possibile realizzare sino a pochi anni addietro. Siamo dunque in presenza di un nuovo capitolo della storia del rapporto tra agire dell'amministrazione e utilizzo della tecnica da cui certamente sorgono problemi nuovi (si pensi per tornare agli esempi fatti all'allocazione della responsabilità per il malfunzionamento dello strumento digitale nel corso dell'esecuzione di una operazione chirurgica), ma da cui si originano anche benefici rispetto alle finalità che la pubblica amministrazione deve perseguire.

Dal punto di vista giuridico si potrebbe dire che gli usi, cui si è accennato, costituiscano doverosa realizzazione del precetto costituzionale del buon andamento [1]. Dunque, pur senza cadere in facili ottimi-

[1] Sempre più speso la dottrina, anche non italiana, collega l'uso delle tecnologie digitali alla *good administration*. Cfr. ad esempio E.M. MENENDEZ SEBASTIAN, *From Bureaucracy to Artificial Intelligence. The tension between effectiveness and guarantees*, Milan, 2023; C. COGLIANESE - A. LAI, *Assessing automated Administration*, in J.B. BULLOCH - Y.C. CHEN - J. HIMMELREICH - V.M. HUDSON - A. KORINEK - M.M. YOUNG - B. ZHANG (eds.), *The Oxford Handbook of AI Governance* (*online* edn., Oxford Academic, 14 February 2022). Per la dottrina italiana cfr., *ex multis*, D.U. GALETTA, *Digitalizza-*

© Wolters Kluwer Italia

smi, l'atteggiamento che il giurista deve avere non può essere pregiudizialmente ostile rispetto all'uso anche massiccio dell'intelligenza artificiale digitale da parte della pubblica amministrazione [2].

Il discorso però si complica quando l'IA viene utilizzata, nei processi di *decision making* delle pubbliche amministrazioni.

La dottrina amministrativistica non è rimasta insensibile al problema. L'attenzione sino ad oggi si è concentrata soprattutto sulle decisioni che producono effetti giuridici unilaterali nei confronti dei destinatari e dunque sulle decisioni che hanno natura e forma di provvedimento amministrativo e che costituiscono esercizio del potere.

Ci si è dunque interrogati sulla utilizzabilità dell'IA rispetto ai provvedimenti vincolati e a quelli discrezionali anche alla luce di alcune pronunce giurisprudenziali. Se per i primi si è ritenuto possibile ricorrere alla cosiddetta decisione robotica, per i secondi sono state avanzate molto riserve.

Il problema è tuttavia più ampio perché esso investe tutte le decisioni che la pubblica amministrazione deve assumere, quand'anche non abbiano natura provvedimentale, ma si inseriscano nel fluire dell'agire amministrativo condizionandone i successivi sviluppi. La scelta del tragitto del servizio pubblico di linea, delle fermate e degli orari, è pur sempre una decisione da cui scaturiscono conseguenze sulle modalità di gestione del servizio stesso e su coloro che saranno i fruitori del medesimo. La scelta di dislocare sul territorio i presidi ospedalieri in un certo modo è nuovamente una decisione che determinerà effetti sulle condizioni materiali della tutela del diritto alla salute. Una diagnosi medica, per strano che possa sembrare agli occhi del giurista, è pur sempre una decisione.

E non c'è dubbio che anche queste decisioni possono essere affidate ad un *software* basato sull'IA e che anzi il naturale terreno di elezione del fenomeno sia proprio questo [3].

---

zione e diritto ad una buona amministrazione (il procedimento amministrativo fra diritto Ue e tecnologie ICT*)*, in R. Cavallo Perin - D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020.

[2] In proposito si può rinviare a E.M. Menendez Sebastian, *Op. cit*., secondo cui *"*Without being excessively optimistic [...] I am inclined to include myself in the group of those who want to imagine a tomorrow with better public services, with a more efficient Administration, one that is concerned about citizens, proactively committed to innovation, but without neglecting the guarantees of the recipients of this public action and, therefore, of all of us" (p. XIII).

[3] Sulle enormi potenzialità dell'uso dell'IA, ad esempio, in ambito medico (dalla diagnostica ai sistemi predittivi di patologie, dalla ricerca clinica a quella farmacologica) ma anche sui rischi cfr. E. Santoro, *La medicina: potenzialità e rischi di una rivoluzione*, in *MicroMega,* 2024, pp. 51 ss.

© Wolters Kluwer Italia

Vi è dunque una prima indicazione che discende da quanto detto: l'intelligenza artificiale obbliga il giurista ad un esame della tematica muovendo dall'assunzione di una prospettiva diversa da quella tradizionale che fa perno sulla decisione amministrativa a prescindere dalla forma e dal regime giuridico dell'atto che le veicola. Non rileva tanto quest'ultimo, quanto l'esserci di una decisione in tutto o in parte affidata all'IA che impatta sulla "vita" delle persone. Si tratta certamente di una novità che la dottrina deve tenere in debita considerazione nelle proprie ricostruzioni sistematiche.

2. Il regolamento UE 2024/1689 e l'impatto sull'uso dell'intelligenza artificiale da parte delle pubbliche amministrazioni

Il quadro di riferimento sull'utilizzo dell'IA è oggi dato dal regolamento europeo 2024/1689, approvato dal Parlamento europeo e dal Consiglio in data 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale. E di esso sono certamente destinatarie le pubbliche amministrazioni atteso che rientrano a pieno titolo nella definizione di *deployer* di cui all'art. 3, punto 3, ai sensi del quale è considerato tale "*una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità*".

Si tratta del primo corposo tentativo (l'atto si compone di 180 "considerando", di 113 articoli e di 12 allegati) di dettare una disciplina organica della materia. Ai fini che qui interessano rilevano in particolare alcune disposizioni, la prima delle quali è sicuramente quella contenente la definizione di intelligenza artificiale. Ai sensi dell'art. 3, punto 1, per sistema di intelligenza artificiale si intende 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*".

Si tratta di una definizione che ricomprende sia la IA deterministica sia la IA non deterministica che certamente rappresenta il tipo di intelligenza artificiale più innovativo e problematico, i cui sviluppi non sono ad oggi prevedibili.

La prima si basa su un algoritmo che processa in modo predeterminato le informazioni immesse, ossia gli *input*, e che produce un *output* (anche sotto forma di decisione) che è in qualche modo esso stesso predeterminato a monte. Detto in altri termini questo tipo di IA lavora

© Wolters Kluwer Italia

secondo le regole proprie della logica deduttiva o, se si preferisce, del ragionamento deduttivo e tutti noi sappiamo che in questo tipo di ragionamento la conclusione è già interamente contenuta nelle premesse.

La seconda si differenzia profondamente dalla prima perché l'*output* che scaturisce dalla macchina non è interamente predeterminato.

È il ben noto fenomeno della *machine learning*, il cui algoritmo agisce in modo diverso dall'algoritmo deterministico. La principale differenza sta nel fatto che la *machine learning* usa un algoritmo che è progettato per consentire alla macchina stessa di interagire con l'ambiente, ossia con i dati disponibili, di imparare autonomamente attraverso questa interazione e di creare altrettanto autonomamente un modello del mondo sulla cui base gli specifici problemi vengono trattati e risolti [4].

La parte più delicata di questo processo è proprio la creazione del modello che viene costruito sulla base dei dati, non soltanto perché gli algoritmi usati sono molto complessi, ma perché, come è stato detto, non siamo in grado di capire come la *machine learning* sia giunta ad elaborare il modello, quand'anche verifichiamo che l'*output* che ne scaturisce sia corretto ed anche utile [5]. Per questo gli algoritmi sono

---

[4] Cfr. G.F. Italiano, *Le sfide interdisciplinari dell'intelligenza artificiale,* in *Analisi giuridica dell'economia*, 1/2019, pp. 9 ss. secondo cui gli algoritmi di *machine learning* agiscono in modo diverso dagli algoritmi tradizionali: "*La differenza principale è che machine learning usa il codice per consentire a un sistema automatico di imparare e di creare un modello del problema che bisogna risolvere. Un modello che non è però spesso facilmente interpretabile come le linee di codice degli algoritmi tradizionali. Per fare un esempio molto approssimativo, e forse anche un po' esagerato, potremmo pensare al modello prodotto da un algoritmo di machine learning come a un cervello umano. Non possiamo dissezionare il cervello per capire cosa è successo, perché è stata presa una certa decisione. Possiamo provare a osservare dall'esterno, a fare delle domande, interrogare la persona e analizzare le sue risposte. Ma questo è un processo lungo, non sempre conduce a conclusioni esatte, e non sempre fa capire perché è stata presa una certa decisione. In questo caso, il meccanismo con cui è stata presa una decisione è poco chiaro, poco trasparente e più difficilmente spiegabile. Per questo gli algoritmi di machine learning sono come una scatola chiusa, una black box, che non può essere aperta molto facilmente. Non è realmente chiaro come fa una macchina a riconoscere le immagini. Si costruisce un suo modello, e ovviamente può anche fare errori. Anche se una macchina può ottenere risultati confrontabili a quelli di un essere umano, il suo modo di operare, la sua logica è completamente diversa da quella di un essere umano*" (p. 13). Sul punto cfr. da ultimo N. Cristianini, *Machina sapiens*, Bologna, 2024, p. 34: "*ogni agente intelligente ha bisogno di un modello del suo ambiente, implicito o esplicito, per potere scegliere le proprie azioni in modo opportuno*" sicché "*parlando di intelligenza artificiale dobbiamo distinguere l'agente dal modello del mondo che lo anima e dall'algoritmo che produce tale modello partendo dall'esperienza*".

[5] N. Cristianini, *Op. cit.*, riporta molti esempi in cui la "*machina sapiens*" ha prodotto decisioni corrette, tra i quali quello relativo alla licenza di avvocato negli Stati Uniti il cui ottenimento prevede il superamento di un test *standard* composto di tre par-

© Wolters Kluwer Italia

considerati come una scatola chiusa od anche come si suole dire una *black box* [6] e il fenomeno ha generato e genera comprensibili timori, che sono quelli che hanno indotto di recente a chiedere una moratoria nello sviluppo dell'IA.

Il regolamento europeo non vieta in via generale l'uso dell'intelligenza artificiale non deterministica, se non in particolari casi, individuando per le altre ipotesi vincoli e limitazioni che dovrebbero consentire di ridurre il rischio connesso al suo utilizzo.

Tanto i divieti quanto i vincoli e le limitazioni impattano certamente sulle pubbliche amministrazioni e sulla loro azione.

E così, ad esempio, tra le pratiche vietate, disciplinate dall'art. 5, vi è quella relativa all'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, a meno che, e nella misura in cui, tale uso sia strettamente necessario per alcuni obiettivi ben definiti.

Ed ancora tra le pratiche ad alto rischio, di cui all'art. 6 del regolamento vi è quella dell'uso di sistemi di IA destinati a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi di cui all'allegato III che certamente riguardano molti compiti affidati alle cure della pubblica amministrazione [7].

---

ti. Ebbene "*Nella primavera del 2023 OpenAI riportò il risultato combinato di 298 punti per questi tre esami, ovvero entrò nel 90° percentile (mentre GPT-3 aveva raggiunto solamente il 10° percentile)*", p. 121. Un tale esempio ci fa capire non solo il livello raggiunto dall'IA ma anche la rapidità dei progressi.

[6] Sul rischio che si realizzi una *black box society* cfr. F. PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge-London, 2015.

[7] Nell'allegato III vi sono molte ipotesi che riguardano in modo diretto una parte, certamente non secondaria dell'azione amministrativa. Sono infatti considerati ad alto rischio nella materia dell'istruzione e della formazione professionale: a) i sistemi di IA destinati a essere utilizzati per determinare l'accesso, l'ammissione o l'assegnazione di persone fisiche agli istituti di istruzione e formazione professionale a tutti i livelli; b) i sistemi di IA destinati a essere utilizzati per valutare i risultati dell'apprendimento, anche nei casi in cui tali risultati sono utilizzati per orientare il processo di apprendimento di persone fisiche in istituti di istruzione o formazione professionale a tutti i livelli; c) i sistemi di IA destinati a essere utilizzati per valutare il livello di istruzione adeguato che una persona riceverà o a cui potrà accedere, nel contesto o all'interno di istituti di istruzione o formazione professionale a tutti i livelli; d) i sistemi di IA destinati a essere utilizzati per monitorare e rilevare comportamenti vietati degli studenti durante le prove nel contesto o all'interno di istituti di istruzione e formazione professionale a tutti i livelli. Sono considerati ad alto rischio nella materia delle servizi pubblici essenziali: a) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria, nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi; b) i si-

© Wolters Kluwer Italia

Quelli fatti sono solo alcuni esempi, sufficienti però a mostrare per un verso il rilevante impatto che la disciplina europea è destinata ad avere sull'azione amministrativa e per altro verso la necessità di un grande impegno da parte dei giuristi volto non soltanto a interpretare correttamente le disposizioni del regolamento, ma anche e soprattutto ad individuare i segmenti dell'azione amministrativa rispetto ai quali sono destinati a trovare applicazione.

3. IA e suo uso da parte delle pubbliche amministrazioni: problemi teorici e di metodo

Come si è accennato l'uso dell'IA per l'assunzione delle decisioni amministrative di tipo provvedimentale è da tempo diventato realtà soprattutto nelle ipotesi di esercizio di poteri amministrativi vincolati ed argomento di discussione e dibattito nella dottrina amministrativistica con riguardo all'esercizio dei poteri discrezionali.

Prima di svolgere qualche sintetica riflessione sullo stato dell'arte è opportuno però ricordare come decisioni della p.a. affidate all'IA pongono, anche nel caso in cui si ritenga che solo per l'esercizio di poteri vincolanti si possa ricorrere all'intelligenza artificiale, diversi problemi il primo dei quali si colloca sul piano teorico-dogmatico, perché l'IA sfida molte delle teorie che sono state sinora elaborate per concettualizzare il fenomeno giuridico.

Tanto per fare un esempio veniamo da una tradizione in cui l'atto amministrativo è stato ricostruito come un atto in cui la volontà che in esso si esprime è pur sempre una volontà del funzionario pubblico, ancorché tale volontà poi venga per così dire oggettivizzata ossia imputata ed ascritta alla pubblica amministrazione [8]. Ebbene, di fronte ad un atto che scaturisce dall'intelligenza artificiale dove è la volontà? Quello appena fatto, peraltro, è soltanto uno dei molti esempi che si potrebbero fare. Si pensi a cosa ne è del procedimento amministrativo allorquando il quest'ultimo si riduce ad un insieme di operazioni interne alla macchina o per meglio dire al *software* che su di essa è installato [9] od anche alla garanzia della partecipazione.

---

stemi di IA destinati a essere utilizzati per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito, a eccezione dei sistemi di IA utilizzati allo scopo di individuare frodi finanziarie; c) i sistemi di IA destinati a essere utilizzati per la valutazione dei rischi e la determinazione dei prezzi.

[8] Il punto è sottolineato in particolare da A. Simoncini, *Profili costituzionali dell'amministrazione algoritmica*, in *Riv. trim. dir. pubb.*, 2019, pp. 1149 ss.

[9] Sono questioni che la stessa giurisprudenza ha affrontato, ma le cui soluzioni

© Wolters Kluwer Italia

Vi è poi un secondo problema che si colloca sul piano del metodo. Non mi intendo riferire al fatto che la diffusione direi pervasiva dell'IA costringe il giurista a confrontarsi con altre discipline e segnatamente con quelle che si occupano in maniera diretta del fenomeno ossia la matematica, l'informatica, le neuroscienze e le scienze cognitive. Messa in questi termini la questione non appare particolarmente problematica e, a ben guardare, neanche nuova soprattutto per lo studioso di diritto amministrativo. Il punto è invece un altro e di tutt'altro spessore: quando ci confrontiamo con l'intelligenza artificiale il tradizionale paradigma a mezzo del quale si procede all'inquadramento delle connessioni tra la scienza giuridica ed un fatto oggetto di studio in altri ambiti scientifici sembra non bastare né a catturare il fenomeno né ad inquadrarlo.

Sino ad oggi infatti le teorie scientifiche hanno rivestito nell'ambito del diritto amministrativo due funzioni ben precise: *i*) sono state di ausilio per l'applicazione in concreto delle norme in tutti quei casi in cui tale applicazione richieda la preventiva qualificazione dei fatti attraverso il ricorso a teorie, metodi e regole scientifiche e tecniche; *ii*) hanno fornito gli strumenti tecnici per operare in modo da soddisfare il principio del buon andamento quantomeno nella sua declinazione, sicuramente presente nell'art. 97 della nostra Costituzione, di principio di efficienza che altro non è se non l'espressione della cosiddetta razionalità strumentale e dunque dell'ottimale rapporto tra mezzi e fini.

Rispetto a questo schema vi è però un elemento di grande novità. La IA non si pone solo in posizione servente rispetto alle due funzioni per così dire tradizionali, perché è essa stessa che si pone come fattore diretto della produzione giuridica. L'intelligenza artificiale sembra avanzare pretese di autoconsistenza, candidandosi a divenire attore non umano del sistema giuridico un funzionario dell'attuazione dell'ordinamento.

Infine, riprendendo quanto si è già avuto modo di dire a proposito dell'intelligenza non deterministica e delle sue peculiarità, si staglia di fronte al giurista un terzo ordine di problematiche.

Rispetto all'operare della *machine learning* il punto di maggior rilievo per il giurista non è soltanto verificare se la decisione discrezionale presenti caratteri tali da precludere ogni possibilità di essere trattata dalla IA.

Vi è infatti una tematica preliminare data dalla circostanza che si è in presenza di una decisione di cui non siamo in grado di comprendere

---

impongono in ogni caso una meditata rivisitazione di alcuni istituti fondanti il diritto amministrativo quale appunto quello di procedimento e di partecipazione.

© Wolters Kluwer Italia

né il processo né le ragioni che l'hanno determinata, potendo al massimo verificarsi *ex post* se consenta di raggiungere l'obiettivo che interessa.

Di fronte al problema della *black box*, il giurista può utilizzare una strategia di contenimento basata in particolare sul principio della riserva di umanità ossia sull'impossibilità, scaturente da questo principio, che la decisione sia affidata unicamente alla "*machina sapiens*", dovendo essere sempre garantita la possibilità dell'intervento umano al fine di correggere la decisione robotica integrandola o sostituendola con un'altra decisione [10]. In questa prospettiva verrebbe fatto salvo il cosiddetto *human in the loop* ossia la possibilità di un'interazione persona-macchina in cui la prima mantiene un ruolo che gli consente due livelli di intervento ossia fornire *feedback* alla macchina e prendere decisioni sulla base degli *output* forniti da quest'ultima.

In questa direzione si è peraltro orientato anche il nostro legislatore, prima di quello europeo, come è evidente dall'art. 30, comma 3, del codice dei contratti pubblici ai sensi del quale le decisioni assunte mediante automazione rispettano tra gli altri il principio della "*non esclusività della decisione algoritmica, per cui comunque esiste nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatizzata*" [11].

Si tratta di una soluzione che è certamente utile a stemperare i timori che aleggiano intorno all'IA. Non si può tuttavia evitare di interrogarsi sull'effettiva praticabilità di tale soluzione. Quale funzionario pubblico si assumerebbe la responsabilità di smentire la decisione della "*machina sapiens*", dal momento che la soluzione al problema da essa elaborata è il più delle volte maggiormente attendibile di quella umana se non altro perché si fonda su una quantità di dati che nessun essere umano potrebbe mai conoscere? Nella pratica vi è dunque il rischio che

[10] Sulla riserva di umanità cfr. in particolare, G. Gallone, *Riserva di umanità e funzioni amministrative*, Padova, 2023. Il problema però è trattato da molti studiosi anche in opere non aventi carattere monografico; cfr. quantomeno B. Marchetti, *La garanzia dello human in the loop alla prova della decisione amministrativa algoritmica*, *in BioLaw Journal*, 2021, pp. 367 ss.

[11] Gli altri due principi previsti dalla norma sono quelli: conoscibilità e comprensibilità, per cui ogni operatore economico ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino e, in tal caso, a ricevere informazioni significative sulla logica utilizzata e di non discriminazione algoritmica, per cui il titolare mette in atto misure tecniche e organizzative adeguate al fine di impedire effetti discriminatori nei confronti degli operatori economici.

© Wolters Kluwer Italia

la garanzia dello *human in the loop* evapori e che si affermi una logica di *human out the loop*.

Se la cosiddetta riserva di umanità si espone al suddetto rilievo, occorre allora verificare se esistano anche altre strade da esplorare per evitare che l'esercizio della funzione amministrativa risulti totalmente, se non in massima parte, delegata all'IA.

Una prima possibile strada potrebbe essere quella di iniziare ad individuare quali siano quelle attività amministrative in relazione alle quali, per ragioni etiche o per la componente empatica ad esse associata, sia da considerare preferibile affidarsi all'agire umano, con la conseguenza di prevedere in tali casi un divieto di utilizzo dell'IA se non per limitati segmenti che sono di mero ausilio all'agire dei funzionari pubblici [12].

Una seconda possibile strada da esplorare è quella di verificare in primo luogo se l'investimento in IA, con il costo che esso comporta, sia maggiore o minore dei benefici attesi ed in secondo luogo se la soluzione "umana" non sia comparativamente preferibile in quanto offra un migliore rapporto costi/benefici [13]. Si tratta, come evidente, di una prospettiva che si fonda direttamente sull'art. 97 della Costituzione ed in particolare sul principio di buon andamento declinato come efficacia ed efficienza delle pubbliche amministrazioni. In questa prospettiva il ricorso all'IA non può essere deciso in astratto una volta per tutte ma va verificato proprio alla stregua ed in applicazione del principio del buon andamento nella logica dell'analisi costi/benefici.

Vi è infine una terza direttrice di marcia che pure può essere considerata. L'IA, come è già stato detto, deve lavorare, per essere efficace, su una grande quantità di dati che siano affidabili. Non è detto però che ciò sia sempre possibile, perché potrebbero esserci ragioni di *privacy* o di qualità dei dati che, per un verso, impediscono di raggiungere quella dimensione quantitativa necessaria all'IA per determinare il modello del mondo sulla cui base risolvere problemi specifici e, per altro verso, impediscono di pervenire a decisioni attendibili ossia non affette da *bias* o pregiudizi [14]. Ogni qualvolta dunque l'entità dei dati non sia

---

[12] Utili considerazioni al riguardo si possono leggere in S. MAZZOCCHI - L. ROMANO, *Io, robot? L'intelligenza artificiale ai tempi della quarta rivoluzione industriale*, in P. SEVERINO (a cura di), *Intelligenza artificiale. Politica, economia, diritto, tecnologia*, Roma, 2022, pp. 31 ss.

[13] Cfr. S. MAZZOCCHI - L. ROMANO, *Op. cit.*, p. 33.

[14] Il tema della qualità dei dati è particolarmente rilevante perché occorre evitare il fenomeno del *garbage in garbage out* ossia che prendendo spazzatura in ingresso

© Wolters Kluwer Italia

adeguata ovvero la loro qualità sia incerta, non vi può né vi deve essere spazio per l'uso dell'IA da parte delle pubbliche amministrazioni.

Molteplici sono dunque le strategie che il diritto può mettere in campo per tentare di governare al meglio l'utilizzo dell'IA da parte delle pubbliche amministrazioni. Tutto ciò richiede però la messa in campo di un approccio ai problemi di tipo spiccatamente interdisciplinare ed una disponibilità da parte dello studioso a rivedere senza remore le categorie con cui sino ad oggi il diritto amministrativo è stato interpretato e ricostruito sistematicamente.

4. La decisione amministrativa affidata all'IA: la questione dei provvedimenti discrezionali

Come detto in apertura, si è già sviluppato in dottrina un intenso dibattito sull'uso dell'IA non soltanto con riferimento all'esercizio dei poteri vincolati, ma anche e soprattutto a quelli discrezionali rispetto ai quali la posizione prevalente è quella connotata da uno scetticismo più o meno marcato [15].

Senza la pretesa di affrontare in profondità una questione di tale portata, non si può non concordare con la posizione scettica se la discrezionalità amministrativa continua ad essere ricostruita nei termini

---

(dati inattendibili), si produce spazzatura in uscita (un modello del mondo sbagliato o, peggio ancora, dannoso).

[15] Il dibattito dottrinale sul punto, suscitato anche da alcune sentenze del giudice amministrativo è molto intenso: Cfr. *ex multis* N. Paolantonio, *Il potere discrezionale della pubblica automazione. Sconcerto e stilemi (sul controllo giudiziario delle "decisioni algoritmiche")*, in *Dir. amm.*, 2021, pp. 813 ss.; D. Carullo, *Decisione amministrativa e intelligenza artificiale*, in *Dir. inform.*, 3/2021, pp. 431 ss.; P. Forte, *Diritto amministrativo e data science. Appunti di intelligenza amministrativa artificiale (AAI)*, in *PA persona e amministrazione*, 2020, pp. 247 ss.; D.U. Galetta, *Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia*, in Aa.Vv., *Scritti per Franco Gaetano Scoca*, vol. III, Napoli, 2020, pp. 2265 ss.; D. Marongiu, *L'automazione delle decisioni amministrative: teorie, esperienze e sentenza*, ivi, pp. 3369 ss.; E. Carloni, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm.*, 2020, pp. 275 ss.; B. Raganelli, *Decisioni pubbliche e algoritmi: modelli alternativi di dialogo tra forme di intelligenza artificiale diverse nell'assunzione di decisioni amministrative*, in *Federalismi.it*, 2020, pp. 242 ss.; R. Ferrara, *Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale*, in *Dir. amm.*, 2019, pp. 773 ss.; S. Civitarese Matteucci, *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in *Dir. pubbl.*, 2019, pp. 5 ss.; E. Picozza, *Politica, diritto e Artifical Intelligence*, in *Giur. it.*, 2019, pp. 1761 ss.; F. Patroni Griffi, *La decisione robotica e il giudice amministrativo*, in A. Carleo (a cura di), *Decisione robotica*, Bologna, 2017, pp. 165 ss.

© Wolters Kluwer Italia

proposti da M.S. Giannini negli anni Trenta del secolo scorso [16]. Secondo tale ricostruzione, che è seguita dalla quasi totalità della dottrina, la discrezionalità consista in una ponderazione comparativa degli interessi secondari (pubblici o privati) con l'interesse pubblico primario che la p.a. deve perseguire [17]. Come è evidente, la definizione presuppone, per un verso, l'esistenza di un rapporto di interdipendenza tra tutti gli interessi in gioco e, per altro verso, che l'interesse pubblico si ponga come uno dei due termini di questo rapporto, l'altro essendo rappresentano dagli interessi diversi dal primo. Ne discende, se si sta a questa definizione, come sia lo stesso interesse pubblico a venire pesato e comparato con gli altri interessi.

La circostanza che l'interesse pubblico sia pesato e comparato con gli altri interessi e che possa addirittura diventare recessivo per effetto di tale comparazione mina la stessa possibilità che si possa utilizzare l'IA per addivenire alla decisione discrezionale. A venire meno infatti è uno dei presupposti affinché l'IA possa funzionare ossia che vi sia chiaramente un obiettivo che deve essere perseguito rispetto al quale quest'ultima sia in grado di elaborare la decisione migliore per perseguirlo. Se la massimizzazione della cura dell'interesse pubblico viene meno come obiettivo prioritario per effetto della possibilità che esso risulti recessivo nella comparazione tra quest'ultimo e gli altri interessi privati e/o pubblici presenti nel caso di realtà che deve essere gestito, è

---

[16] Cfr. M.S. GIANNINI, *Il potere discrezionale della pubblica amministrazione. Concetti e problemi*, Milano, 1939.

[17] Tale definizione è ancora oggi, come detto nel testo, quella seguita dalla dottrina maggioritaria. Cfr. ad esempio, tra la trattatistica e la manualistica più recente, R. VILLATA - M. RAMAJOLI, *Il provvedimento amministrativo*, Torino, 2002, in particolare pp. 85 ss.; G. DELLA CANANEA - M. DUGATO - B. MARCHETTI - A. POLICE - M. RAMAJOLI, *Manuale di diritto amministrativo*, Torino, 2022, dove si ribadisce la definizione di M.S. Giannini con una particolare sottolineatura del carattere politico della ponderazione comparativa (la parte cui si fa riferimento è di A. POLICE); G. CORSO, *Manuale di diritto amministrativo*, IX ed., Torino, 2020, p. 208, dove si riporta la definizione di M.S. Giannini, pur avendo cura di precisare che non è corretto ritenere che "*laddove c'è discrezionalità, c'è necessariamente una valutazione compartiva di interessi*"; M. CLARICH, *Manuale di diritto amministrativo*, III ed., Bologna, 2017, p. 126, dove si afferma che la scelta discrezionale "*avviene attraverso una valutazione comparativa (ponderazione) degli interessi pubblici e privati rilevanti nella fattispecie*"; F.G. SCOCA (a cura di), *Diritto amministrativo*, VII ed., Torino, 2021, p. 186, dove si afferma che la scelta discrezionale "*va eseguita valutando comparativamente tutti gli interessi pubblici (secondari), collettivi e privati presenti nella concreta fattispecie alla luce dell'interesse pubblico primario*" (la parte riportata è di E. FOLLIERI); S. LICCIARDELLO, *Diritto amministrativo. Principi, organizzazione e azione*, Firenze, 2020, p. 246.

© Wolters Kluwer Italia

evidente come si sia in presenza di un limite concettuale all'utilizzo dell'IA.

Ma la discrezionalità consiste realmente nella ponderazione dell'interesse pubblico primario con gli altri interessi in gioco? È lecito in proposito esprimere qualche dubbio, partendo da un dato che è difficilmente contestabile. Ogni decisione discrezionale muove da uno stato di realtà che si presenta all'origine problematico e da cui si evince la potenziale necessità della cura dell'interesse pubblico. Tutto il processo decisionale che si svolge attraverso il procedimento amministrativo è volto dunque alla chiarificazione di tale stato di realtà, sicché al termine di tale processo ciò che emergeva a livello di ipotesi, ossia la necessità di intervenire per tutelare l'interesse pubblico, troverà conferma oppure smentita. Nel primo caso, però, è evidente come si determini una doverosità in capo alla pubblica amministrazione di agire e dunque di assumere quella decisone che serve per curare il predetto interesse [18].

Ebbene è proprio questa doverosità che impedisce che si possa, sul piano logico prima ancora che giuridico, affermare che l'interesse pubblico sia soggetto ad una ponderazione con gli altri interessi che vengono in rilievo rispetto alla situazione di realtà. L'interesse pubblico, ove la situazione di fatto lo richieda, va infatti necessariamente curato e il problema che residua è quello di adottare la decisione che consenta di perseguirlo con il minor sacrifico possibile degli interessi secondari. Ma, affinché ciò avvenga, è necessario scegliere l'alternativa decisionale che rispecchia il peso previamente attribuito agli interessi secondari o, per meglio dire, l'ordine scaturente dal "peso" attribuito, ordine che a sua volta discende dalla consistenza di tali interessi secondari nella realtà (profilo quantitativo), dalla loro rilevanza dal punto di vista giuridico (profilo qualitativo) e dal valore che a tali interessi è stato attribuito in sede di determinazione dell'indirizzo politico o politico-amministrativo (profilo politico). La dinamica della ponderazione si inserisce (e si esaurisce) dunque in questo preciso segmento del processo decisionale e riguarda i soli interessi secondari. Detto in altri termini la necessità di intervenire per la cura dell'interesse pubblico discende unicamente dalla situazione di fatto e non certo dagli altri interessi in

[18] Quanto detto nel testo consente di recuperare la centralità del tema della doverosità in concreto della scelta discrezionale che, nella ricostruzione sulla discrezionalità oggi prevalente, sembra non trovare il giusto peso, rimanendo confinata ad una doverosità, per così dire, generica in contrasto con la centralità che tale nozione ha rispetto all'esercizio del potere non in astratto, ma in concreto.

© Wolters Kluwer Italia

essa presenti, la cui rilevanza entra in gioco solo successivamente come elemento che condiziona la scelta tra le alternative decisionali disponibili.

Dalle sintetiche considerazioni svolte discende come la discrezionalità amministrativa non vada ricostruita nei termini di una ponderazione comparativa dell'interesse pubblico primario con gli interessi secondari, bensì nei termini di una scelta volta nel contempo alla massimizzazione della cura dell'interesse pubblico e alla sua ottimizzazione dal punto di vista sociale (ossia tenendo conto del contesto di interdipendenza con gli altri interessi), scelta che dunque, fermo restando la (sola) comparazione degli interessi secondari, si risolve nell'adottare, tra le alternative decisionali, quella che arrechi il minore sacrifico possibile agli interessi secondari. Si tratta dunque di una decisione che a pieno titolo può rientrare nell'ambito della teoria della decisione razionale (piuttosto che ragionevole) rispetto alla quale viene mantenuto fermo un obiettivo preciso, che è la massimizzazione dell'interesse pubblico nel rispetto dei vincoli in precedenza indicati [19].

La riformulazione della teoria della discrezionalità può aprire nuovi orizzonti per riflettere sulla possibilità di applicare l'IA anche alle decisioni amministrative discrezionali oltre che a quelle vincolate. Se per queste ultime come detto la dottrina ha già messo a fuoco ed in par-

---

[19] Per una più compiuta riformulazione della discrezionalità, nel senso indicato nel testo sia consentito rinviare ad A. ZITO, *Teoria della scelta razionale e teoria giuridica della discrezionalità amministrativa: prolegomeni per un inquadramento sistematico*, in *Nuove Autonomie*, 2022, pp. 87 ss.; ID., *La scelta discrezionale della p.a. tra principio di esauribilità del potere e controllo effettivo sul suo esercizio: per una ridefinizione del concetto di discrezionalità*, in *Dir. amm*., 2023, p. 29 ss. La ricostruzione sinteticamente proposta nel testo della discrezionalità amministrativa riprende, peraltro, una intuizione già presente nella dottrina e troppo velocemente messa da parte, ossia che la scelta discrezionale sia volta a risolvere un problema di massimizzazione della (cura) di un interesse pubblico. È sufficiente al riguardo ricordare le considerazioni svolte da M.S. Giannini che, in relazione a questo profilo, notava come in "*un mondo immaginario, in cui ogni interesse pubblico esistesse solitario, la scelta dell'autorità dovrebbe corrispondere alla soluzione che comporta la massimizzazione di quell'interesse*". Il riferimento al mondo immaginario portava ad escludere decisamente che la discrezionalità potesse risolversi in un problema di massimizzazione proprio in ragione del fatto che nella realtà "*un interesse pubblico non esiste mai solitario ma sta insieme ad altri interessi, pubblici collettivi e privati*": v. M.S. GIANNINI, *Diritto amministrativo,* vol. I, Milano, 1970, p. 480. Ebbene, la ragione ostativa alla ricostruzione della discrezionalità come scelta di massimizzazione dell'interesse pubblico può senz'altro essere superata perché, come si è tentato di dimostrare, un problema di massimizzazione della cura di un interesse (e di scelta razionale finalizzata a ciò) si pone (e può ben essere risolto) dentro uno schema che dia rilevanza al problema dell'interdipendenza tra gli interessi.

© Wolters Kluwer Italia

te risolto i problemi della cosiddetta decisione amministrativa robotica ossia di quella che scaturisce dall'esercizio del potere vincolato, grazie anche agli orientamenti della giurisprudenza amministrativa [20], molte sono le questioni che attendono di essere affrontate in relazione all'applicazione dell'IA anche alla decisione che scaturisce dall'esercizio del potere discrezionale [21].

Non è naturalmente possibile, nell'economia del presente lavoro, esaminare in profondità questa tematica. In proposito, e nella consapevolezza che il concetto di IA sia difficile da definire con precisione [22]

---

[20] In proposito si può rinviare all'analisi svolta da A. Simoncini, *Op. cit.*, pp. 1149 ss.

[21] Su questa tematica cfr. N. Paolantonio, *Op. cit*., pp. 11 ss., il quale bene illustra la problematicità della questione ed i dubbi che essa suscita: "*Se è ancor valida – e a mio avviso lo è – l'idea che l'attività conoscitiva è strumentale alla razionalizzazione dell'azione amministrativa, bisogna altresì tenere conto dello sviluppo scientifico di tale premessa: ossia che l'attività conoscitiva precedente la decisione si concreta nella acquisizione di fatti felicemente distinti in «significativi» e «probatori», la cui doverosità di selezione esclude che l'amministrazione possa predeterminare quali fatti giudicherà rilevanti in vista della concretizzazione e realizzazione dell'interesse pubblico specifico; e ciò perché la significanza o valore indiziario dei fatti sono fissati dalle norme attributive del potere. Il principio della programmazione delle capacità predittive nelle decisioni algoritmiche «complesse» (machine e deep learning) vacilla, quindi, a fronte di un valore che non è programmabile o prevedibile ex ante, neppure attraverso un numero indefinito di casi, desunti dall'esperienza, da tradurre in dati. Si è scritto che l'amministrazione dovrebbe mediare e comporre gli interessi ex ante, e poi aggiornare ed adeguare l'algoritmo, e il giudice dovrebbe valutare correttezza e legittimità dell'agire del processo automatizzato. Tuttavia, non è facile comprendere come si possano mediare interessi ex ante: il processo ponderativo si conclude nella fase decisionale e non può quindi risolversi nel momento della fase di programmazione, altrimenti si incorrerebbe nella contradizion che nol consente, ossia quella di premettere che il machine learning, con la propria capacità di autoadeguarsi ed apprendere da sé stesso*".

[22] In proposito si è affermato nella letteratura specialistica che "*la novità più rilevante che scaturisce dall'utilizzo dei nuovi sistemi di automazione intelligente è rappresentata dalla possibilità per l'uomo di delegare alle macchine non più soltanto lo svolgimento autonomi di funzioni che, per quanto complesse, non presentano margini di imprevedibilità nell'esecuzione [...] ma anche e soprattutto di svolgere funzioni che richiedono capacità predittive in contesti di incertezza attraverso una lettura autonoma dei dati di contesto*" (cfr. S. Manzocchi - L. Romano, *Op. cit.*, p. 32). Come è evidente, l'elemento qualificante della IA è da individuare nella capacità della macchina di interagire on l'ambiente esterno acquisendo informazioni che vengono autonomamente rielaborate dalla stessa al fine di produrre l'*output* a prescindere da ogni elemento di programmazione previamente dato (è il cosiddetto fenomeno della *learning machine*). Da questo punto di vista è facile comprendere la differenza tra i robot del passato e quelli attuali: i primi operavano su una base logico-deduttiva (secondo lo schema se x allora y), mentre i secondi operano su una base statistica (y è correlato ad x) ovvero su una base logico-induttiva di tipo probabilistico (in presenza di date informa-

© Wolters Kluwer Italia

stante l'incertezza che regna sulla stessa definizione di intelligenza [23], si può però ricordare come l'elaborazione di una teoria della decisone robotica da parte degli studiosi che di tale problema si occupano (ossia in particolare i matematici, gli informatici e gli ingegneri) risulti sufficientemente chiarita nei suoi termini essenziali [24]. Affinché una tale decisione possa aversi è necessario che essa, fermo restando le informazioni di fatto disponibili e i vincoli che devono essere rispettati

---

zioni su y allora è probabile che x). Una volta scoperta la possibilità di costruire macchine intelligente, che interagiscono con il contesto e sono in grado di prendere decisioni anche sulla base delle informazioni acquisite e rielaborate dalle stesse, la ricerca sulla IA si è divisa in due autonomi campi d'indagine: da un lato vi è l'IA che si può denominare "riproduttiva", che è oggetto di studio da parte della scienza informatica ed ingegneristica, e dall'altro vi è l'IA "produttiva", che è studiata soprattutto nell'ambito delle neuroscienze: la prima "*cerca di ottenere con mezzi non biologici l'«esito» [...] del nostro comportamento intelligente, cioè risolvere problemi o svolgere compiti con successo in vista di un fine*" mentre la seconda "*cerca di ottenere l'equivalente no biologico della nostra intelligenza*" (in questo senso, L. FLORIDI, *L'intelligenza artificiale come nuova forma di agire e i suoi problemi etici*, in L. FLORIDI - F. CABITZA, *Intelligenza artificiale. L'uso delle nuove macchine. Martini Lectures*, Firenze-Milano, 2021). E se alcuni autori si dicono scettici sulla possibilità di ottenere risultati nell'ambito della IA "produttiva", secondo altri sarà possibile in un futuro non molto lontano vedere all'opera macchine con una intelligenza non umana che superano di gran lunga l'intelligenza umana. Per la prima posizione cfr. L. FLORIDI, *Op. cit*., p. 143-144, secondo cui "*l'IA «produttiva», come branca della «scienza cognitiva» interessata alla produzione di intelligenza umana (o magari anche superiore), è un fallimento completo [...] e non abbiamo davvero la minima idea di come migliorare la situazione, non fosse altro perché sappiamo veramente pochissimo della stessa intelligenza umana*". Secondo altri il traguardo sarebbe alla portata dell'uomo e non così lontano: "*molti scienziati [...] sono sicuramente d'accordo sul fatto che non c'è niente nella natura del cervello umano che renda impossibile la realizzazione di una IA. I cervelli, in fin dei conti, sono macchine biologiche che seguono le leggi di base della fisica: pertanto possono essere analizzati e modellizzati in ogni loro aspetto. Del resto se un processo cieco come l'evoluzione è stato capace di produrre l'intelligenza umana, lo stesso processo, adeguatamente ottimizzato grazie alla scienza, potrà farlo nuovamente e in modo più rapido. In questa prospettiva la IA diventa un problema fondamentalmente tecnologico dove la questione rilevante non è il se, bensì il come e, in misura minore, il quando*" (cfr. S. PARRA -M. TORRENS, *Intelligenza artificiale. La strada verso la superintelligenza*, in *Le frontiere della scienza National Geographic*, 2/2018, p. 21).

[23] Cfr. S. LEGG - M. HUTTER, *A Collection of Definitions of Intelligence*, in B. GOERTZEL - P. WANG (eds.), *Advances in Artificial General Intelligence. Concepts, Architecture and Algorithms,* pp. 17-24, (pubblicazione edita *online*), che elencano 53 definizioni scientifiche di intelligenza e 18 definizioni di IA.

[24] Cfr. in proposito A. CARCATERRA, *Machinae autonome e decisione robotica*, in A. CARLEO (a cura di), *Op. cit*., pp. 33 ss. ed in particolare p. 50 ss., dove l'Autore affronta in via diretta il tema della decisione giuridica e di quella robotica delineando parallelismi "*che possono suggerire spunti di riflessione sull'estensione del metodo di decisione robotico in campo giuridico*" ed elaborando una proposta "*per prendere decisioni secondo una metrica del valore*", p. 50.

© Wolters Kluwer Italia

(che possono attenere sia al rispetto di regole, per così dire, di natura sia al rispetto di regole giuridiche), soddisfi l'obiettivo perseguito [25].

Un passaggio ineliminabile della decisione robotica è costituito dunque dall'introduzione nel relativo processo decisionale della cosiddetta funzione obiettivo o funzione di utilità del decisore grazie alla quale verificare le conseguenze delle decisioni possibili e scegliere quella che meglio soddisfa l'obiettivo. E, sebbene l'introduzione della funzione obiettivo o di utilità avviene attraverso una valutazione quantitativa delle conseguenze delle scelte, è possibile però, come è stato di recente sottolineato, "*rendere più elastico il concetto di funzione di utilità [...] evitando di ordinare le scelte secondo un valore puramente numerico*" sicché "*ci possono essere casi in cui le decisioni si muovono su un terreno diverso, per cui anziché associare un numero ad ogni conseguenza, possiamo ordinare le conseguenze secondo un criterio di comparazione di preferenza, ossia specificando quali delle alternative preferiamo senza stilare una graduatoria assoluta, ma una graduatoria relativa e condizionale*" [26].

Senza andare oltre in un discorso che meriterebbe un approfondimento specifico, è però evidente come da quanto detto emerga a sufficienza un fatto: la ricostruzione dell'esercizio della discrezionalità della p.a. nei termini di una decisione che rientra nell'ambito della teoria della scelta razionale apre nuovi scenari alla riflessione sulla possibilità di una decisione amministrativa robotica discrezionale che sarebbero senz'altro preclusi o resi più difficili ove, si continuasse ad utilizzare la definizione tradizionale.

A conferma di ciò è sufficiente seguire la riflessione svolta dall'Autore il cui pensiero è stato appena citato. Dopo avere premesso che qualunque decisione robotica può essere così scomposta "*la decisione S è azione collocata nel presente, si basa sull'esame dei dati passati, su una ipotesi di sviluppo degli scenari futuri, sul rispetto dei vincoli/regole ed è finalizzata alla massimizzazione della funzione di utilità U*" [27] e che dunque "*la funzione obiettivo U dipende dal presente attraverso S, dal passato P, dal futuro F e dalle regole R*" da cui consegue "*sinteticamente: U (S, P, F, R)*" [28], viene precisato che il problema della decisione giuridica robotica è quello di stabilire l'analogo giuridico degli elementi P, F, R e U.

---

[25] *Id.*, p. 45.
[26] *Id.*, p. 46.
[27] *Id.*, p. 48.
[28] *Id.*, p. 50.

© Wolters Kluwer Italia

Ebbene ciascuno di questi elementi è presente nella decisione discrezionale della p.a. se ricostruita come una decisione razionale sul modello della teoria della scelta razionale. Ed infatti, fermo restando la decisione S da assumere (ossia il provvedimento amministrativo) finalizzata alla massimizzazione della cura dell'interesse pubblico (ossia la funzione obiettivo U), è evidente come tale decisione si basi sull'esame dei dati P, su una ipotesi di sviluppo degli scenari futuri F (ossia l'elaborazione delle alternative decisionali) e sul rispetto dei vincoli normativi R.

Per lo meno dal punto di vista strutturale, dunque, esistono importanti analogie tra la decisione robotica e la decisone amministrativa discrezionale, ricostruita come decisione razionale, che possono essere proficuamente esplorate così da aprire una nuova strada all'esercizio efficace della funzione amministrativa.

Il che peraltro non significa che dalla possibilità concettuale di una decisione discrezionale affidata all'IA si debba passare alla sua applicazione pratica, perché altri potrebbero essere i motivi ostativi non ultimi quelli che emergenti da una meditata ed organica analisi del regolamento europeo.

© Wolters Kluwer Italia

Sezione Terza

LE QUESTIONI CONNESSE ALL'USO DELLE NUOVE TECNOLOGIE NEL PROCESSO E LA GIUSTIZIA PREDITTIVA

LA GIUSTIZIA AMMINISTRATIVA DIGITALE *

LAURA ANCORA

SOMMARIO: 1. Premessa. – 2. IA come giudice: una negazione dello Stato di diritto. – 3. L'uso strumentale dell'IA da parte del giudice: vantaggi e criticità.

Abstract: The topic of the digital administrative justice has been widely debated over the past few years. Specifically, it can be analysed from different points of view. First of all, this subject matter can be examined in reference to electronic administrative process. In particular, it is necessary to verify how new advances in technology have affected the organisation of administrative process. Moreover, this topic concerns the possibility of reaching robotic judicial decisions, which will be examined in this essay. In this regard, there are two supposable models: the first one involves the complete replacement of a judge by the AI, while the second one postulates AI as a tool to assist the judge in resolving dispute. Therefore, the possible compatibility of the implementation of these models in the administrative process with the right to due process will be verified. Indeed, the implementation of these models would allow a greater efficiency and speed but, at the same time, the observance of the constitutional guarantees could be damaged.

1. Premessa

L'intelligenza artificiale (o IA) [1] interessa la giustizia amministra-

* Contributo sottoposto a doppio referaggio in forma anonima.

[1] Occorre avvertire che non esiste una definizione di IA generalmente condivisa: tendenzialmente, essa viene definita quale la tecnologia che consente ad un *computer*

© Wolters Kluwer Italia

tiva sotto due profili differenti [2]: in primo luogo, essa rileva quale oggetto del giudizio. Difatti, il crescente utilizzo di tecnologie all'interno del procedimento amministrativo – con le connesse problematiche che ne derivano [3] – impone una rimodulazione delle tecniche di sindacato giurisdizionale, stante l'esigenza di adattare le tradizionali categorie giuridiche alla nuova realtà emergente.

In secondo luogo, si pone la questione in ordine alla possibilità di addivenire a decisioni giudiziali robotiche. A tal proposito, due sono i modelli ipotizzabili: il primo si risolve nell'integrale sostituzione del giudice da parte dell'IA, sì da comportare quello che viene definito

---

di analizzare una grande quantità di dati e, in forza della conoscenza e dell'esperienza acquisita, adottare comportamenti intelligenti e/o proporre decisioni. Secondo la definizione elaborata dalla Commissione europea (comunicazione "*L'intelligenza artificiale per l'Europa*", 25 aprile 2018), con l'espressione intelligenza artificiale si indicano "*i sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi*". Sulla nozione di IA v., *ex pluribus*, M.A. BODEN, *Artificial intelligence: a very short introduction*, Oxford, 2018; R. CALO, *Artificial intelligence Policy: A Primer and Roadmap*, in *UCDL Rev.*, 2017, pp. 404 ss.; J. COPELAND, *Artificial Intelligence: A Philosophical Introduction*, Oxford-Malden, Massachusetts, 1993.

[2] Per dovizia espositiva occorre evidenziare che il tema della giustizia amministrativa interessa, oltre ai profili indicati nel testo, anche la digitalizzazione del processo, inteso quale flusso di informazioni e atti preliminari rispetto alla decisione giudiziale. Per un approfondimento sul processo amministrativo telematico (c.d. Pat) v., fra gli altri, F. FRENI - P. CLARIZIA, *Il nuovo processo amministrativo telematico*, Milano, 2016.

[3] La letteratura sul tema è amplissima: si rimanda, senza pretesa di completezza, a G. AVANZINI, *Decisioni amministrative e algoritmi informatici. Predeterminazione, analisi predittiva e nuove forme di intelligibilità*, Napoli, 2019; E. CARLONI, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm*., 2/2020, pp. 271 ss.; L. CASINI, *Lo Stato nell'era di Google. Frontiere e sfide globali*, Città di Castello, 2020; A. CASSATELLA, *La discrezionalità amministrativa nell'età digitale*, in *Scritti per Franco Gaetano Scoca*, vol. I, Napoli, 2020, pp. 675 ss.; M.C. CAVALLARO - G. SMORTO, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *Federalismi.it*, 2019; R. CAVALLO PERIN - D.U. GALETTA (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020; S. CIVITARESE MATTEUCCI, *"Umano troppo umano". Decisioni amministrative automatizzate e principio di legalità*, in *Dir. pubbl*., 1/2019, pp. 5 ss.; S. CIVITARESE MATTEUCCI - L. TORCHIA, *La tecnificazione*, Firenze, 2016; B. MARCHETTI, *La garanzia dello "*human in the loop*" alla prova della decisione amministrativa algoritmica*, in *BioLaw Journal*, 2/2021, pp. 367 ss.; D. MARONGIU, *L'automazione delle decisioni amministrative: teorie, esperienze e sentenze*, in *Scritti per Franco Gaetano Scoca*, vol. IV, cit., pp. 3369 ss.; N. PAOLANTONIO, *Il potere discrezionale della pubblica automazione. Sconcerto e stilemi. (Sul controllo giudiziario delle "decisioni algoritmiche")*, in *Dir. amm*., 4/2021, pp. 813 ss.; L. PREVITI, *La decisione amministrativa robotica*, Napoli, 2022; M. SIMONCINI, *L'agire provvedimentale dell'amministrazione e le sfide dell'innovazione tecnologica*, in *Riv. trim. dir. pubbl*., 2/2021, pp. 529 ss.

© Wolters Kluwer Italia

quale "*vero e proprio genocidio*" dell'autorità giudiziaria come essere umano [4]; il secondo modello, di contro, postula l'IA quale strumento di ausilio del giudice nella risoluzione della controversia che, dunque, si concluderebbe pur sempre con una decisione umana [5].

Ebbene, oggetto di questo scritto sarà quest'ultimo profilo ora menzionato: segnatamente, ci si interrogherà sulle ripercussioni, specie in tema di garanzie costituzionali e convenzionali, di un sistema giustizia così concepito, atteso che in Italia – diversamente da altri Stati come Canada, Stati Uniti, Cina e Regno Unito – non si è ancora registrato l'impiego di strumenti di intelligenza artificiale all'interno del processo [6].

---

[4] Così, M. Luciani, *La decisione giudiziaria robotica*, in *Rivista AIC*, 3/2018, p. 871.

[5] A tal proposito, oltre alla letteratura citata nelle pagine successive, v., *ex pluribus*, F. Patroni Griffi, *La decisione robotica e il giudice amministrativo*, in A. Carleo (a cura di), *Decisione robotica*, Bologna, 2019, pp. 165 ss.; T. Sourdin, *Judges, Technology and Artificial Intelligence. The artificial Judge*, Cheltenham, 2021.

[6] Per completezza espositiva, si rammenta che il g.a. ha, invece, avuto già modo di pronunciarsi sull'attività amministrativa c.d. algoritmica, ossia quella caratterizzata per il ricorso – in sede procedimentale – allo strumento informatico del calcolo algoritmico. In particolare, dalle poche pronunce che si registrano sul tema, il giudice amministrativo, pur salutando con favore l'impiego di tali strumenti da parte della P.A. visti i plurimi vantaggi che ne derivano soprattutto alla luce della considerevole riduzione della tempistica procedimentale, asserisce però che "*l'utilizzo di procedure «robotizzate» non può, tuttavia, essere motivo di elusione dei principi che conformano il nostro ordinamento e che regolano lo svolgimento dell'attività amministrativa*", sicché "*la regola algoritmica deve essere non solo conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato del giudice amministrativo*". Così, Cons. St., sez. VI, 8 aprile 2019, n. 2270. Nei medesimi termini, Cons. St., sez. VI, 4 febbraio 2020, n. 881, che, ribadendo l'esigenza di assicurare le generali garanzie procedimentali anche con riferimento all'attività amministrativa algoritmica, ha enucleato i principi che devono orientare l'impiego di strumenti informatici da parte dell'Amministrazione: più dettagliatamente, essi si compendiano nei principi di conoscibilità, di non esclusività della decisione algoritmica e di non discriminazione algoritmica. In questo senso, fra le altre, Cons. St., sez. VI, 13 dicembre 2019, n. 8472; TAR Lazio, Roma, sez. III *bis*, 22 marzo 2017, n. 3769; TAR Lazio, Roma, sez. III *bis*, 1° luglio 2020, n. 7526. Per una ricostruzione degli indirizzi giurisprudenziali sul punto, v., *ex multis*, R. Ferrara, *Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale*, in *Dir. amm*., 4/2019, pp. 773 ss.; D.U. Galetta, *Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia*, in *Riv. dir. pubbl. com*., 3/2020, pp. 501 ss.; N. Mucciaccia, *Algoritmi e procedimento decisionale: alcuni recenti arresti della giustizia amministrativa*, in *Federalismi.it*, 2020; I.A. Nicotra - V. Varone, *L'algoritmo, intelligente ma non troppo*, in *Rivista AIC*, 4/2019; N. Posteraro, *Procedimento amministrativo e decisione amministrativa robotizzata: gli orientamenti della giurisprudenza amministrativa*, in *Irpa.eu*, 2020; A. Sola, *La giurisprudenza e la sfida*

© Wolters Kluwer Italia

L'approfondimento di questa tematica risulta, a ben vedere, quanto mai di preminente interesse: si tratta, invero, di un'evenienza non soltanto avvincente e al contempo inquietante [7], ma altresì di grande attualità. Infatti, come si avrà modo di osservare nel prosieguo della trattazione, si è assistito ad un progressivo interesse da parte del Legislatore al tema in esame, sicché si può ragionevolmente preconizzare un imminente utilizzo di tali strumenti all'interno del processo anche nel nostro Paese.

Pertanto, se, come è stato acutamente osservato, il compito della scienza giuridica è "*quello di interpretare, ordinare a sistema, presentare nuovi punti di vista, partecipare all'elaborazione di nuove norme o di riforme*" [8], non ci si può esimere dal domandarsi se e in che termini l'IA potrebbe incidere sulle situazioni giuridiche soggettive e sulle prerogative dei cittadini nel processo. Solo in questo modo, infatti, sarà possibile evitare che l'intelligenza artificiale da strumento di ausilio, ora della P.A. ora del giudice, diventi una sistematica forma di abuso dei diritti delle parti del giudizio.

Peraltro, non si può fare a meno di notare che un più attento esame della tematica *de qua* si impone soprattutto per la dottrina amministrativistica, atteso che il processo amministrativo si atteggia a divenire, come detto, lo spazio deputato a giudicare l'intelligenza artificiale con l'intelligenza artificiale.

2. IA come giudice: una negazione dello Stato di diritto

Come anticipato, una delle possibili applicazioni dell'IA al processo potrebbe risolversi nell'introduzione di un giudice robot, con integrale soppressione della figura del giudice umano.

I sostenitori di tale modello, già sperimentato in altri ordinamenti quali quello estone [9], facendo propri i risultati degli studi scientifici sul

---

dell'utilizzo di algoritmi nel procedimento amministrativo, in *Giustamm*., 2020; A. VALSECCHI, *La spersonalizzazione della funzione giudicante: un primo sguardo sulla giustizia algoritmica*, in *La Rivista del Gruppo di Pisa*, 3/2021, pp. 625 ss.

[7] In questi termini, G. ALPA, *L'intelligenza artificiale. Il contesto giuridico*, Modena, 2021, p. 10.

[8] S. CASSESE, *Degli usi e abusi della giurisprudenza (e dei suoi limiti) nel diritto pubblico*, in *Riv. it. sc. giur*., 4/2013, p. 142.

[9] In Estonia, è stata introdotta la figura del giudice robot per la risoluzione delle controversie civili di minore valore economico (fino a € 7000). In particolare, il sistema sperimentato prevede che le parti del giudizio carichino atti e documenti su una piattaforma in modo che l'algoritmo, in base agli stessi, possa pervenire ad una decisione, salva la possibilità di fare appello ad un giudice umano. Per una rassegna dei

© Wolters Kluwer Italia

tema, sostengono che l'IA – quantomeno quella c.d. forte (*strong AI*) [10] – non solo risulta indistinguibile dall'umano, ma è altresì idonea a superarlo in termini di capacità di azione e ragionamento. Più dettagliatamente, si pone in rilievo che la macchina non solo ha la capacità di operare incessantemente e più celermente dell'umano (con evidenti effetti positivi sulla deflazione del contenzioso), ma anche che la stessa è priva di tutti quei preconcetti e di stati d'animo che confluiscono in qualsiasi determinazione umana, dunque anche in quella giudiziale [11]. Pertanto, alla luce di tali rilievi, si asserisce che "algorithms do better than humans in the role of final decision maker" [12].

Un siffatto modello, a ben vedere, non si può certamente impiantare nell'ordinamento nostrano, ponendosi irrimediabilmente in contrasto con i principi e le garanzie minime di ogni Stato di diritto [13]: un giudizio deciso da un giudice robot, infatti, non è idoneo ad assicurare nessuna delle garanzie imposte dal principio del giusto processo, se non esclusivamente quella di pervenire ad una decisione in tempi rapidissimi. Tuttavia, non si può certamente ritenere che l'esigenza di celerità e speditezza dei processi possa giustificare il sacrificio delle restanti garanzie di cui agli artt. 111 Cost. e 6 CEDU e ciò, si badi, quand'anche un siffatto modello dovesse essere circoscritto alle sole controversie bagatellari come pure è stato proposto da taluno [14]. Il valore della controversia, invero, non può legittimare un *minus* (*rectius* una totale compressione) delle garanzie costituzionali e convenzionali predette.

---

diversi modelli di IA impiegati nei processi di plurimi Stati, v. A.A. Martino, *Chi teme i giudici robot*, in *Riv. it. infor. e dir.*, 2/2020, pp. 15 ss.

[10] Per completezza espositiva, si rammenta la dicotomia tra IA debole (*weak AI*) e IA forte (*strong AI*) risiede nel fatto che la prima è tesa a svolgere specifici compiti senza, però, poter comprendere e quindi operare al di fuori della funzione designata; la seconda, invece, possiede capacità cognitive simili a quelle umane che le consentono di comprendere e risolvere problemi in modo autonomo.

[11] In questi termini, fra gli altri, D. Kahneman - O. Sibony - C.R. Sunstein, *Noise: a flaw in human Judgment*, New York, 2021, p. 37, per i quali "noise in human judgment is as undesirable variability in judgments of the same problem".

[12] D. Kahneman - A.M. Rosenfield - L. Gandhi - T. Blaser, *Noise: How to Overcome the High, Hidden Cost of Inconsistent Decision Making. Algorithmic judgment is more efficient than human variety*, in *Harvard Business Review*, 2016.

[13] In questo senso, fra gli altri, B. Marchetti, *Giustizia amministrativa e transizione digitale. Spunti per riflettere su un futuro non troppo lontano*, in M. Ramajoli (a cura di), *Una giustizia amministrativa digitale?*, Bologna, 2023, p. 66; L. De Renzis, *Primi passi nel mondo della giustizia "*high tech*": la decisione in un corpo a corpo virtuale fra tecnologia e umanità*, in A. Carleo (a cura di), *Decisione robotica*, cit., pp. 139 ss.

[14] R. Susskind, *Online Courts and the Future of Justice*, Oxford, 2019, pp. 287 ss.

© Wolters Kluwer Italia

Da ultimo, una limitazione di tal fatta all'impiego dei sistemi di IA all'interno del processo si rinviene nel disegno di legge n. 1146 recante "*Disposizioni e delega al Governo in materia di intelligenza artificiale*". In particolare, all'art. 14, comma 1, è previsto che i sistemi di IA possono essere utilizzati solamente per l'organizzazione e la semplificazione del lavoro giudiziario e per la ricerca giurisprudenziale e dottrinale, sicché, al comma 2, viene riconosciuta una riserva esclusiva a favore del giudice per quanto concerne l'interpretazione della legge, la valutazione dei fatti e delle prove, nonché l'adozione di ogni provvedimento [15].

Infine, conformemente agli insegnamenti di Filosofia del diritto, non ci si può esimere dal notare che il diritto – da considerarsi nella sua pienezza – non è solo scienza, ma è altresì esperienza umana, che rappresenta comunque una forma di conoscenza, dalla quale non si può certo prescindere per comprendere e, quindi, giudicare i fatti umani [16]. "*Questa umanità*", difatti, "*che comprende una sensibilità per le situazioni sottoposte al suo giudizio, permette al giudice di considerare la dimensione umana delle sue decisioni. Spetta a lui, nella valutazione dei fatti come nella fase decisionale, trovare un equilibrio tra empatia, compassione, comprensione, rigore e severità, in modo che la sua applicazione del diritto sia avvertita come legittima e giusta*" [17].

3. L'uso strumentale dell'IA da parte del giudice: vantaggi e criticità

Se quella del giudice robot è, come visto poc'anzi, un'evenienza incompatibile con le garanzie proprie di ogni Stato di diritto quale

---

[15] Tale previsione è, a ben vedere, in linea con il regolamento UE 2024/1689 (c.d. *AI Act*), ove sono stati considerati ad alto rischio i sistemi di IA destinati all'amministrazione della giustizia, alla luce del loro impatto potenzialmente significativo sulla democrazia, sullo Stato di diritto, sulle libertà individuali nonché sul diritto a un ricorso effettivo e a un giusto processo.

[16] In questi termini anche S. SATTA, *La vita della legge e la sentenza del giudice*, in *Soliloqui e colloqui di un giurista*, Padova, 1968; G. CAPOGRASSI, *Studi sull'esperienza giuridica*, in *Opere*, vol. II, Milano, 1959, pp. 211 ss.; V. COLESANTI, *Sulla legittimazione a giudicare (meditazioni su un altro pensiero "chi sono io per giudicare")*, in *Riv. trim. dir. proc. civ.*, 4/2019, pp. 1081 ss. Per una ricostruzione dei rapporti tra giustizia digitale e umanità del giudice, v. pure S. GABORIAU, *Libertà e umanità del giudice: due valori fondamentali della giustizia. La giustizia digitale può garantire nel tempo la fedeltà a questi valori?*, in *Questione Giustizia*, 4/2018, pp. 200 ss.

[17] *Report* di deontologia giudiziaria 2009-2010 dell'*European Networks of Councils for the Judiciary* (ENCJ).

© Wolters Kluwer Italia

quello nostrano, occorre a questo punto della disamina verificare se ed in che termini il giudice possa far uso, in funzione strumentale, dell'IA. Invero, se è fuor dubbio che l'utilizzo dell'intelligenza artificiale all'interno del processo potrà comportare innegabili vantaggi per il sistema giustizia (v. *infra*), è altresì necessario individuare specifici limiti (oltre a quelli già menzionati) all'impiego della stessa: infatti, non è affatto remoto il rischio che l'IA possa risolversi in una "*rivoluzione numerica*" nella quale si possa concretamente abbandonare la "*liturgia della parola*" per "*decidere senza giudicare*" [18].

Ebbene, a tal riguardo, l'indirizzo dottrinale assolutamente maggioritario afferma – condivisibilmente – che l'autorità giudiziaria può ricorrere agli strumenti di IA, tra cui i sistemi di giustizia predittiva, soltanto fino al momento della decisione, atteso che quest'ultima non rappresenta semplicemente il momento conclusivo di ogni giudizio, ma costituisce, piuttosto, il nucleo essenziale e irrinunciabile dello stesso [19]. Pertanto, anche laddove si dovesse assistere all'utilizzo dell'IA nel processo, il potere decisorio del giudice dovrebbe rimanere immutabile: in questa prospettiva, quindi, egli potrà decidere se accostarsi o meno alle raccomandazioni della macchina.

Dunque, l'impiego dell'IA all'interno del processo, seppur così circoscritto, potrà produrre notevoli vantaggi per il sistema giudiziario: si pone in rilievo, invero, che "*il ricorso agli algoritmi nel processo consentirebbe forse all'interprete di affrontare con maggiore consapevolezza il peso dei precedenti e le prospettive di evoluzione, operando [...] come una sorta di specchio, nel quale si riflettono e si rendono trasparenti anche le storture del sistema*" [20].

In questo modo, allora, si potrebbe porre un freno a quello che viene da taluno definito come il "*diritto incalcolabile*" [21] proprio "*dell'età della giurisdizione*" [22], ossia al fenomeno, registratosi soprattutto a par-

---

[18] V. Manes, *L'oracolo algoritmico e la giustizia penale*, in V. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, p. 567.

[19] A. Pajno, *L'uso dell'intelligenza artificiale nel processo tra problemi nuovi e questioni antiche*, in *BioLaw Journal*, 1/2022, p. 217. Negli stessi termini, *ex multis*, U. Ruffolo, *Giustizia predittiva, decisione algoritmica e ruolo ancillare della macchina come ausiliare necessario del giudice umano*, in A. Pajno - F. Donati - A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol. II, *Amministrazione, responsabilità, giurisdizione*, Bologna, 2022, pp. 453 ss.

[20] L. Torchia, *La giustizia amministrativa digitale*, in M. Ramajoli (a cura di), *Una giustizia amministrativa digitale?*, cit., p. 56.

[21] Così, N. Irti, *Un diritto incalcolabile*, in *Riv. dir. civ.*, 1/2015, pp. 11 ss., ora in Id., *Un diritto incalcolabile*, Torino, 2015, pp. 3 ss.

[22] In questi termini, A. Di Porto, *Calcolo giuridico secondo la legge nell'età del-*

© Wolters Kluwer Italia

tire dagli anni Novanta del secolo scorso, per cui la giurisprudenza si è riconosciuta una sempre maggiore discrezionalità e creatività nella sua attività sì da compromettere la certezza del diritto [23] e, conseguentemente, l'affidamento dei cittadini. In un simile contesto, dunque, il massiccio impiego degli algoritmi potrebbe certamente giovare alle distonie ora rilevate, dando nuova linfa all'esigenza di prevedibilità e stabilità del diritto [24].

Tuttavia, vi è chi evidenzia che la previsione della mera strumentalità della macchina non esclude – per ciò solo – il pericolo di un suo dominio: in particolare, a tal proposito, si è soliti parlare di "effetto *moutonnier*" (*i.e.* "effetto pecorone") [25] per indicare la difficoltà che molto probabilmente incontrerebbe il giudice nel discostarsi dall'esito suggerito dall'algoritmo, finendo così a delegare il giudizio al calcolo automatico. Più dettagliatamente, si nota che, una volta introdotto un sistema automatico di decisione all'interno di un processo decisionale umano, non può negarsi che "*il sistema automatico tende, nel tempo, a catturare la decisione stessa*", specie se si consideri la "*forza «pratica» di qualsiasi automatismo valutativo che, da un lato, solleva il decisore dal* burden of motivation*, dal peso dell'esame e della motivazione; dall'altro, gli consente di «qualificare» la propria decisione con il crisma della «scientificità» e della «neutralità» che oggi circonda la valutazione algoritmica*" conferendole una sorta di autorità indiscussa [26].

Evidentemente, se questo rischio paventato si dovesse effettivamente verificare, si avrebbe solo la parvenza di un utilizzo strumentale dell'IA da parte del giudice, finendo – nei fatti – a realizzarsi l'affermazione della figura del giudice robot prima negata con forza.

Peraltro, a tal proposito, non si può non osservare che se ciò dovesse effettivamente verificarsi, non solo non si registrerebbe più un'evoluzione degli indirizzi pretori che, specie nel diritto amministrativo (basti pensare alla tutela cautelare), hanno consentito alla giurispruden-

---

la giurisdizione. Il ritorno al testo normativo, in A. CARLEO (a cura di), *Calcolabilità giuridica*, Bologna, 2018, p. 123.

[23] Sulla nozione di certezza, cfr. G. ALPA, *La certezza del diritto nell'età dell'incertezza*, Napoli, 2006; G. GOMETZ, *La certezza giuridica come prevedibilità*, Torino, 2005.

[24] Sul punto, M. LUCIANI, *La decisione giudiziaria robotica*, cit., pp. 875-876, ricorda che "*lo Stato moderno nasce (nel disastro delle guerre civili e di religione) come erogatore di prestazioni di sicurezza (fisica) per i sudditi e la certezza giuridica non è altro che la proiezione della sicurezza nel dominio del diritto. Statualità, sicurezza e certezza sono, dunque, una triade politica indissolubile*".

[25] Trattasi di un'espressione, oggi largamente impiegata in letteratura, coniata da A. GARAPON - J. LASSÉGUE, *Justice digitale*, Paris, 2018.

[26] A. SIMONCINI, *Op. cit.*, p. 81.

© Wolters Kluwer Italia

za – spesso a fronte dell'inerzia del Legislatore – di tutelare in maniera più efficace le pretese dei cittadini, ma vi sarebbe altresì una violazione dell'art. 101 Cost., in quanto il giudice verrebbe ad essere subordinato non più alla legge, bensì alla giurisprudenza.

Ora, non si può certo asserire che l'esigenza di certezza del diritto, sebbene centrale nel nostro ordinamento giuridico, possa dirsi che essa costituisca l'esigenza primaria. Infatti, differentemente dai sostenitori della teoria weberiana del diritto calcolabile [27], si ritiene che ai precedenti giurisprudenziali debba essere certamente riconosciuto un peso, come peraltro depongono una serie di disposizioni quale l'art. 99 c.p.a., ma al contempo non è senz'altro auspicabile, per le ragioni summenzionate, un'aprioristica stagnazione degli orientamenti pretori [28]. Il passato, quindi, non può divenire indiscussa regola per il futuro.

Pertanto, al fine di scongiurare i pericoli ora paventati in ordine alla giustizia amministrativa digitale, si dovrebbe addivenire ad una maggiore valorizzazione della garanzia della motivazione della pronuncia giudiziale. Il giudice, invero, non potrà limitarsi a far proprie le raccomandazioni della macchina, ma dovrà argomentare in maniera logica, coerente ed esaustiva, le ragioni per le quali ritiene che la predizione operata dalla macchina sia applicabile anche al caso di specie. Solo in questa maniera, dunque, si eviterà l'asettico conformismo giudiziario e il giudice manterrà il suo ruolo di *peritus peritorum* all'interno del processo, sebbene tale espressione acquisterà un significato parzialmente differente in quello che sarà il futuro della giustizia amministrativa.

---

[27] Per un approfondimento, v. M. Weber, *Economia e società*, vol. II, Milano, 1974.

[28] Sul valore del precedente, si rimanda a A. Carleo (a cura di), *Il vincolo giudiziale del passato. I precedenti*, Bologna, 2018.

© Wolters Kluwer Italia

GIUDIZIO DI DIRITTO, PREVEDIBILITÀ DELLE DECISIONI E INTELLIGENZA ARTIFICIALE *

MATTEO CECILIA

SOMMARIO: 1. Interrogativi strutturali sull'interpretazione e possibile ruolo dell'intelligenza artificiale. – 2. La distopia di un'intelligenza artificiale sostitutiva del giudice. – 3. L'IA quale ausilio per l'attività del giudice.

Abstract: The judge's activity is an interpretative activity the result of which is uncertainty. Furthermore, the exercise of the jurisdictional function passes through the attribution of meaning to the delegation received. The judge exercises a discretionary power that is qualitatively homogeneous to that of all other delegates to exercise administrative powers, without the possibility of directing the values of the social group of reference. Since it is impossible to administer justice by law, the desire to satisfy the needs of legal certainty could push lawyers to hastily rely on new machines. However, artificial intelligence (AI) will never be able to replace the human judge in light of the unavoidable margins of discernment of the judge delegate, as it is not equipped with the sensitivity necessary for this. AI could assist the judge: for example, it is able to simultaneously compare the weight of different interpretative arguments while remaining immune to any emotional influence.

1. Interrogativi strutturali sull'interpretazione e possibile ruolo dell'intelligenza artificiale

Accrescendosi la complessità della vita associata, si è sempre più sentito il bisogno di limitare i margini di operatività dell'organo di giu-

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

stizia, tanto che la funzione giurisdizionale è stata delegata, secondo certi limiti e regole, a specifiche figure tecniche [1]. Con il passaggio dal cosiddetto "diritto dei giuristi" alle codificazioni moderne la legge è divenuta un punto di riferimento fondamentale per il giudice in un'ottica di esaltazione della sovranità popolare che si esprime attraverso i suoi rappresentanti.

Già in questo senso l'attività del giudice è un'attività interpretativa in quanto egli deve attribuire un significato ad un simbolo oggettivo [2].

E ogni attività ermeneutica pone un problema comunicativo: la relazione tra referente e significante, infatti, ha natura convenzionale e può essere intesa diversamente dai destinatari della comunicazione [3]. Occorre, dunque, comprendere se debba essere ricercata la volontà effettiva dell'autore, se debba aversi riguardo al significato del simbolo in sé e per sé considerato o se l'esegeta vi possa aggiungere qualcosa di suo, considerando che si pone l'esigenza in questo campo di conciliare la soggettività dell'interprete con la legalità e la prevedibilità [4] e che l'attività del giudice, privo di legittimazione popolare, non si sovrapponga a quella del legislatore.

Il giudice è, però, condizionato non solo dalle indicazioni legislative, ma l'esercizio della sua funzione passa attraverso l'attribuzione di

---

[1] Il diritto ha assunto così sempre più la connotazione di un sapere per specialisti.

[2] Cfr. E. BETTI, *Interpretazione della legge e degli atti giuridici (teoria generale e dogmatica)*, Milano, 1949; L. BIGLIAZZI GERI, *L'interpretazione. Appunti delle lezioni di teoria generale del diritto*, Milano, 1994; V. ROPPO, *Il concetto di interpretazione del diritto*, Torino, 1947; G. TARELLO, *L'interpretazione della legge*, in A. CICU - F. MESSINEO (diretto da), *Trattato di diritto civile e commerciale*, Milano, 1980; F. VIOLA - G. ZACCARIA, *Diritto e interpretazione. Lineamenti di teoria ermeneutica del diritto*, Roma-Bari, 2016; G. ZACCARIA, *L'arte dell'interpretazione. Saggi sull'ermeneutica giuridica contemporanea*, Padova, 1990; ID., *Il giudice e l'interpretazione*, in *Pol. dir.*, 3/2006, pp. 461-474; ID., *I giudizi di valore nell'interpretazione giuridica*, in *Persona y Derecho*, 61/2009, pp. 103-113; ID., *L'interpretazione della legge*, in *Enc. dir., Annali*, vol. V, 2012, pp. 694-709; ID., *Legalità e legittimità, bilanciamento e proporzionalità nell'interpretazione giuridica*, in M. BERTOLISSI (a cura di), *Scritti per Paolo Grossi offerti dall'Università di Padova*, Torino, 2019, pp. 463-482; ID., *Introduzione a "Ars Interpretandi"*, 2/2021, pp. 7-20.

[3] Cfr. F. DE SAUSSURE, *Corso di linguistica generale*, Bari, 1970; J. ESSER, *Precomprensione e scelta del metodo nel processo di individuazione del diritto*, Napoli, 1983; B. LUZZATI, *Interpretazione della legge, interpretazione del diritto e interpretazione nel diritto*, in *Scritti per Luigi Lombardi Vallauri,* Padova, 2016.

[4] Cfr. L. FERRAJOLI, *Contro il creazionismo giudiziario*, Modena, 2018, pp. 24 ss.; R. GAROFOLI, *Il giudice tra creatività interpretativa e esigenze di legalità e prevedibilità*, in *Federalismi.it*, 2019; N. IRTI, *Un diritto incalcolabile*, Torino, 2016; M. TARUFFO, *Legalità e giustificazione della creazione giudiziaria del diritto*, in *Riv. trim. dir. proc. civ.*, 1/2001, pp. 11 ss.

© Wolters Kluwer Italia

significato alla delega ricevuta. Si potrebbe allora configurare nell'attività giudiziale un potere discrezionale qualitativamente omogeneo a quello di tutti gli altri delegati all'esercizio di poteri amministrativi, col suo particolare contenuto [5].

In estrema sintesi, il giudice, quale delegato, ha anche oggi un certo margine di manovra entro una determinata cornice.

Essa è rappresentata, quale limite inferiore, dalla non passiva applicazione di soluzioni già impacchettate dalla politica. Al giudicante permane una sussidiaria possibilità di attingere direttamente allo spirito del gruppo di appartenenza [6]. Gli organi che svolgono una funzione di giustizia, infatti, sono inevitabilmente condizionati dal parametro esterno rappresentato dalla scala di valori del gruppo di appartenenza, subendo, in questa prospettiva anche una qualche forma di controllo sociale [7].

Il limite superiore di tale cornice è costituito, invece, dall'assenza di poteri di indirizzo politico-amministrativo. Un potere di indirizzo dei valori comuni del gruppo sociale di riferimento è, infatti, riconosciuto in via generale solo all'organo politico.

Non è possibile, dunque, amministrare la giustizia solo per legge; la funzione giurisdizionale non può essere erosa fino all'annichilimento dalla normazione. Permangono ineliminabili margini di operatività del delegato-giudice nella dialettica fra istruzioni e discernimento.

È da rigettare, quindi, anche solo l'idea dell'opportunità e della idoneità della legislazione a disciplinare nel dettaglio ogni aspetto della vita sociale, col giudice che si limita ad affermarne il volere nel singolo caso.

In questo quadro, lo spasmodico desiderio di soddisfare le esigenze di certezza giuridica, intesa come prevedibilità delle conseguenze dei comportamenti sociali, e di controllo dell'organo di giustizia potrebbe spingerci ad affidarci frettolosamente ad una scienza esatta quale la matematica, soprattutto ora che le macchine che ne fanno applicazione sono divenute, oltre che veloci nell'effettuare operazioni, anche intelligenti [8]. A tal punto da arrivare a pensare che l'odierno auto-

---

[5] Cfr. R. Lupi, *Il diritto tra discrezionalità e interpretazione. Profili generali e riflessi sulla fiscalità*, Napoli, 2004.

[6] Cfr. P. Grossi, *Ritorno al diritto*, Roma-Bari, 2019.

[7] Già ai tempi della cosiddetta *giustizia ritenuta*, la società si aspettava che chi esercitava tale funzione si facesse interprete e tenesse conto dei propri valori comuni, anche dando a questi un certo indirizzo.

[8] Cfr. F. Palazzo, *Considerazioni minime sulla prevedibilità della decisione giudiziale (tra miti, illusioni e pragmatismi)*, in *Cass. pen.*, 3/2022, pp. 941 ss.

© Wolters Kluwer Italia

ma possa divenire bocca della legge [9] o dei precedenti giurisprudenziali o dei valori della società di riferimento.

2. La distopia di un'intelligenza artificiale sostitutiva del giudice

Occorre preliminarmente considerare che, ferma restando la mancanza di una definizione univoca di "intelligenza artificiale" [10], se ne possono individuare due forme.

L'intelligenza artificiale "forte" è quella in grado di operare in modo del tutto autonomo, manifestando anche la capacità di auto-apprendere.

Essa, in linea puramente teorica, potrebbe, dunque, effettivamente sostituire l'organo di giustizia nello svolgimento della sua funzione, tanto da potersi parlare di *giudice robot* [11] e di produzione automatica della sentenza. Ciò evidentemente nell'ottica (o meglio, nella speranza) di assicurare la calcolabilità del diritto [12] e la possibilità di prevedere come esso verrà applicato nel caso concreto, in linea con i principi del giusto processo e della sua ragionevole durata.

In una siffatta prospettiva di ricerca di un nuovo feticcio che possa sostituire la legge nel compito di eliminare ogni forma di incertezza, espressioni quali giustizia predittiva o decisione algoritmica appaiono assai rassicuranti.

Del resto, già Leibniz [13] aveva profetizzato l'uso di sistemi per

---

[9] Si ricorda che quella del giudice come *bouche de loi* di montesquieuiana memoria è un'affermazione da intendersi in senso più politico che giuridico come l'apoteosi della sovranità popolare.

[10] Cfr. G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in C. BERIA DI ARGENTINE (a cura di), *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, p. 10; M.B. MAGRO, *Robot, cyborg e intelligenze artificiali*, in A. CADOPPI - S. CANESTRARI - A. MANNA - M. PAPA (a cura di), *Cybercrime*, Milano 2019, p. 1181; S. SIGNORATO, *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo, in Riv. it. dir. proc. pen.*, 2020, p. 614.

[11] Cfr. A.C. AMATO MANGIAMELI, *Informatica giuridica*, Torino, 2015, pp. 216 ss.; M. CATERINI, *Il giudice penale robot*, in *www.lalegislazionepenale.eu*, 19 dicembre 2020, p. 5; C. TARQUINI, *L'automa-giudice: distopie e prospettive concrete in tema di algoritmi predittivi*, in L. DANIELE - A. VIGNOLI - M.N. CAMPAGNOLI (a cura di), *Giustizia e Potere(i). Riflessioni sull'indipendenza del giudice*, Milano, 2024.

[12] Cfr. A. CARLEO, *Calcolabilità giuridica*, Bologna, 2017; N. IRTI, *Il tessitore di Goethe (per la decisione robotica)*, in A. CARLEO (a cura di), *Decisione robotica,* Bologna, 2019, pp. 17 ss.

[13] Cfr. G. W. LEIBNIZ, *Dissertatio de arte combinatoria, in qua, ex arithmeticae fundamentis*, Lipsia, 1666.

© Wolters Kluwer Italia

prevedere l'esito del giudizio tali da rendere superfluo il ricorso alla macchina processuale, incentivando modi alternativi di risoluzione delle liti.

Siffatta IA, però, ad oggi ancora non esiste in modo compiuto, nonostante siano già stati sviluppati algoritmi in grado di offrire attendibili previsioni circa il possibile esito di determinate controversie. Si pensi, a tal proposito, solamente al *software* sviluppato dall'*University College of London* nel 2016 con riferimento alle possibili violazioni della Corte europea dei diritti dell'uomo [14].

Più facilmente ipotizzabile sarebbe, poi, un modello di giustizia predittiva per cui la decisione del giudice risulti essere automatizzata in funzione dei precedenti giurisprudenziali. Tale modello, però, non è in linea con il nostro vigente sistema di *civil law*.

In ogni caso, l'utilizzo dell'intelligenza artificiale in senso forte presenta alcune insuperabili criticità.

In primo luogo, i risultati della macchina dipendono dalle scelte effettuate a monte dall'operatore umano in punto di selezione dei materiali cui il *software* può attingere e di modalità della loro analisi. È, in fin dei conti, sempre l'intelligenza umana a nutrire e a addestrare l'intelligenza artificiale. Si potrebbe allora affermare che i preconcetti e le inesattezze dell'uomo non vengono eliminati dall'algoritmo, ma solo anticipati per poi riflettersi nell'attività della macchina dando vita a *bias* [15].

C'è anche da considerare che spesso i criteri e le modalità di funzionamento degli algoritmi si dimostrano poco accessibili agli operatori del diritto, di talché risulta poco chiaro l'*iter* seguito dagli stessi per giungere ad una certa soluzione. Ciò non consentirebbe nemmeno l'esercizio del diritto di difesa da parte del destinatario della decisione in sede d'impugnazione.

L'affidarsi all'automazione, inoltre, finirebbe di fatto per soffocare ogni nuovo indirizzo del diritto rendendo il sistema rigido: la decisione deviante, infatti, verrebbe letta dalla macchina come una decisione ingiusta e, pertanto, da rigettare. Al contrario, il mutamento giurisprudenziale rappresenta la linfa vitale soprattutto di una società in continua evoluzione come quella attuale.

---

[14] Cfr. M. Medvedeva - M. Vols - M. Wieling, *Using machine learning to predict decisions of the European Court of Human Rights*, in *Artificial Intelligence Law*, 2019.

[15] S. Quattrocolo, *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"*, in *Cass. pen.*, 4/2019, pp. 1748 ss.

© Wolters Kluwer Italia

Al di là delle suddette problematiche, specificamente in tema di giudizio di diritto, come già osservato nel primo paragrafo del presente contributo, vi sono intrinseci elementi di incertezza dell'attività interpretativa giudiziale ed ineliminabili margini di discernimento del delegato-giudice. Proprio in questi ambiti il giudicante-uomo non può essere sostituito dalla macchina. Quest'ultima, infatti, non è in grado di azzerare i margini di discrezionalità interpretativa e di contestualizzazione degli incarichi e delle deleghe ricevute e di individuare autonomamente, fra più possibili interpretazioni, quella globalmente più in linea con il senso comune proprio della società di appartenenza e, quindi, più accettabile. Per fare tutto ciò occorrerebbe una sensibilità che pare difficilmente replicabile dall'automa.

Tali coordinate devono essere tenute ben salde nell'affrontare, senza esserne "ammaliati", le travolgenti novità che l'intelligenza artificiale ci proporrà con forza nell'immediato futuro, se non si vuole che l'ingiustizia, e spesso persino l'assurdità, delle decisioni, la soppressione di ogni nuovo indirizzo giurisprudenziale e la sottrazione dell'attività giudiziale al controllo sociale diventino il prezzo da pagare per perseguire la certezza del diritto [16].

3. L'IA quale ausilio per l'attività del giudice

Se la tecnologia algoritmica non può sostituire il giudice, il quale mantiene il controllo su di essa quale *dominus* della funzione giurisdizionale, essa se usata e guidata sapientemente senza appiattirsi sui risultati che produce, risulta assai promettente e può senz'altro già oggi svolgere una funzione di ausilio per l'organo di giustizia [17]. Ciò anche nell'ottica di rendere più efficiente la giurisdizione e di ridurre la durata dei tempi processuali.

---

[16] Così scrive significativamente R. LUPI, *Interazione tra intelligenza naturale e artificiale nel diritto predittivo*, in A. MARCHESELLI - E. MARELLO (a cura di), *Loading Prodigit. Dal diritto naturale al diritto digitale: l'intelligenza artificiale nella giustizia tributaria*, Pisa, 2022: "*L'automazione, come aspetto fondamentale della socialità, ha da sempre presupposto una buona conoscenza di quanto andava automatizzato, dai tempi del telaio meccanico fino forse a quelli della clava, come nella scena iniziale del film 2001 Odissea nello spazio. Nella stessa misura la giustizia predittiva, basata sull'intelligenza artificiale, ha bisogno di inserirsi in una cornice socialmente condivisa di ragionamento giuridico e quindi – salvi atti di fede – basata sull'intelligenza naturale*".

[17] A. SANTOSUOSSO, *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Milano, 2020.

© Wolters Kluwer Italia

Viene, a tal proposito in rilievo una IA cosiddetta "debole", in grado di eseguire velocemente operazioni complesse nell'ambito in cui viene istruita.

Detta intelligenza artificiale, in primo luogo, ben può venire utilmente in rilievo in riferimento ad attività che si pongono al di là del procedimento intellettivo che porta alla decisione quali corollari della stessa. Si pensi solamente ai casi in cui l'applicazione del diritto richiede ripetitive operazioni di calcolo [18].

I sistemi di archiviazione informatici, poi, consentono il veloce reperimento di ogni informazione giuridica collocata nel relativo *database*, di regola molto ampio e in continuo aggiornamento, costituito da disposizioni normative, ma eventualmente anche da precedenti giurisprudenziali relativi ad un determinato ambito del diritto [19].

La tecnologia in esame ben potrebbe anche essere utilizzata per rilevare possibili lacune nel sistema normativo e antinomie fra le norme vigenti.

Con riferimento specifico al giudizio di diritto, l'organo di giustizia potrebbe verificare come il *giudice robot* analizza e confronta simultaneamente il peso delle diverse ragioni della decisione e di tutti gli argomenti interpretativi e le conseguenze, anche negative o assurde, di una certa interpretazione, controllandone i risultati.

Per poter costruire tale algoritmo, però, occorre, innanzitutto, avere conoscenza del funzionamento dell'intelligenza naturale al fine di replicare i medesimi ragionamenti e collegamenti depurati da ogni contaminazione umana. L'operatore, poi, deve indicare alla macchina tutti i parametri ritenuti rilevanti, eventualmente dando a questi un ordine di importanza, e inserire il *database* di informazioni cui il *software* può attingere.

Un siffatto "algoritmo interpretativo", immune da qualsiasi influenza emotiva e condizionato dai soli *input* introdotti, potrebbe risultare uno strumento assai utile al servizio del giudice posto che si occuperebbe di svolgere un'attività difficile per l'intelligenza naturale, caratterizzata dall'istinto e dalla suggestione.

Del resto, come anche sostenuto da autorevoli psichiatri [20], la tecnologia attuale è mentale, a differenza di quella passata, di talché ap-

---

[18] È l'ipotesi, per esempio, della quantificazione della prestazione alimentare.

[19] S. Simitis, *Crisi dell'informazione giuridica ed elaborazione elettronica dei dati*, Roma, 1977, pp. 85-86.

[20] Fra gli altri, cfr. T. Cantelmi - V. Carpino, *Amore tecnoliquido. L'evoluzione dei rapporti interpersonali tra social, cybersex e intelligenza artificiale*, Milano, 2020.

© Wolters Kluwer Italia

pare possibile l'integrazione del cervello umano con quello artificiale. Il cervello dell'uomo è l'organo più adattabile in assoluto ed è oggi già pronto ad essere coprotagonista insieme con quello dell'IA, che, infatti, si sta evolvendo insieme a noi.

© Wolters Kluwer Italia

RIFLESSIONI SULL'USO DELL'INTELLIGENZA ARTIFICIALE NEL GIUDIZIO DI FATTO *

GIANLUIGI SCALA

SOMMARIO: 1. Le caratteristiche dell'IA ed i criteri in base a cui opera. – 2. Le prospettive di impiego dell'IA nel giudizio di fatto come occasione per seguitare a riflettere sul funzionamento dell'intelligenza naturale. – 3. La struttura ed i caratteri essenziali del giudizio di fatto: tra constatazione oggettiva e ricostruzione *personale* del reale. – 4. L'impiego dei modelli di IA nel giudizio di fatto: verso una funzione di normalizzazione nella ponderazione degli elementi di prova. – 5. Conclusioni sulla dimensione strumentale e non sostitutiva dell'IA nel giudizio di fatto.

Abstract: Artificial intelligence, as a tool for self-learning, and reprocessing of information, that can find significant applications in the evaluation of law-relevant evidence. The aim of this contribution is to analyse the many advantages of AI, such as that of enabling the rapid analysis of large volumes of data and the subsequent connections between. The use of artificial intelligence could decrease the risk of errors related to the emotionality of the judge. Nevertheless, the use of AI raises some concerns related to possible imperfections in the designs of the provided instructions under which it proceeds. There is little use of functions posing as search engines, structurally unsuitable for standardising the probabilistic empiricism of the factual judgment. Another problem is that of attribution of authorship of reconstruction and responsibility arising from negligence in the development or use of AI.

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

1. Le caratteristiche dell'IA ed i criteri in base a cui opera

L'intelligenza artificiale opera attraverso criteri che la rendono idonea a molteplici usi e ciò ne rende complessa la classificazione [1]. Può prospettarsi una prima *summa divisio* per criteri operativi: quello di analisi e quello di automazione. Il criterio di analisi, utile alle attività che adoperano grandi basi dati, mira a organizzare e valorizzare le informazioni, estrapolando i risultati ritenuti coerenti con la chiave di ricerca e giungendo ad evidenziare l'esistenza di elementi di comunione. Proprio per la sua attitudine ad esaminare dati forniti in misura vasta ma pur sempre predeterminata, l'IA analitica non può definirsi propriamente *generativa*. Il criterio di automazione, differentemente da quello di analisi, caratterizza le più recenti versioni di IA e opera sostituendo parzialmente o totalmente l'opera umana in compiti che richiedono l'impiego di capacità di rielaborazione. In questo caso, l'algoritmo assume le informazioni, le ordina e combinandole giunge ad elaborare le conclusioni. Questo secondo tipo di IA è comunemente definito "generativo" poiché tende a restituire un *output* non direttamente predeterminato dal programmatore. In realtà, come vedremo, anche questo secondo tipo di IA è comunque bisognoso nella fase iniziale di un obiettivo chiaramente ideato e formulato dall'utente, non essendo in grado di individuarlo autonomamente [2].

Alternativamente, si è soliti suddividere i modelli di IA in "forte" e "debole" in base al grado di fungibilità rispetto al pensiero umano oppure in "articolata" o "generalizzata" in base all'ampiezza dell'ambito di impiego. Il modello può assumere la qualità "generativa" laddove in esecuzione del comando sia in grado di offrire un elaborato non meramente estratto dalla base dati, ma frutto di una elaborazione ossequiosa delle indicazioni fornite. L'intelligenza artificiale debole, nota come "intelligenza simulata", si focalizza con precisione sui compiti per cui è strettamente programmata, senza immettere nel risultato alcun

---

[1] S. RUSSELL - P. NORVIG, *Artificial Intelligence: A Modern Approach*, London, 2016; I. GOODFELLOW - Y. BENGIO - A. COURVILLE, *Deep Learning*, III ed., Cambridge, Massachusetts, 2016; N.J. NILSSON, *Artificial Intelligence: A New Synthesis*, San Francisco, California, 1998; D. POOLE - A. MACKWORTH, *Artificial Intelligence: Foundations of Computational Agents,* II ed., Cambridge, 2017; R.S. SUTTON - A. BARTO, *Reinforcement Learning: An Introduction*, II ed., Cambridge, Massachusetts, 2018.

[2] In questo senso è indispensabile per chi impiega l'IA apprendere le metodologie di formulazione dei comandi, affinché risultino chiari ed intellegibili al sistema di IA: il risultato emesso dal sistema, infatti, dipendente proprio dalla qualità degli *input* forniti dall'utente.

© Wolters Kluwer Italia

profilo di creatività che esuli dai comandi. Essa è impiegata per la realizzazione di assistenti virtuali o nei sistemi di automazione industriale. L'IA debole è quindi bisognosa della supervisione umana, non essendo in grado di restituire un prodotto qualitativamente paragonabile a quello umano. Volendo ulteriormente chiarire, l'IA debole è programmata per agire deliberatamente "come se" fosse un soggetto intelligente, ma non essendolo è in grado di elaborare solo un risultato non creativo. Tecnologie simili sono state per lungo tempo alla base dei comuni motori di ricerca per banche dati: è sufficiente che un risultato non rispetti i parametri imposti affinché venga scartato, pur essendo rilevante ai fini della ricerca secondo i criteri dell'intelligenza naturale. In antitesi rispetto al modello descritto, si colloca l'IA forte, in fase di avanzato impiego sperimentale, che si pone come evoluzione della precedente versione debole poiché aspira ad emulare il pensiero umano. Per quanto, infine, concerne l'ampiezza dell'ambito di impiego, si definisce "articolato" quel modello di IA che è in grado di eseguire bene solo un compito, mentre è definito "generale" il modello di intelligenza artificiale capace di spaziare tra plurimi compiti eterogenei.

2. Le prospettive di impiego dell'IA nel giudizio di fatto come occasione per seguitare a riflettere sul funzionamento dell'intelligenza naturale

Le riflessioni sull'impiego dell'IA nel giudizio di fatto sono un'importante occasione per capire meglio il funzionamento dell'intelligenza naturale: l'algoritmo riveste, infatti, il ruolo di un "programma di ragionamento" e scandisce una sequenza di operazioni logiche prefigurate dall'uomo per simulare il ragionamento umano, sgravandone l'utente. L'algoritmo racchiude sia la funzione analitica, che è quella del *data*, sia la funzione generativa, che è quella del *processing*, con una grande differenza rispetto al passato [3]: mentre prima la base dati

[3] Il confronto con il passato è tutt'altro che fuorviante: al contrario di quanto potrebbe sembrare, l'elaborazione elettronica dei dati non è una novità del momento, ma affonda le radici negli albori degli EDP (*electronic data processing*), ossia i primi *computer*, anche noti come "elaboratori elettronici". Essi venivano equipaggiati direttamente dai fornitori da quelle che oggi chiameremmo *apps*, ossia programmi realizzati dai programmatori per consentire alla macchina di emettere un *output* coerente e logico rispetto agli *input* immessi dall'utilizzatore, simulando il modo di ragionare umano. A ben vedere, quindi, pur nella consapevolezza della diversità dei contesti, è possibile dire che già allora vi era la compresenza di funzioni di analisi, ossia il *data*, e di fun-

© Wolters Kluwer Italia

doveva essere predeterminata dal fornitore ed i risultati erano selezionati tra un insieme chiuso di dati, adesso i recenti sistemi di IA sono in grado non solo di popolare autonomamente la base dati, ma anche di elaborare soluzioni sempre nuove grazie i meccanismi di autoapprendimento.

Quanto accennato consente già di intravedere l'ampio sussidio che l'IA può offrire tanto alle organizzazioni private, quanto alla Pubblica Amministrazione. La diffusione di questa tecnologia nel settore delle funzioni pubbliche, tuttavia, abbisogna di essere affiancata da studi sociali che sintetizzando, filtrando e rielaborando i bisogni della collettività contribuiscano ad indicare le modalità di impiego agli organi legislativi ed esecutivi, per prevenire quanto più possibile le esternalità negative di cui sovente si dibatte in sede pubblica [4]. Si tratterà, quindi, di affrontare le questioni legate al possibile disallineamento della scelta artificiale rispetto allo spettro valoriale giuridico collettivo sinora plasmato dall'intelligenza umana. A differenza degli esseri umani, infatti, l'IA emette un risultato senza aver sviluppato, rielaborato e sperimentato interiormente i valori su cui si fonda il *patto sociale*: non possiamo nascondere a noi stessi che l'IA non è (ancora) in grado di scoprire di apprezzare una certa attività o di trovare un significato alla propria esistenza, giungendo a decidere se e come impiegare in essa il suo tempo. Il non essere soggetta alla finitezza della vita umana comporta per l'IA l'impossibilità di condurre un'autonoma ricerca di senso, come invece fa l'intelligenza umana. Tali basilari considerazioni ci consentono meglio di riaccreditare il ruolo dell'impulso umano comprendendo i limiti dell'IA: questi ultimi, poi, emergono con grande rilevanza negli ambiti ove sono impiegate conoscenze tecniche e discrezionali, qual è l'attività dello *ius dicere*. L'intelligenza artificiale può descrivere un fenomeno materiale analiticamente, spiegare cosa sia e reperire le informazioni e le opinioni su determinate classi di fatti (ad esempio gli incidenti stradali), ma la valutazione concreta sulla ricostruzione causale e la determinazione del fatto, soprattutto quando si tratta di casi particolari, rimane una prerogativa umana. Ciò perché in questo contesto,

---

zioni generative, ossia il *processing*, seppur non originali rispetto all'insieme delle soluzioni predeterminate dai programmatori.

[4] Il problema delle esternalità negative derivanti dall'impiego dell'IA è molto sentito nel dibattito pubblico, ma spesso liquidato sbrigativamente dagli "esperti", che anziché risolvere i dubbi sociali ne creano ulteriori definendo queste preoccupazioni come *luddiste* ed affidandosi a provvidenziali e imprecisati meccanismi di accomodamento salvifici. In questo modo, rimangono inevasi i dubbi sulla perdita dell'autonomia decisionale umana, sulla perdita di posti di lavoro, sulla compromissione della *privacy*, ecc.

© Wolters Kluwer Italia

l'IA si limiterebbe tutt'al più ad attenersi alle generiche ed aspecifiche informazioni reperite in rete, oppure alle poche informazioni specifiche già di dominio pubblico su un determinato fatto (ad esempio gli indizi già divenuti di pubblico dominio), ma non potrebbe mai scoprire informazioni specifiche *nuove* rispetto a quelle già presenti nel *world wide web*, che costituisce la base dati di riferimento. L'IA può quindi fornire dati e informazioni, ma l'attività euristica sul fatto e di interpretazione empirico-probabilistica sulla casualità richiede sempre la sensibilità e il giudizio umano, elementi che l'IA non può (ancora) replicare. Lo sviluppo della riflessione su questi elementi, come vedremo avanti, consentirà di far emergere i vantaggi e svantaggi dell'impiego dell'IA *in iudicando* [5], tra massivo potenziamento quantitativo delle capacità amministrative e l'inevitabile imbrigliamento della singolarità del decidente [6]; tra l'efficienza nell'espletamento della delega sociale ed il rispetto dei diritti dei soggetti attinti dalla decisione. Gli studiosi sociali che si cimenteranno con il tema, sotto un profilo metodologico, dovranno guardare ad un fenomeno multidisciplinare non regolato legislativamente e che perciò non può essere affrontato in chiave puramente tecnico-descrittiva del dato positivo [7]. Lo sviluppo degli avanzati modelli di IA è infatti spesso accompagnato da ideologismi che rivendicano assoluta libertà da ogni condizionamento, regola o forza cogente, sventolando il vessillo dell'antigiuridismo [8]: è quindi prevedibile l'insuccesso di un approccio meramente normativista, imbrigliato al corto spettro del dato positivo.

Il compito dovrà essere adempiuto con equilibrio e adoperando un linguaggio accessibile che permetta di raggiungere la platea degli inte-

---

[5] La funzione giurisdizionale è, infatti, una delle pubbliche funzioni in cui si sta sperimentando questo strumento: v. al riguardo la Carta etica per l'uso dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, emessa nel dicembre 2018 dalla Commissione europea per l'efficienza della giustizia (CEPEJ), disponibile su: *www.rm.coe.int*; quale tentativo di implementazione si consideri, invece, il progetto PRODIGIT, finanziato mediante il PON "*Governance e Capacità Istituzionale 2014-2020*", che prevede una serie di attività per l'innovazione della Giustizia tributaria, con il supporto della tecnologia digitale e dell'intelligenza artificiale.

[6] Ci riferiamo a ciò che riteniamo alla base del processo evolutivo del diritto, ossia alla possibilità che il decidente, discostandosi in termini migliorativi dal *precedente conforme*, renda una decisione autorevole condivisa nei successivi giudizi e in grado di arrecare un generalizzato beneficio alla comunità.

[7] Per una completa ricostruzione sul concetto di studi sociali e sul metodo con cui essi dovrebbero essere affrontati si rinvia a R. Lupi, *Studi sociali e diritto*, Roma, 2022.

[8] In tal senso anche A.C. Amato Mangiameli, *Ia e diritto: in luogo di un'introduzione,* in *Riv. elettr. dir., econ., manag.*, 1/2024, p. 18.

© Wolters Kluwer Italia

ressati, rifuggendo le tentazioni di mimesi con le scienze fisiche [9]. Infatti, differentemente da queste ultime, che appaiono protese migliorare il funzionamento dei sistemi artificiali d'intelligenza senza occuparsi dei problemi etico-collettivi, gli studi sociali si manifestano più idonei – per scopi, eterogeneità ed ampiezza – ad indagare sul tema [10].

3. La struttura ed i caratteri essenziali del giudizio di fatto: tra constatazione oggettiva e ricostruzione *personale* del reale

Come noto, la funzione giurisdizionale viene esplicata attraverso due momenti valutativi che si ricongiungono nella motivazione finale, costituiti rispettivamente dal giudizio di fatto e dal giudizio di diritto. In questa sede sarà nostro interesse esaminare solo il primo dei menzionati segmenti. Con l'espressione "giudizio di fatto" si designa tanto il processo quanto il risultato cui il giudice perviene dopo aver esaminato gli elementi di prova offerti dalle parti o ricercati dal medesimo con i modi imposti dal paradigma processuale di riferimento. Tale giudizio svolge, quindi, il fine di delimitare i fatti su cui dovrà pronunciarsi. Autorevoli opinioni ritengono sussistere una interrelazione ed anzi un condizionamento [11] tra la ricostruzione del fatto e la susseguente qualificazione giuridica; tuttavia, per quanto si sovrastimino i profili di interessenza tra i due momenti, è immediato constatare che permane un ambito valutativo, comunque, antecedente alla qualificazione giuridica, collocato alla base del percorso che porta alla decisione. In tale frangente, il giudice-uomo è il perno di un accertamento empirico, in

[9] Sebbene le scienze fisiche giungano a ricavare le leggi regolative del mondo semplificando quanto più possibile le variabili e costituendo modelli ipotetici, ciò non risulta possibile allo studioso sociale, il quale, riducendo a modello le complesse dinamiche sociali, finirebbe inconsapevolmente col privarsi dell'oggetto stesso della propria indagine, finendo a discettare sul nulla.

[10] In questa direzione e con metodo pluralistico già risultano compiuti primi passi da parte di alcune comunità accademiche. Al riguardo si segnala il lavoro svolto dal gruppo di ricerca "Diritto e Intelligenza Artificiale", ospitato dal Centro di Ricerca *Católica per il Futuro del Diritto* radicatosi presso l'*Universidade Católica* di Lisbona, e guidato da A. Henrique Sousa e A. Oliveira, che sull'argomento ha dato il via ad un continuo dialogo scientifico tra studiosi con provenienza e interessi diversi: diritto, informatica, neuroscienze ed etica, giungendo a pubblicare in *open access* il volume collettaneo *Multidisciplinary Perspectives on Artificial Intelligence and the Law*, Cham, 2024.

[11] Così G. UBERTIS, *Quaestio facti e Quaestio iuris*, in *Quaestio facti. Revista Internacional sobre Razonamiento Probatorio*, 1/2020, pp. 67-74, in cui si afferma che la prospettiva giuridica orienta il giudizio di fatto.

© Wolters Kluwer Italia

cui si concentra puramente senza già badare alle sovrastrutture delle disposizioni, (ma come vedremo, senza mai riuscire a spogliarsi della mediazione del proprio pensiero) [12]. Esso risponde al compito di acquisire i lineamenti materiali del fatto senza necessariamente già ricondurlo alle regole, bensì collocandolo entro limiti spaziali, temporali e causali. L'attività descritta si risolve nella ricostruzione di ciò che è comunemente noto come "fattispecie concreta": essa è già il risultato di una manipolazione e frutto del pensiero del giudicante; il fatto, essendosi verificato prima e fuori dall'aula di giustizia, esiste tanto e nella misura in cui l'uomo che giudica arriva a concepirlo [13]. Per quanto deludente, non appare equivocabile che la fattispecie concreta sia fatto pensato (*δόξα*) e non semplicemente fatto in *rerum natura* (*ἀλήθεια*). A tale fase di ricostruzione consegue, come da alcuni approfondito [14], un momento argomentativo, dialettico-retorico ed opinativo che si forma durante il processo e, nutrendosi del contraddittorio, si proietta verso la qualificazione giudica, esitando con il saldarsi ad essa nella motivazione finale. È quest'ultimo momento, che a ben vedere, può considerarsi "spurio" giacché inquinato e proteso verso la qualificazione giuridica, ma certamente non il primo, connotato da una cifra marcatamente empirica. È altrettanto necessario, però, che il risultato di questo momento argomentativo finisca col rispondere ad una ricostruzione logico-razionale che si basi sul modo di essere del mondo e sia ossequiosa delle regole causali che lo reggono, di modo che non patisca le considerazioni serbate dall'uomo cui è dato di decidere: ossia le personali vedute del reale, le esperienze vissute o le emozioni provate rispetto ad un insieme di fatti analoghi a quello controverso.

Per quanto l'eliminazione dei pregiudizi appaia una misura auspicabilmente attuabile, non possiamo evitare di confrontarci con quella parte di studi sull'euristica giunti postulare nell'attività del percepire l'indissolubile compresenza di elementi aprioristicamente condizio-

---

[12] Così anche M. Orlandi, *Gnoseologia della fattispecie,* in *Questione Giustizia*, 1/2020, pp. 95 ss., che opportunamente ricorda: "*(...) lo sguardo sul mondo è sempre un concepire, ossia un porre in concetto fatti e cose. Il mondo non ci si offre immediatamente; esso sempre reclama la mediazione del pensiero. Si può dire in una sintesi breviloquente che il mondo è una rappresentazione razionale. Un far presente in concetto; un concepire ciò che prima dell'idea è un nulla, opaco e assente*".

[13] In questo contesto non può che rimanere valido il noto insegnamento di Protagora, secondo cui: "*l'uomo è misura di tutte le cose; delle cose che sono in quanto sono, delle cose che non sono in quanto non sono*".

[14] Cfr. R. Poli, *Prova e convincimento giudiziale del fatto*, in *La prova nel diritto e nel processo*, Torino, 2023, pp. 12-13.

© Wolters Kluwer Italia

nanti il giudizio, definiti *precomprensioni* [15]. Essi sono l'insieme delle conoscenze sull'oggetto che l'interprete racchiude in sé prima ancora di confrontarsi con l'oggetto. Sotto un profilo strettamente ontologico ciò finisce, secondo queste ricostruzioni, per rendere la valutazione umana del fatto sempre lontana dai caratteri della neutralità o dell'oggettività ed inevitabilmente connessa al contesto storico e culturale cui appartiene il decidente.

Ignorando (o fingendo di ignorare) questa ricostruzione, la teoria giuridica dello scorso secolo [16], mimando il metodo delle scienze fisiche, ha seguitato a propugnare un modello di giudizio di fatto incentrato più sul dover essere che sull'essere, rilegando il problema della percezione soggettiva a mera stortura eventuale facilmente emendabile, senza mai giungere a considerarla come elemento costitutivo ed ineludibile. Secondo questi orientamenti il giudice dovrebbe eseguire senza titubare il compito di spogliarsi della sua umanità e basarsi su dati verificabili e conoscenze scientifiche, rifiutando ogni influenza derivante da pregiudizi o valutazioni, financo inconsce, astenendosi dal diventare un "creatore di fatti", ma piuttosto un "riconoscitore" di essi in favore dell'imparzialità e dell'equità del processo. Per dirla autorevolmente "*(...) nella ricostruzione che deve fare il giudice si loda, come in quella del vero storico, la imparzialità e la cosiddetta «oggettività», e si addita come sentenza perfetta [...] quella che riesca ad essere niente altro che una copia esatta, quasi si direbbe un calco ottenuto con precisione meccanica, di una realtà che sta tutta quanta al di fuori del giudicante*" [17].

In definitiva, il problema della percezione individuale pare elemento ineludibile sia della teoria oggettivista che di quella soggettivista del giudizio di fatto [18].

---

[15] H.G. GADAMER, *Verità e metodo*, Milano, 1960, pp. 274-290.

[16] Cfr. F. STEIN, *Das private Wissen des Richters: Untersuchungen zum Beweisrecht beider Prozesse*, Leipzig, 1893, la cui partizione tra massime di esperienza e fatti notori è stata successivamente rielaborata in Italia da F. CARNELUTTI, *La prova civile*, Roma, 1915.

[17] P. CALAMANDREI, *Il giudice e lo storico*, in *Opere giuridiche*, Padova, 1950, p. 394, disponibile su *https://romatrepress.uniroma3.it.*

[18] A ben vedere la stessa autorevole opinione riammette l'esistenza di distorsioni soggettive alla percezione del giudice, sotto il diverso profilo della "*valutazione soggettiva del contegno della parte*" ossia la percezione sulla sua onestà e credibilità della parte: cfr. P. CALAMANDREI, *Il processo come giuoco,* in *Opere giuridiche*, cit., p. 559.

© Wolters Kluwer Italia

4. L'impiego dei modelli di IA nel giudizio di fatto: verso una funzione di normalizzazione nella ponderazione degli elementi di prova

Introdotti i caratteri essenziali del giudizio di fatto, si tratta di riflettere sul possibile apporto dei sistemi di intelligenza artificiale all'interno del giudizio di ricostruzione della fattispecie concreta e tentare di avanzare alcune ipotesi circa i conseguenti effetti. Nel far ciò, per ragioni di spazio, ci limiteremo a prendere in considerazione due opposti modelli, quello analitico-debole non generativo e quello forte, generativo e dotato di automazione, rinviando ad altri studi l'esame delle altre combinazioni.

Il modello di IA analitico, debole e non generativo, essendo più limitato ed operando alla stregua di un motore di ricerca, non appare in grado di supportare il giudice se non nell'elaborazione di grandi quantità di dati che non abbisogni di apporto deduttivo-generativo: tale circostanza spesso ricorre negli affari legali appartenenti al settore commerciale, bancario o tributario, in cui può rendersi necessaria la disamina e la comparazione di grandi volumi di dati, specie contabili, altrimenti acquisibili con maggiore dispendio di tempo. L'utilità derivante dall'impiego di siffatta tipologia di intelligenza artificiale risulta comunque limitata poiché priva, nei termini di cui al par. 1, di efficacia creativo-generativa. Nell'ipotesi di utilizzo di IA debole, quindi, il momento valutativo rimarrebbe completamente in capo al giudice, con i noti problemi di parzialità e fallibilità cui si accennava prima. È possibile pervenire alle medesime conclusioni anche ove si scegliesse di estendere la base dati impiegata a tutti i contenuti a fonte aperta: in questo caso, però, accettando il rischio che dati errati confluiscano nel sistema, la ricostruzione potrebbe persino divenire aspecifica rispetto al fatto e, quindi, ostacolare il giudizio.

Maggiori potenzialità, invece, rivelerebbe l'impiego di un sistema di IA forte, generativo e dotato di automazione. È, infatti, ragionevole ipotizzare che l'impiego di questo avanzato modello consentirebbe di ridurre gli aspetti opinativi che caratterizzano il giudizio di fatto, rendendolo oggettivo. In realtà, a nostro avviso, essendo l'oggettività ineffabile nella sua natura concettuale, in questo caso sarebbe più corretto parlare di omogeneità nella ponderazione degli elementi di fatto: riteniamo che sia più opportuno parlare di omogeneità e non di oggettività, stante il fatto che il modello di analisi e comparazione con cui procede la macchina è pur sempre arbitrariamente determinato a priori dal programmatore e potrebbe risultare non necessariamente il migliore e,

© Wolters Kluwer Italia

purtuttavia, opererebbe egualmente all'interno dei diversi giudizi pendenti in un dato momento storico.

Del pari, con l'impiego di un sistema di IA forte e generativo, verrebbe a ridursi il rischio che il giudicante, spesso privo delle capacità tecniche, si trovi con basso grado di consapevolezza a dover scegliere la deduzione cui aderire tra quelle offerte dai consulenti, spesso in contrasto tra loro per parzialità, oppure condizionate dal diverso grado di professionalità dell'autore o financo dalla differente selezione della legge regolativa del fatto.

Nonostante le maggiori potenzialità, l'impiego del modello forte di IA comporta altrettante complicazioni: ad esempio, uno dei fattori critici che dovrà essere risolto, attiene alla propensione dell'uomo ad affidarsi ciecamente agli algoritmi reputandoli aprioristicamente inoppugnabili, comunemente definita come "*automation bias*" [19], perfino accettando il rischio che la decisione risulti errata. Pur di migliorare l'efficienza, quindi, si potrebbe elidere il controllo critico sulla decisione e il giudice potrebbe essere indotto ad accettare supinamente la ricostruzione offerta dalla macchina, trasferendole la responsabilità della decisione [20]. Il carattere forte, poi, consentirebbe al sistema di IA di attingere a informazioni esterne al processo, delle quali è in grado di entrare in possesso mediante l'analisi delle più disparate risorse, comprese quelle che auto-alimentiamo, come i *social network*, i *blog* e i *forum*. Questo modo di procedere, peraltro, confliggerebbe irrimediabilmente con i modelli processuali imperniati sulle garanzie del principio dispositivo: il giudizio sul fatto che si verrebbe a costituire finirebbe per risultare "arricchito" da elementi e circostanze non ritualmente dedotte dalle parti e, ciò nonostante, reperite dalla macchina *aliunde* e veicolate all'interno del processo. Questo "arricchimento" degli ele-

---

[19] Sul tema si segnalano: M.L. CUMMINGS, *Automation bias in intelligent time-critical decision support systems*, in *1st Intelligent Systems Technical Conference*, Chicago, Illinois, 2004, in cui l'Autore ha esplorato l'impatto dell'automazione nel controllo del traffico aereo, dimostrando come l'affidamento eccessivo su strumenti automatizzati possa portare a errori critici in situazioni di emergenza. Un precedente studio, condotto da R. PARASURAMAN - V. RILEY, dal titolo *Humans and automation: Use, misuse, disuse, abuse*, in *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 2/1997, era però già addivenuto a comprendere l'importanza nel bilanciamento tra il controllo umano e l'affidamento sull'automazione, per mitigare i rischi legati all'effetto di *automation bias*.

[20] Cfr. A. HENRIQUE SOUSA - P.M. FREITAS - A.L. OLIVEIRA - C. MARTINS PEREIRA - E. VAZ DE SEQUEIRA - L. BARRETO XAVIER (eds.), *Multidisciplinary Perspectives on Artificial Intelligence and the Law*, Cham, 2024, pp. 281-297, disponibile su: *www.link.springer.com.*

© Wolters Kluwer Italia

menti del fatto potrebbe avvenire anche a discapito dell'aderenza alle trame materiali e comportamentali del caso specifico, rispetto alle quali potrebbero non essere disponibili in rete elementi coerenti. In questo caso, comunque, l'intelligenza artificiale forte potrebbe limitarsi ad ordinare le domande utili alla ricostruzione del fatto e le diverse ipotesi causali. Ad ogni modo, l'ampliamento degli elementi su cui si forma il giudizio di fatto confliggerebbe con i vigenti differenziati gradi di autonomia istruttoria di cui dispone il giudice; la macchina, difatti, procedendo secondo le istruzioni dettate dai programmatori, finirebbe per operare, anche grazie alle funzioni di auto-apprendimento, l'ampliamento a tutti gli esperimenti potenzialmente utili alla ricostruzione del fatto, finendo con l'intralciare l'istruttoria. Parallelamente, verrebbe integrata ed ampliata la categoria delle massime di esperienza mediante le *esperienze della rete* maturate e diffuse dai singoli utenti, note per fallacia e ciononostante imperversanti. Se così fosse, si ammetterebbe che questa versione allargata delle "massime di esperienza" cooperi nella ricostruzione del fatto senza che il giudice ne abbia previamente vagliato l'effettiva attinenza e non superfluità rispetto all'indagine.

Al di fuori del giudizio di primo grado, poi, l'influsso dell'*automation bias* potrebbe condurre il giudice *ad quem* a sottovalutare le istanze di revisione sul fatto avanzate dalla parte, riducendone ulteriormente il già ristretto ambito di effettività nella proposizione dell'impugnazione, in parte dettato dal paradigma devolutivo che caratterizza i vigenti riti [21], prono a soddisfare istanze sociali di celerità anche a scapito della corretta ricostruzione del fatto sussunto nella disposizione che ha risolto il contenzioso nel precedente grado di giudizio.

5. Conclusioni sulla dimensione strumentale e non sostitutiva dell'IA nel giudizio di fatto

L'intelligenza artificiale può servire alla formalizzazione dei dubbi, perché non ha profili emotivi e neppure contingenze rispetto alle quali adattare il risultato da consegnare (scadenze, pressioni per lo smaltimento degli arretrati, questioni di natura personale atte ad alterare il ritmo produttivo). Può assumere, quindi, il ruolo di strumento au-

[21] Con qualche diversificazione, specie nel rito tributario, in cui le eccezioni dell'Amministrazione sono spesso riproponibili perché soventemente qualificate come mere difese o eccezioni in senso lato.

© Wolters Kluwer Italia

siliario utile ad affiancare il giudice nella valutazione del fatto: ordinare percezioni, collegamenti, ipotesi, anche dubbi, a patto che la decisione rimanga del giudice. Ciò è possibile in quanto la ricostruzione fattuale è intrinsecamente casistica, e, sebbene ai suoi fini risulti poco utile il supporto generico che può essere offerto dalle configurazioni di IA deboli e analitiche, che operano alla stregua di motori di ricerca generalizzati, può trovare valido sostegno nei sistemi di IA forti, generativi e dotati di automazione. Questi ultimi possono assumere una funzione di supporto, fornendo al giudice uno strumento di guida che indichi la corretta ponderazione dei fattori e degli elementi di prova disponibili. In questo senso, l'IA può aiutare a mitigare l'influenza dell'istinto umano, che è spesso vulnerabile alla fatica, a cali di attenzione o alla sopravvalutazione di elementi più immediati ma meno decisivi. In tal modo, l'IA riesce a esaltare i vantaggi dell'intelligenza naturale, pur senza possedere la capacità di mettere in discussione i propri assunti autonomamente e con autocritica.

In conclusione, l'uso dell'IA come ausilio all'intelligenza naturale può rappresentare un supporto efficace per migliorare la qualità del giudizio di fatto, sebbene permanga il problema ontologico dei limiti alla conoscenza a fini giuridici del fatto [22]: rimarrà, quindi, insuperabile dalla tecnica la difficoltà costitutiva legata all'oggetto della ricostruzione, che è pur sempre un fatto avvenuto al di fuori dell'aula di giustizia in un tempo passato e imperfettamente sondabile nella sua esatta materialità

[22] In una certa qual misura è possibile sul punto riconciliarsi con i fautori della tesi oggettivistica del giudizio di fatto. Costoro, infatti, lo definiscono pur sempre come l'accertamento "*di una realtà che sta tutta quanta al di fuori del giudicante*" (P. CALAMANDREI, *Il giudice e lo storico*, cit., p. 394).

© Wolters Kluwer Italia

L'IMPATTO DELL'EVOLUZIONE TECNOLOGICA NEI PROCESSI DECISIONALI AMMINISTRATIVI DI TIPO AMBIENTALE *

MATTEO DE BIASE

SOMMARIO: 1. Il quadro normativo e scientifico di riferimento. – 1.1. Cenni al ruolo dell'evoluzione tecnologica. – 2. Aspetti normativi e frizioni della transizione digitale ed ambientale. – 3. Riflessioni di chiusura e spunti critici: i cc.dd. ESG.

Abstract: Starting from the new constitutionally guaranteed protection aimed at the "interest of future generations" (Articles 9 and 41 of the Constitution), this contribution seeks to relate environmental protection with technological evolution and its implications. Scientific progress has a dual nature: while it poses risks for environmental damage, it also serves as a potential tool for solving future challenges. Questions arise regarding the limits that public administration's decision-making process must follow when utilising artificial intelligence and algorithms, given the increasing legislative attention on environmental assets. The technological and ecological transitions are complementary, even if an anthropocentric view of decision-making processes is maintained. Thus, the analysis will briefly examine some applications that technological evolution currently guarantees in the public sector, in comparison with sustainable finance norms (ESG) included in Directive 2022/2464/EU, which are central to this development process.

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

1. Il quadro normativo e scientifico di riferimento

L'analisi sulla compatibilità tra la nuova tecnologia, in particolare nella forma di intelligenza artificiale (IA), ed i processi amministrativi, specificamente quelli di tipo ambientale, impone di premettere brevi cenni al quadro legislativo ed a quello di tipo scientifico che si è andato ad affermare di recente, al fine di comprendere la rilevanza, ormai anche costituzionale, della questione [1].

Senza voler entrare in campi scientifici differenti, basti segnalare circa il primo punto che la tecnologia, come fenomeno legato all'applicazione della scienza alla realtà sociale, incide ormai in maniera decisiva sulla vita dell'uomo. Partendo dai cicli produttivi, industriali, informativi il processo tecnologico ha invaso altri campi progressivamente, fino ad assumere piena rilevanza anche nel campo giuridico. L'uso tecnologico, si è oggettivamente esteso se si pensa che si è avuta l'esigenza di regolamentare in modo diretto il funzionamento dell'attività informatica in singoli ambiti o nel suo complesso (a titolo esemplificativo, si veda il Codice dell'Amministrazione Digitale). Al contempo, soprattutto nel diritto amministrativo, sono emersi i limiti di compatibilità con i processi decisionali che sono tipicamente caratterizzati dalla presenza dell'uomo e che, ove sostituiti da scelte algoritmiche, possono porre un problema per l'intero sistema [2]. Anche la giurisprudenza ha, invero, implicitamente confermato la portata delle in-

---

[1] Cfr. S. MAGNOLO - A. TAURINO, *Il diritto, la scienza e la tecnologia*, in *Revista Opinião Jurídica*, 23/2018, pp. 13-27.

[2] Sul tema del progresso scientifico in ambito giuridico la letteratura è vasta ormai: F. MIGNELLA CALVOSA - F. PILOZZI - S. TOTAFORTI, *Politiche e strategie di better regulation*, Roma, 2015; S. PENASA, *Nuove dimensioni della ragionevolezza? La ragionevolezza scientifica come parametro della discrezionalità legislativa in ambito medico-scientifico*. *Spunti dalla sentenza n. 162 del 2014 della Corte costituzionale*, disponibile su *www.forumcostituzionale.it*, 16 giugno 2014; M. PICCHI, *Tecniche normative e tutela del buon andamento della pubblica amministrazione: dalla Corte Costituzionale un nuovo impulso per preservare la certezza del diritto*, in *Federalismi.it*, 21/2013, pp. 1-12; M.G. DELLA SCALA, *Le valutazioni tecniche nel procedimento amministrativo*, in A. ROMANO, *L'azione amministrativa*, Torino, 2016, pp. 552 ss.; A. FRANCESCONI, *Innovazione organizzativa e tecnologica in sanità*, Milano, 2007. Cons. St., sez. VI, 13 dicembre 2019, n. 8472, peraltro afferma che "*(...) sempre in linea generale va richiamato quanto già evidenziato dalla sezione in ordine all'elemento positivo derivante dal nuovo contesto di digitalizzazione; in proposito, non può essere messo in discussione che un più elevato livello di digitalizzazione dell'amministrazione pubblica sia fondamentale per migliorare la qualità dei servizi resi ai cittadini e agli utenti. In tale ottica lo stesso Codice dell'amministrazione digitale rappresenta un approdo decisivo in tale direzione*".

© Wolters Kluwer Italia

novazioni tecnologiche nei procedimenti amministrativi poiché, riconoscendone la portata, ha spesso dato vita ad indirizzi ondivaghi come dimostrano le pronunce antitetiche del TAR Lazio e del Consiglio di Stato. Con la sentenza 13 settembre 2019, n. 10964, il TAR Lazio, sez. III *bis*, è tornato a occuparsi dell'utilizzo degli algoritmi informatici da parte delle pubbliche amministrazioni, ribadendo la propria convinzione già espressa con le sentenze 10 settembre 2018, n. 9924, e 27 maggio 2019, n. 6606 sintetizzabile nell'assunto secondo cui l'utilizzo dell'algoritmo fa venire meno l'attività amministrativa, devolvendola ad un meccanismo matematico od informatico impersonale che vìola i principi generali propri della l. 7 agosto 1990, n. 241 [3]. I Giudici di Palazzo Spada, invece, osservano come un più elevato livello di digitalizzazione dell'amministrazione pubblica è fondamentale per il miglioramento della qualità dei servizi ai cittadini e agli utenti, esaltandosi così la trasparenza ed imparzialità amministrativa [4].

Il secondo aspetto evidenziato è relativo al nuovo contesto normativo che, soprattutto in campo ambientale, merita di essere segnalato poiché esso è tangibile ormai anche nel dettato costituzionale. Una corretta disamina dello scenario interno deve necessariamente confrontarsi con la Carta Costituzionale ufficialmente modificata da quando con la Gazzetta Ufficiale n. 44 del 22 febbraio 2022 è stata pubblicata la legge costituzionale 11 febbraio 2022, n. 1, recante "*Modifiche agli articoli 9 e 41 della Costituzione in materia di tutela dell'ambiente*".

Sebbene la tutela ambientale fosse innegabilmente presente già prima, per essere coerenti con la dimensione descritta, si può dire che la Costituzione italiana, una volta riformati gli artt. 9 e 41, ha introdotto un criterio paradigmatico in forza del quale vagliare le attività economiche, che devono conformarsi a tale valore "verde", che passa da principio a vincolo effettivo e che, dunque, consente un riconoscimento particolare innovativo alla Costituzione italiana.

---

[3] Nella sentenza TAR Lazio, sez. III *bis*, 10 settembre 2018, n. 9924 si legge: "*(...) Invero il Collegio è del parere che le procedure informatiche, finanche ove pervengano al loro maggior grado di precisione e addirittura alla perfezione, non possano mai soppiantare, sostituendola davvero appieno, l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere (...)*".

[4] Al punto 7.2 della sentenza n. 8472/2019, il Consiglio di Stato, sez. VI, osserva: "*l'impiego di tali strumenti comporta in realtà una serie di scelte e di assunzioni tutt'altro che neutre: l'adozione di modelli predittivi e di criteri in base ai quali i dati sono raccolti, selezionati, sistematizzati, ordinati e messi insieme, la loro interpretazione e la conseguente formulazione di giudizi sono tutte operazioni frutto di precise scelte e di valori, consapevoli o inconsapevoli (...)*".

© Wolters Kluwer Italia

Al contempo, deve prendersi atto del mancato riferimento ai principi sovranazionali di sviluppo sostenibile o salubrità o non regressione che divide tra chi ha rinvenuto essenzialmente una formula sintetica ma soddisfacente [5] e chi, al contrario, ha evidenziato una carenza colpevole del Legislatore [6].

1.1. *Cenni al ruolo dell'evoluzione tecnologica*

L'ordinamento giuridico è sempre più sensibile alle trasformazioni sociali ed economiche che riguardano la collettività e non può certo dirsi, al fine di individuare un sistema integrato in tutte le sue componenti, che sia auspicabile una logica a compartimenti stagni, privi di legami e di punti di contatto reciproco. In un simile contesto, non può sottacersi il ruolo fondamentale ricoperto dall'evoluzione tecnologica, e prima ancora da quella scientifica, di cui si intende dare atto nel presente contributo, seppure con alcuni passaggi sommari. Si ritiene, infatti, che tali premesse siano utili a comprendere lo scenario che incide sul ruolo nel campo giuridico della tecnologia, e soprattutto dell'intelligenza artificiale (IA), specificamente avendo riguardo ai procedimenti amministrativi in campo ambientale [7].

La stessa nozione che inquadra l'evoluzione tecnologica fa riferimento ad un processo che si protrae nel tempo di creazione di determinati prodotti e servizi, dovuto all'ampliamento delle conoscenze tecni-

---

[5] Cfr. F. DE LEONARDIS, *Lo stato ecologico*, *Approccio sistemico, economia, poteri pubblici e mercato*, Torino, 2023, p. 138, afferma: "*(...) non si può quindi non sottolineare con favore, pur essendo prevalso il cd. modello sintetico di riforma rispetto a quello più analitico (che prevedeva l'inserimento in Costituzione, ad esempio, anche dei principi del diritto ambientale), l'entrata nel lessico della Costituzione di tre nuovi termini («biodiversità», «generazioni future» e «animali») e la precisazione al plurale di un altro, quello di «ecosistema»*".

[6] Talune critiche per l'incompletezza del testo sono state avanzate da chi ha ritenuto che sarebbe stato necessario un riferimento esplicito al concetto di sviluppo sostenibile, peraltro da tempo recepito nella giurisprudenza interna e sovranazionale. Tra tali autori si segnalano per tutti L. BARTOLUCCI, *Il più recente cammino delle generazioni future nel diritto costituzionale,* in *Osservatorio AIC*, 4/2021, p. 215; G. SANTINI, *Costituzione e ambiente: la riforma degli artt. 9 e 41 Cost.,* in *Forum di Quaderni Costituzionali*, 2/2021, pp. 471 ss.

[7] Oggetto dello studio pertanto sono l'insieme di regole e politiche concernenti le c.d. *twin transitions*, quella digitale ed ecologica, assumendo che esse non possano essere affrontate e gestite isolatamente, né da un punto di vista pratico né da un punto di vista giuridico. La necessità di mantenere unite le due transizioni è una sfida particolarmente complessa, considerati gli obiettivi, spesso contrastanti, posti per la realizzazione dell'una o dell'altra.

© Wolters Kluwer Italia

che e scientifiche. All'innovazione tecnologica contribuisce la crescita culturale, scientifica e tecnica che si concretizza attraverso l'attività di ricerca e sperimentazione [8].

Preso atto di un progressivo ed inesorabile sviluppo scientifico e tecnologico, deve segnalarsi che un momento di svolta è rappresentato dal noto interrogativo che si pose A.M. Turing [9], nel domandarsi se le macchine fossero anche in grado di pensare [10].

Da allora, la crescita per implementare un sistema di pensiero applicato alla macchina è stata intensa e a partire dagli anni Ottanta sono state sviluppate le prime applicazioni di intelligenza artificiale in ambito industriale. Oggi, l'IA rappresenta uno dei principali ambiti di interesse della comunità scientifica, con aspetti ancora essenziali per la ricerca potenzialmente in grado di realizzare un nuovo ed importante sviluppo come il *machine learning*, la robotica e l'IA generativa (ne è un esempio ChatGPT) [11].

Tanto è cresciuto il fenomeno che si pone l'esigenza di una regolamentazione che non si è riusciti a garantire in modo progressivo a causa della velocità con cui si è assistito al cambiamento generale. In tal senso, prima tra tutti, l'Unione europea ha promosso il c.d. *AI Act* [12], prima regolamentazione giuridica sull'intelligenza artificiale, che affronta i rischi ad essa correlata ed implementa la Strategia europea per IA [13] (ma già il *Next Generation EU* offriva una prospettiva di

---

[8] Cfr. G. Sirilli, *Innovazione tecnologica,* in *Enciclopedia della scienza e della tecnica Treccani*, 2004.

[9] Alan Mathison Turing è stato un matematico, logico, crittografo e filosofo britannico, considerato uno dei padri dell'informatica e uno dei più grandi matematici del XX secolo.

[10] "*Can machines think?*". Cfr. A.M. Turing, *Computing machinery and intelligence*, in *Mind-A Quarterly Review of Psychology and Philosophy*, 236/1950, pp. 433 ss.

[11] Spunti di interesse per la tematica, ormai attualissima, sono G. Finocchiaro, *Intelligenza artificiale. Quali regole?*, Bologna, 2024; L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, 2021; H. Kissinger - D. Huttenlocher - E. Schmidt, *L'era dell'intelligenza artificiale. Il futuro dell'identità umana*, Milano, 2023.

[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), in G.U.U.E. L/2024/1689 del 12 luglio 2024.

[13] V. in proposito la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni,

© Wolters Kluwer Italia

sviluppo tecnologico). Senza volersi sovrapporre alla normativa sovranazionale, la disciplina interna ha cercato di colmare ulteriori zone grigie con lo schema di disegno di legge recante disposizioni e delega al governo in materia di intelligenza artificiale, approvato in prima battuta dal Consiglio dei Ministri del 23 aprile 2024, al fine di esaltare l'uso corretto dei nuovi strumenti tecnologici [14].

2. Aspetti normativi e frizioni della transizione digitale ed ambientale

Tratteggiato il quadro generale, occorre concentrarsi sul modello amministrativo, nella sua compatibilità e potenziale frizione rispetto a procedimenti che restano altamente peculiari per la sensibilità dei beni che vengono tutelati: l'ambiente entra appieno in questa riflessione.

Come accennato, il regolamento UE sull'intelligenza artificiale rispecchia lo sforzo di individuare un equilibrio tra il progresso tecnologico e la salvaguardia dell'ambiente. Ciò che appare maggiormente critico, e ad oggi non indagato in modo compiuto, è se il procedimento decisionale in materia ambientale possa essere interessato dall'utilizzo di sistemi di intelligenza artificiale, o da progressioni tecnologiche alternative che, negli anni a venire ci si potranno presentare.

Nell'insieme delle disposizioni che assumono rilievo vi è la l. 29 luglio 2021, n. 108, che ha convertito, con talune modificazioni, il d.l. 31 maggio 2021, n. 77, recante "*Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure*". La normativa ha essenzialmente semplificato gli *iter* in materia ambientale, con specifico riguardo alla VIA ed alla VAS, in attuazione degli obblighi europei derivanti dal PNRR. Pur senza riconoscere un diretto riferimento all'utilizzo di sistemi tecnologici avanzati o "intelligenti", l'intero quadro si concentra su un efficientamento e su una esigenza di celerità nella decisione amministrativa che appare, dunque, direttamente collegata all'utilizzo di strumenti informativi ed algoritmici. Lo stesso art. 1, co. 2, esplicita che "*Ai fini del presente decreto e della sua attuazione assume preminente valore l'interesse nazionale alla sollecita*

"*L'intelligenza artificiale per l'Europa*", Bruxelles, 25 aprile 2018, COM(2018)237 final.

[14] Il disegno di legge sull'intelligenza artificiale (d.d.l. intelligenza artificiale), è stato presentato in Senato in data 20 maggio 2024, ed annunciato nella seduta parlamentare n. 191 del 21 maggio 2024.

© Wolters Kluwer Italia

e puntuale realizzazione degli interventi inclusi nei Piani indicati al comma 1, nel pieno rispetto degli standard e delle priorità dell'Unione europea in materia di clima e di ambiente". È indubbio che il procedimento amministrativo algoritmico ha il pregio di velocizzare le procedure decisionali vincolate, come lo stesso Consiglio di Stato ha affermato senza smentire "*canoni di efficienza ed economicità dell'azione amministrativa (art. 1 l. n. 241/90), i quali, secondo il principio costituzionale di buon andamento dell'azione amministrativa (art. 97 Cost.), impongono all'amministrazione il conseguimento dei propri fini con il minor dispendio di mezzi e risorse e attraverso lo snellimento e l'accelerazione dell'iter procedimentale*" [15].

Anche l'art. 54 dell'*AI Act* europeo ricorda che deve mirarsi ad un elevato livello di protezione e di miglioramento della qualità dell'ambiente, peraltro frutto di autonoma regolamentazione con il *Green Deal*, così da offrire una visione integrata e strategica delle due transizioni, per il raggiungimento degli obiettivi di tutela ambientale e di trasformazione digitale [16].

A fronte di questo, tuttavia, si deve segnalare che il Legislatore nazionale ha espresso a chiare lettere l'esigenza di assicurare un approccio di tipo antropocentrico, come emerge dall'art. 3 del d.d.l. sull'intelligenza artificiale [17].

Accanto alla giurisprudenza che ha sposato un orientamento sfa-

---

[15] Per brevità si consenta sul tema del procedimento amministrativo algoritmico e sulle decisioni automatizzate della P.A. di rinviare a D. Marongiu, *L'attività amministrativa automatizzata. Profili giuridici*, Rimini, 2005; A. Masucci, *Procedimento amministrativo e nuove tecnologie. Il procedimento amministrativo elettronico ad istanza di parte*, Torino, 2011; L. Viola, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in *Federalismi.it*, 21/2018, pp. 2-44; Id., *Attività amministrativa e intelligenza artificiale*, in *Cib. dir.*, 1-2/2019, pp. 64 ss.; G. Avanzini, *Decisioni amministrative e algoritmi informatici. Predeterminazione, analisi predittiva e nuove forme di intelligibilità*, Napoli, 2019; E. Carloni, *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni*, in *Dir. pubbl.*, 2/2019, pp. 363 ss.; M.C. Cavallaro - G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *Federalismi.it*, 16/2019, pp. 2-22; S. Civitarese Matteucci, *"Umano troppo umano". Decisioni amministrative automatizzate e principio di legalità*, in *Dir. pubbl.*, 1/2019, pp. 5 ss. La sentenza di cui trattasi è Cons. St., sez. VI, 4 febbraio 2020, n. 881.

[16] Cfr. F. Camisa, *Ambiente e tecnologia: l'interconnessione tra le transizioni gemelle,* in *Federalismi.it*, 14/2024, pp. 55-75; W. D'Avanzo, *Intelligenza artificiale e tutela dell'ambiente*, in *Dir. giur. agr. alim. amb.*, 2/2019.

[17] Cfr. l'art. 3 cit.: "*I sistemi e i modelli di intelligenza artificiale devono essere sviluppati ed applicati nel rispetto della autonomia e del potere decisionale dell'uomo, della prevenzione del danno, della conoscibilità, della spiegabilità e dei principi di cui al comma 1*".

© Wolters Kluwer Italia

vorevole all'uso algoritmico nelle procedure discrezionali [18], si può pensare che a maggior ragione in tale settore sarebbe difficile immaginare una decisione robotizzata, automatica o totalmente artificiale [19].

Tuttavia, ciò non convince. L'apparato normativo non pone delle espresse limitazioni circa l'utilizzo, in senso ausiliario e finanche sostitutivo, di strumenti di IA, se non richiedendosi la salvaguardia della dignità umana, di bisogni comuni, di sostenibilità, per assicurare esigenze comuni e non più individuali. Linea interpretativa che, si può dire, appare confermata non solo dallo schema di disegno di legge in fase di approvazione dal Parlamento italiano, ma anche dal Libro Bianco dell'Unione sull'intelligenza artificiale (COM(2020)65 final) che richiama la centralità della componente umana e la necessità di una corretta gestione del dato, dell'informazione che, ad oggi, è funzionale alla sostenibilità [20].

3. Riflessioni di chiusura e spunti critici: i cc.dd. ESG

Il tentativo di valorizzare una sorta di super-bene a seguito della riforma costituzionale, mai idoneo a recedere rispetto ad altre situazioni giuridiche [21], altamente discrezionale nelle formule di applicazione e, quindi, inidoneo a subire dei condizionamenti tecnologici nel pro-

---

[18] Da un lato, TAR Lazio, sez. III *bis*, 10 settembre 2018, n. 9227; TAR Lazio, sez. III *bis*, 27 maggio 2019, n. 6606. Dall'altro, Cons. St., sez. VI, 13 dicembre 2019, n. 8472/8473/8474 in cui si legge che non vi sono "*ragioni di principio, ovvero concrete, per limitare l'utilizzo all'attività amministrativa vincolata piuttosto che discrezionale, entrambe espressione di attività autoritativa svolta nel perseguimento del pubblico interesse*".

[19] Cfr. N. POSTERARO, *Procedimento amministrativo e decisione amministrativa robotizzata: gli orientamenti della giurisprudenza amministrativa,* in *Osservatorio sullo Stato digitale IRPA*, 27 maggio 2020, il quale evidenzia come la giurisprudenza aperturista "*suscita delle perplessità, posto che non è del tutto chiaro in che termini sia possibile tradurre in linguaggio informatico le espressioni del lessico giuridico che sono connotate da inevitabile incertezza interpretativa*".

[20] Così P. PERLINGIERI, *L'informazione come bene giuridico,* in *Rass. dir. civ.*, 1990, pp. 327 ss.; S. SCHAFF, *La nozione di informazione e la sua rilevanza giuridica,* in *Dir. inform.*, 1987, pp. 445 ss.

[21] Così G. AZZARITI, *Appunto per l'audizione presso la Commissione Affari costituzionali del Senato della Repubblica del 16 gennaio 2020 - Modifica articolo 9 della Costituzione*, in *Osservatorio AIC*, 1/2020, p. 6, ove dice che il bilanciamento tra interessi economico finanziari ed ambiente è destinato ad essere "*ineguale*" alla luce del nuovo assetto costituzionale. Impostazione che può porsi in apparente conflitto con l'insegnamento di Corte Cost., 9 maggio 2013, n. 85, per cui il bilanciamento tra interessi tutti costituzionalmente rilevanti deve essere condotto senza consentire "*l'illi-*

© Wolters Kluwer Italia

cesso decisionale, non appare condivisibile. Il punto cruciale è, anzi, se alla luce di quanto emerso possa dirsi che esiste una totale equiparabilità della valutazione umana e della macchina tanto da ammettere, soprattutto in una dimensione ambientale, la possibilità di far ricorso totalmente a sistemi di IA per la valutazione di dati, l'elaborazione di informazione, l'assunzione di decisioni.

Se ad oggi l'uso in campo pubblico si registra con riguardo alla prevenzione degli illeciti ambientali e monitoraggio di aree a rischio (si pensi ai droni di controllo), alla capacità di prevedere eventi atmosferici anomali e pericolosi, alla ricerca di agenti inquinanti presenti in natura e nel suolo, è il settore privato che appare pioniere circa la combinabilità della transizione tecnologica e di quella ecologica.

Nel sistema aziendale, deve prendersi atto della pubblicazione della direttiva (UE) 2022/2464, nota come *CSRD* (acronimo di *Corporate Sustainability Reporting Directive*), finalizzata ad esaltare la finanza sostenibile. Senza voler entrare nei dettagli della nuova disciplina eurounitaria, sono le normative di *environmental, social and governance (ESG)* che attraggono, per il fine che qui interessa, la nostra attenzione. Gli indicatori *ESG*, consentono di valutare l'impegno dell'azienda nella tutela dell'ambiente e nella riduzione delle emissioni inquinanti [22]. Per la corretta elaborazione degli *ESG* assume rilievo proprio l'intelligenza artificiale, poiché, a fronte dell'enorme numero di variabili, permette di monitorare, analizzare e gestire in modo più preciso i dati legati all'ambiente, le problematiche sociali e le necessità che attengono alla *governance* aziendale potendo contare sulla capacità di disporre di una importante capacità predittiva e ridurre il *risk management*.

Ritenere incompatibile l'utilizzo del *machine learning* con la tutela ambientale solo perché gli interessi in gioco sarebbero molteplici ed imporrebbero un bilanciamento tra quelli pubblici e secondari, appare non accettabile, anche perché pure nell'attività aziendale non esiste un unico fine cui si tende, ma vi è l'esigenza di costante contemperamento di posizioni diverse. Da ciò può dirsi che il sistema analizzato sia precursore utile per i procedimenti amministrativi involgenti il bene ambiente.

---

mitata espansione di uno dei diritti, che diverrebbe «tiranno» nei confronti delle altre situazioni giuridiche costituzionalmente riconosciute e protette".

[22] Cfr. S. Scalzini - R. Rota, *Implementazione della Corporate Sustainability Reporting Directive 2464/2022 a livello europeo e suo recepimento in Italia: i contenuti della Direttiva,* in *Astrid Rassegna*, 16/2023, pp. 1-44.

© Wolters Kluwer Italia

PROCESSO PENALE E *DIGITAL EVIDENCE*: SFIDE IRRISOLTE NELL'ACQUISIZIONE DI CONVERSAZIONI DIGITALI *

Iacopo Chianello

Sommario: 1. La prova digitale nel processo penale. – 2. L'acquisizione di conversazioni digitali. – 3. Sequestro *omnibus* e lesione del diritto alla riservatezza. – 4. I principali correttivi. – 5. L'intervento della Corte costituzionale. – 6. Il nuovo disegno di legge. – 7. Considerazioni conclusive.

Abstract: The evolution of technology had a deep impact on the field of criminal law, opening up new frontiers for crime and forcing legislators to reshape traditional criminal categories to adapt to the constantly evolving digital reality. At the same time, this phenomenon has significantly influenced criminal justice, which, in its attempt to investigate and repress these new types of crimes, has had to deal with the issue of so-called digital evidence. As of today, the rules governing the acquisition of digital evidence under the Code of Criminal Procedure are highly inadequate, particularly when it comes to acquiring communicative digital data stored within the memory of a computer device, such as conversations exchanged via instant messaging platforms or e-mail inboxes. In recent years, this issue has sparked intense debate, first engaging the jurisprudence of legitimacy, then the Constitutional Court, and more recently, the legislature. The latter has recently intervened with a new legislative proposal, currently under review. This contribution will examine the issue of acquiring digital communication data in criminal proceedings, analysing the issues of violation of fundamental rights and identifying potential corrective measures.

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

1. La prova digitale nel processo penale

La crescente diffusione globale di dispositivi informatici e nuovi mezzi di comunicazione di massa, risultato dell'incessante avanzamento tecnologico, ha profondamente rivoluzionato la giustizia penale. Da un lato, il legislatore è stato chiamato a rivedere e adattare molti istituti del processo penale; dall'altro, la giurisprudenza ha dovuto ridefinire i criteri di ammissibilità delle prove ottenute tramite le nuove tecnologie.

Da questo cambiamento è emersa una questione cruciale, ossia quella di salvaguardare i principi costituzionali dal potenziale abuso di tali nuovi strumenti tecnologici per fini investigativi. Da tempo, infatti, è stato evidenziato come i dispositivi informatici rappresentino una proiezione digitale dell'individuo, un'estensione della sua vita privata e relazionale, come tali rientranti nella sfera di protezione di norme costituzionali poste a salvaguardia di diritti fondamentali, quali la libertà personale, l'inviolabilità del domicilio (inteso come "domicilio informatico"), la libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione, la riservatezza della vita privata [1].

Con la l. 18 marzo 2008, n. 48 (con cui è stata ratificata la Convenzione di Budapest sulla criminalità informatica del 2001) è stata per la prima volta introdotta all'interno del codice di procedura penale una specifica disciplina in materia di acquisizione della *digital evidence*.

Caratteristica peculiare dell'attività di ricerca e acquisizione delle prove digitali regolamentata dalla l. n. 48/2008 è quella di essere circondata da garanzie procedurali ulteriori rispetto a quelle già previste per gli ordinari strumenti di ricerca della prova. Ciò è dovuto alla particolare natura della prova digitale, che, in quanto dematerializzata, esiste indipendentemente dal supporto informatico all'interno del quale si trova ed è in grado di transitare, con estrema facilità, da un "contenitore" all'altro, esponendosi inevitabilmente ad un più alto rischio di manipolazione e alterazione.

Nella prassi, proprio al fine di garantire la genuinità e non alterabilità dei dati digitali, gli inquirenti procedono dapprima al sequestro del dispositivo informatico per poi acquisirne il contenuto attraverso la c.d. copia forense o *bit stream image*, la quale consiste nella integrale duplicazione, *bit* per *bit,* dell'*hard disk* del dispositivo, comprese le

[1] Cfr. sul punto S. SIGNORATO, *Le indagini digitali profili strutturali di una metamorfosi investigativa*, Torino, 2018, pp. 57 ss.

© Wolters Kluwer Italia

cosiddette "aree non allocate" del disco fisso, contenenti *file* cancellati e non visibili all'utente. Le informazioni clonate vengono poi trasferite all'interno di un diverso supporto, mantenendo la medesima sequenza di valori binaria del documento digitale originario.

Una volta formata una copia conforme al documento digitale originario, occorre poi assicurare la non modificabilità della copia clone, attraverso la c.d. catena di custodia.

La migliore e più diffusa metodica idonea a garantire una corretta catena di custodia consiste nell'applicare una funzione di *Hash* [2] alla copia forense ottenuta con il sistema della *bit stream image*. Si tratta di una funzione che trasforma una sequenza di *bit* di lunghezza variabile (*input*) in un'altra sequenza di *bit* di lunghezza predefinita chiamata *digest*. Ciò ne garantisce l'immodificabilità, poiché ogni minima alterazione della copia originaria avvenuta nel corso dei diversi "passaggi di mano" risulterà immediatamente visibile una volta calcolato il relativo *digest*.

Solo a questo punto, gli inquirenti possono compiere la vera e propria attività di ricerca al fine di rinvenire e, conseguentemente, acquisire agli atti del procedimento le informazioni digitali pertinenti al reato. È chiaro quindi che, a differenza di quanto avviene nel campo dei tradizionali mezzi di ricerca della prova, quando si tratta di acquisire dati digitali, il sequestro probatorio precede la perquisizione informatica.

2. L'acquisizione di conversazioni digitali

Uno degli aspetti più controversi della disciplina in materia di ricerca della prova informatica riguarda le modalità di acquisizione delle conversazioni digitali intercorse attraverso l'utilizzo di piattaforme di messaggistica istantanea o caselle di posta elettronica e conservate all'interno della memoria del dispositivo informatico (*Pc, Tablet, smartphone*). Si tratta, in particolare, di SMS, messaggi *WhatsApp*, *e-mail* spedite, ricevute, ovvero giacenti nella cartella "Bozze" della casella di posta elettronica.

Il tema ha sollevato un acceso dibattito in giurisprudenza data la mancanza di una disposizione in grado di attribuire una precisa qualificazione giuridica a tali particolari dati informatici. In astratto, infatti,

[2] Più in dettaglio cfr. C. PARODI - V. SELLAROLI (a cura di), *Diritto penale dell'informatica*, I ed., Milano, pp. 26 ss.

© Wolters Kluwer Italia

tale attività di acquisizione della prova si presta ad essere inquadrata entro tre diverse discipline: quella delle intercettazioni di flussi di comunicazioni informatiche e telematiche (artt. 266-*bis* e 268, comma 3-*bis*, c.p.p.); quella del sequestro probatorio del corpo del reato e delle cose pertinenti al reato (art. 253 c.p.p.); ovvero ancora quella del sequestro di corrispondenza (art. 254 c.p.p.).

Da principio, la Suprema Corte [3] ha scelto di aderire alla tesi incentrata sul criterio dell'"inoltro", in base alla quale, tutte le volte in cui il messaggio è stato inoltrato al destinatario, è pur sempre intervenuto un "flusso informatico", come tale intercettabile, indipendentemente dalla sussistenza del requisito dell'"attualità" della conversazione rispetto all'atto acquisitivo. Solo quando le *e-mail* non sono state inoltrate, ma sono rimaste archiviate all'interno cartella "Bozze", deve trovare applicazione la disciplina del sequestro probatorio, per il quale, come noto, non occorre alcuna autorizzazione da parte del Giudice [4].

Successivamente, la giurisprudenza di legittimità [5], seguendo un approccio diametralmente opposto, ha stabilito che i dati informatici di natura comunicativa memorizzati all'interno di un dispositivo informatico hanno sempre natura documentale e, di conseguenza, la relativa attività acquisitiva non soggiace né alle regole previste per la corrispondenza, né tantomeno a quelle stabilite per le intercettazioni, ma deve essere regolata dalle disposizioni relative al sequestro probatorio di cui all'art. 253 c.p.p.

Secondo quest'ultimo arresto, infatti, l'impossibilità di applicare le disposizioni previste in materia di corrispondenza e intercettazioni deriva dal fatto che queste ultime, per loro natura, implicano la captazione di flussi comunicativi in corso; circostanza questa che risulta del tutto assente quando si deve procedere all'acquisizione di dati "freddi", giacenti all'interno della memoria digitale di un dispositivo [6].

---

[3] Cass. pen., sez. IV, 28 giugno 2016, n. 40903.

[4] Sul punto cfr. L. GIORDANO, *L'intercettazione delle e-mail (già) ricevute o inviate e l'acquisizione di quelle parcheggiate nella cartella "bozze"*, in *Ilpenalista.it*, 14 novembre 2016.

[5] Cass. pen., sez. V, 21 novembre 2017, n. 1822.

[6] Analogo problema è sorto con riferimento all'acquisizione mediante ordine europeo di indagine di conversazioni digitali intercorse su canali criptati (come *Sky ECC* e *Encrochat*), già autonomamente raccolte e decrittate dalla autorità giudiziaria estera. Sul punto cfr. Cass. pen., sez. un., 14 giugno 2024, n. 23755 e Cass. pen., sez. un., 14 giugno 2024, n. 23756, con le quali è stato stabilito che, trattandosi di una situazione che implica una collaborazione transfrontaliera e non un intervento esclusivo della autorità giudiziaria italiana, l'acquisizione del contenuto di tali conversazioni, anche nel caso in cui fossero state carpite all'estero mediante intercettazione, non deve essere

© Wolters Kluwer Italia

3. Sequestro *omnibus* e lesione del diritto alla riservatezza

È facile, tuttavia, rendersi conto di come quest'ultimo indirizzo della giurisprudenza di legittimità finisca per ledere irrimediabilmente diritti fondamentali della persona, quali, *in primis*, quello della *privacy* e della libertà e segretezza di ogni forma di comunicazione.

Escludendo, infatti, l'applicazione della disciplina delle intercettazioni e del sequestro di corrispondenza vengono meno anche le relative garanzie. Ciò significa che il Pubblico Ministero può disporre il sequestro dei dati senza che sia necessario un previo provvedimento autorizzativo del Giudice e, in questo modo, procedere alla integrale e indiscriminata apprensione di tutti i dati archiviati all'interno della memoria del dispositivo sequestrato, anche di quelli più risalenti nel tempo e di natura strettamente personale e sensibile.

Invero, dall'analisi della disciplina in materia di sequestro di dati informatici non emerge alcun limite rispetto l'attività di acquisizione probatoria compiuta dagli inquirenti [7].

La l. n. 48/2008 si preoccupa esclusivamente che la copia forense dei dati informatici venga realizzata mediante una procedura che ne assicuri la genuinità e immodificabilità, senza richiedere alcun vincolo di pertinenzialità tra i dati informatici duplicati e il reato per il quale si procede. Ciò consente al Pubblico Ministero di compiere indagini di natura "esplorativa" e di entrare in contatto con una mole potenzialmente smisurata di dati informatici [8].

---

preceduta da alcuna autorizzazione del giudice italiano, poiché quest'ultima, nella disciplina nazionale relativa alla circolazione delle prove, non è richiesta per conseguire la disponibilità del contenuto di comunicazioni già acquisite in altro procedimento. La mancanza di un'autorizzazione preventiva non esclude tuttavia un vaglio giurisdizionale postumo, poiché l'utilizzabilità in giudizio del contenuto di tali conversazioni deve essere esclusa se il giudice italiano rileva che il loro impiego determinerebbe una violazione dei diritti fondamentali, fermo restando che l'onere di allegare e provare i fatti da cui inferire tale violazione grava sulla parte interessata. Cfr. sul punto anche C. giust. UE, 30 aprile 2024, C-670/22, *M.N. (EncroChat)*.

[7] Invero, la mancanza di limiti rispetto all'attività di duplicazione dei dati informatici contenuti all'interno del dispositivo sequestrato sembra sussistere solo quando è il Pubblico Ministero a procedere al sequestro. Viceversa, quando ad effettuare il sequestro è la polizia giudiziaria, l'art. 354 c.p.p., comma 2, prevede espressamente che si possa procedere ad un sequestro selettivo dei dati pertinenti al reato.

[8] Sul pericolo di attività investigative di natura "esplorativa" cfr. anche M. PITTIRUTI, *Dalla Corte di cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus*, in *Sist. pen.*, 14 gennaio 2021.

© Wolters Kluwer Italia

4. I principali correttivi

Il *vulnus* ai diritti fondamentali insito nei casi di sequestro *omnibus* di dati informatici è stato in parte mitigato a seguito dell'intervento della giurisprudenza di legittimità con la sentenza n. 34265/2020 [9].

Tale pronuncia trae origine da una nota vicenda giudiziaria (caso *Fondazione Open*) in cui il Pubblico Ministero aveva proceduto al sequestro presso terzi di numerosi dispositivi elettronici contenenti conversazioni intercorse con esponenti politici.

Nel caso di specie, il Supremo Collegio ha individuato un fondamentale limite al sequestro *omnibus* di dati digitali. È stato infatti stabilito che, una volta sequestrati i dispositivi elettronici ed effettuata la copia integrale dei dati contenuti al loro interno, il Pubblico Ministero ha il dovere non soltanto di restituire il dispositivo, ossia il c.d. "contenitore" in cui sono stati rinvenuti i dati (così come previsto dall'art. 262 c.p.p.) [10], ma deve provvedere anche alla restituzione della stessa copia integrale, dopo aver opportunamente selezionato solo le informazioni pertinenti al reato per il quale si procede.

La copia integrale è dunque una semplice "copia-mezzo", non una "copia-fine", e, come tale, deve essere restituita all'avente diritto nel più breve tempo possibile e il trattenimento della stessa non deve eccedere i limiti di quanto è strettamente necessario alla selezione dei contenuti rilevanti per il processo.

Tale orientamento, tuttavia, argina solo in parte il rischio di compromissione della *privacy* tipico dei casi di sequestro generalizzato di dati digitali.

La restituzione della copia integrale non garantisce, infatti, che l'autorità procedente abbia correttamente selezionato i dati contenuti al suo interno, escludendo ogni informazione che non presenti correlazione con il reato oggetto del procedimento.

Per tale ragione, la dottrina [11] ha individuato ulteriori possibili correttivi al problema.

Uno di questi consiste nel qualificare la procedura di *bit stream*

---

[9] Cass. pen., sez. VI, 22 settembre 2020, n. 34265.

[10] Sull'interesse a proporre riesame anche a seguito della restituzione del dispositivo cfr. Cass. pen., sez. un., 20 luglio 2017, n. 40963, con nota di P. RIVELLO, *L'interesse alla richiesta di riesame del provvedimento di sequestro probatorio di materiale informatico*, in *Cass. pen.,* 1/2018, pp. 131 ss.

[11] Sul punto cfr. F. CERQUA, *Tra comunicazioni telematiche e rito: il sequestro della corrispondenza elettronica*, in L. LUPÁRIA - L. MARAFIOTI - G. PAOLOZZI (a cura di), *Dimensione tecnologica e prova penale*, I ed., Torino, 2019, pp. 105 ss.

© Wolters Kluwer Italia

image dei dati digitali conservati all'interno del supporto informatico come "accertamento tecnico irripetibile" ai sensi dell'art. 360 c.p.p., in modo da consentire alle parti di presenziare all'attività di duplicazione e attivare sin dalla fase investigativa le garanzie del contraddittorio, contribuendo così alla corretta selezione dei dati pertinenti al reato [12].

5. L'intervento della Corte costituzionale

Il tema dell'acquisizione di conversazione digitali memorizzate all'interno di dispositivi informatici e la conseguente necessità di tutelare le aspettative di riservatezza del singolo a fronte di "derive esplorative" dei mezzi di ricerca della prova è stato di recente affrontato anche dalla Corte costituzionale, chiamata a pronunciarsi in ordine ad un conflitto di attribuzione tra poteri dello Stato. Tale conflitto era stato promosso dal Senato nei confronti della Procura della Repubblica presso il Tribunale ordinario di Firenze per avere quest'ultima acquisito agli atti del procedimento penale, nell'ambito del già citato caso *Fondazione Open*, messaggi di testo scambiati tramite piattaforma *WhatsApp* e caselle di posta elettronica, che erano stati acquisiti per mezzo del sequestro di *smartphone* (appartenenti a terzi) in mancanza di una previa autorizzazione da parte dell'assemblea legislativa ai sensi dell'art. 68 Cost.

Con tale cruciale sentenza [13] la Consulta, allineandosi all'orientamento della Corte europea dei diritti dell'uomo [14], ha stabilito che la nozione di "corrispondenza" si presta senz'altro a ricomprendere, oltre alla tradizionale corrispondenza cartacea recapitata a mezzo del servizio postale e telegrafico, anche i messaggi scambiati attraverso strumenti di tipo informatico e telematico, resi disponibili dall'evoluzione tecnologica. Ciò avviene anche nel caso in cui tali messaggi siano già giunti a conoscenza del destinatario e conservati nella sua casella di posta elettronica (nel caso delle *e-mail*), ovvero nella memoria del dispositivo mobile su cui è installata l'applicazione utilizzata per la loro trasmissione (nel caso dei messaggi *WhatsApp*); diversamente opinan-

---

[12] Di contrario avviso è la giurisprudenza maggioritaria, la quale ritiene che l'attività di estrazione di copia di dati digitali da un dispositivo elettronico oggetto di sequestro non determini alcuna alterazione dello stato delle cose, essendo sempre assicurata la riproducibilità d'informazioni identiche a quelle contenute nell'originale. Sul punto cfr. Cass. pen., sez. II, 4 aprile 2015, n. 24998.

[13] C. Cost., 27 luglio 2023, n. 170.

[14] Cfr., *ex multis*, C. eur. dir. uomo, 17 dicembre 2020, ricorso n. 459/18, *Saber* c. *Norvegia*.

© Wolters Kluwer Italia

do, le garanzie di cui agli artt. 15 e 68, comma 3, Cost. risulterebbero facilmente aggirabili, poiché piuttosto che captare le comunicazioni nel momento in cui si svolgono, basterebbe attenderne la ricezione, per poi sequestrare il dispositivo in cui vi è traccia del loro contenuto senza particolari cautele.

6. Il nuovo disegno di legge

Nel tentativo di recepire i principi enucleati dalla Consulta, il legislatore è intervenuto con il disegno di legge n. 806, il cui testo è stato poi sostituito dall'emendamento n. 1.100, attualmente in fase di approvazione, recante "*Modifiche al codice di procedura penale in materia di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali*".

Secondo tale proposta normativa, la procedura di sequestro dei dispositivi informatici deve articolarsi in tre fasi.

Nella prima fase, il Giudice per le indagini preliminari, su richiesta del Pubblico Ministero, dispone il sequestro del dispositivo in presenza di due presupposti: la necessità per la prosecuzione delle indagini e il rispetto del criterio di proporzionalità della misura [15].

Successivamente, gli inquirenti procedono alla integrale duplicazione del contenuto dei dispositivi in sequestro, ma anche di tutti i dati e le informazioni accessibili da remoto.

La novità rispetto al passato deriva dal più intenso coinvolgimento delle parti, le quali sono avvisate del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico per la duplicazione del contenuto dei dispositivi informatici in sequestro, con facoltà di nominare consulenti tecnici e di partecipare allo svolgimento delle operazioni di duplicazione formulando osservazioni e riserve [16].

La terza fase è a sua volta scomponibile in due diversi segmenti.

Infatti, una volta terminata l'analisi del patrimonio informatico sequestrato, se i dati da acquisire non presentano natura comunicativa, il Pubblico Ministero può sequestrali con proprio decreto motivato nel

[15] Nei casi di urgenza la polizia giudiziaria può procedere di propria iniziativa e, nelle quarantotto ore successive, trasmettere il verbale al Pubblico Ministero ai fini della convalida.

[16] Sono tuttavia previste alcune eccezioni che permettono di derogare a tali disposizioni, come nel caso in cui vi sia un pericolo per la vita o l'incolumità di una persona, per la sicurezza dello Stato, o in presenza di un concreto pregiudizio per le indagini in corso.

© Wolters Kluwer Italia

rispetto dei criteri di necessità e proporzione; qualora invece l'autorità procedente si trovi in presenza di dati inerenti a conversazioni, al fine di procedere al relativo sequestro deve ottenere una seconda autorizzazione da parte del G.I.P., il quale provvede con decreto motivato in presenza degli stessi presupposti previsti in materia di intercettazioni agli artt. 266 e 267 c.p.p.

In particolare, l'autorizzazione potrà essere rilasciata solo per determinate tipologie di delitti, a patto che sussistano gravi indizi di reato e l'acquisizione dei dati risulti assolutamente indispensabile ai fini della prosecuzione delle indagini.

Di fondamentale importanza è poi la conservazione del duplicato informatico, che avviene presso la Procura della Repubblica, in luogo protetto da specifiche misure di sicurezza, con modalità tali da assicurarne l'assoluta riservatezza, fino a sentenza (o decreto penale) non più soggetta ad impugnazione, salva la possibilità per gli interessati di richiedere la distruzione anticipata dei dati non necessari per il procedimento.

7. Considerazioni conclusive

Nell'attuale scenario giuridico la tutela della riservatezza è sicuramente un tema di primaria importanza come dimostrano i continui *revirement* giurisprudenziali sul tema e il recente ricorso per conflitto di attribuzione tra poteri dello Stato promosso del Senato avverso la Procura della Repubblica di Firenze in relazione al caso *Fondazione Open*.

In un contesto di questo genere, l'orientamento della giurisprudenza di legittimità, secondo cui l'acquisizione di dati informatici memorizzati all'interno di un dispositivo elettronico non soggiace né alla disciplina relativa alla corrispondenza né a quella inerente alle intercettazioni, non può che apparire manifestamente iniquo, soprattutto alla luce della recente sentenza della Corte costituzionale.

Coglie pertanto nel segno il nuovo progetto normativo che sceglie di percorrere la strada dell'armonizzazione tra la disciplina del sequestro probatorio e quella più garantita delle intercettazioni. L'avvento delle nuove tecnologie informatiche, la loro rapida diffusione e il loro costante utilizzo per esigenze comunicative ha infatti già da tempo dimostrato come il concetto di "comunicazione intercettabile" debba essere ampliato fino a ricomprendere qualsiasi flusso comunicativo riservato ed intercorrente tra più sistemi o di tipo unidirezionale, anche in

© Wolters Kluwer Italia

quei casi in cui manchi del tutto il requisito dell'attualità della conversazione rispetto all'atto acquisitivo [17].

Occorre tuttavia segnalare come la proposta normativa lasci irrisolte alcune cruciali problematiche, che, a ben vedere, derivano proprio dalla non totale equiparazione alla disciplina delle intercettazioni. In particolare, non convince la scelta di consentire in un primo momento l'illimitata e totalizzante apprensione dei dati digitali contenuti nel dispositivo, per poi differenziare la procedura solo successivamente a seconda della natura comunicativa o meno dei dati acquisiti.

Infatti, una volta che si è proceduto alla integrale acquisizione del contenuto informatico, il danno alla riservatezza e agli altri diritti fondamentali coinvolti si è già pienamente consumato. In altri termini, nella nuova proposta normativa mancano apposite garanzie che, in ossequio alla riserva di legge rinforzata posta dall'art. 15 Cost., siano in grado di limitare a quanto strettamente necessario per il procedimento penale l'iniziale intrusione nella sfera di comunicazioni private dell'individuo, assicurando l'effettivo rispetto del criterio della proporzionalità [18].

Sarebbe pertanto auspicabile una revisione della normativa in fase di approvazione, attraverso l'introduzione di limiti più rigorosi all'attività di duplicazione del contenuto del dispositivo informatico, in modo da garantire una più intensa tutela dei principi di matrice costituzionale e sovranazionale.

Qualunque strada il legislatore decida di intraprendere per affrontare le questioni appena esposte, una cosa è certa: occorre procedere il prima possibile ad una revisione complessiva della disciplina relativa all'acquisizione dei dati digitali, poiché la regolamentazione attuale continua a porsi in netto contrasto con i diritti fondamentali e, in particolare, con un principio che nell'attuale periodo storico assume sempre più rilevanza, ossia quello dell'intangibilità della vita digitale [19].

---

[17] Ne parla A. BARBIERI, *I limiti di utilizzabilità dei messaggi crittografati scaricati da server estero ed acquisiti mediante ordine europeo di indagine*, in *Giur. pen. web*, 2/2023, pp. 23 ss.

[18] Tali criticità sono rilevate anche da O. MURRO, *Sequestro di dispositivi informatici: verso l'art. 254 ter c.p.p.? Brevi note a margine del D.D.L. A.S. N. 806*, in *Penaledp.it*, 12 marzo 2024.

[19] Sul punto cfr. S. SIGNORATO, *Le indagini digitali*, cit., pp. 69 ss.

© Wolters Kluwer Italia

Sezione Quarta

DIVIETO DI DISCRIMINAZIONE E TUTELA DEI DIRITTI DELLA PERSONA

IL RISCHIO DI DISCRIMINAZIONE ALGORITMICA NEL MERCATO DEL LAVORO DELL'ERA DIGITALE: LE NORME DELL'UNIONE EUROPEA NEL QUADRO DELLA *GIG ECONOMY* *

SILVIA VENTRELLI

SOMMARIO: 1. Un algoritmo che "impara" a discriminare: i pericoli dei sistemi automatizzati nel mondo del lavoro. – 2. La risposta dell'Unione europea alla discriminazione algoritmica. – 2.1. Le garanzie antidiscriminatorie previste nella proposta di direttiva in materia di lavoro su piattaforma digitale. – 3. Riflessioni finali.

Abstract: With the advent of modern technologies, the European Union has emphasised the need to promote anthropocentric artificial intelligence that ensures a high level of protection for fundamental rights. The use of AI algorithms for automatic or semi-automatic decision-making is rapidly expanding in various areas, including the labour market. This has raised concerns about algorithmic discrimination, which threatens workers' fundamental rights. The EU prioritises combating discrimination (as stated in Article 3 TEU and Article 21 CFREU) and has recently adopted the European Pillar of Social Rights to promote fair treatment in labour relations. A significant development in this area is the European Parliament's approval of a new Directive on the working conditions of digital platform workers. These new rules aim to prevent platform workers from being dismissed based on automated decisions. The purpose of this contribution is to examine the EU's measures to counter algorithmic discrimination, highlighting how the new Directive and the AI Act aim to promote AI that respects individual fundamental rights.

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

1. Un algoritmo che "impara" a discriminare: i pericoli dei sistemi automatizzati nel mondo del lavoro

Con l'avvento delle più recenti tecnologie il mondo del lavoro appare in profonda evoluzione. Lo sviluppo impetuoso dell'intelligenza artificiale sta determinando imponenti e radicali trasformazioni nel settore lavoristico. Nelle aziende, ad esempio, ha favorito un'organizzazione orizzontale della produzione attraverso l'utilizzo, come forza lavoro, di una molteplicità di operatori sparsi in tutto il mondo [1]. La tecnologia digitale rende infatti estremamente facile offrire sul mercato, ad altre imprese o sempre più frequentemente a singoli lavoratori, il compito di fornire, dietro corrispettivo, una prestazione singola e tendenzialmente semplice. Si parla, a questo riguardo, di *GIG economy*, termine che, secondo la definizione del *Cambridge Dictionary,* individua una struttura di lavoro nella quale singoli individui svolgono, in via assolutamente temporanea, singoli lavori o parti di lavoro e vengono retribuiti separatamente per ogni prestazione effettuata [2].

La *GIG economy* può determinare, e molto spesso determina, svantaggi notevoli per i prestatori di lavoro, quali, ad esempio: guadagni bassi e non prevedibili nel loro ammontare, disparità di trattamento e isolamento rispetto agli altri lavoratori, minore potere contrattuale. Altri problemi di grande rilievo sono dati dalla mancanza di *privacy,* atteso che, di fatto, il controllo sull'attività dei lavoratori consentito dalle nuove tecnologie può essere estremamente pervasivo. Si pensi alla geolocalizzazione consentita dallo *smartphone*, che rende possibile, nel caso dei *riders*, il monitoraggio costante e in tempo reale del numero di consegne effettuato, della velocità di spostamento e del percorso effettuato.

È evidente dunque che, in tale sistema, il problema della tutela del lavoro gestito da piattaforme informatiche (come quello dei *riders*) sta diventando oggetto di un crescente dibattito. Soprattutto la letteratura americana [3], comunque poi seguita anche dalla dottrina europea, ha già da tempo messo in evidenza i pericoli derivanti dal cosiddetto *ma-*

---

[1] Il modello organizzativo tradizionale delle aziende è invece caratterizzato da imprese grandi e integrate in senso verticale, che utilizzano una forza lavoro tendenzialmente stabile.

[2] Non a caso il termine originale *GIG* era usato negli Stati Uniti per individuare l'incarico per una serata conferito a un suonatore di jazz per suonare in un club. Di fatto attualmente la *GIG economy* raccoglie nel suo ambito e nella sua definizione gli esempi più importanti di lavoro basato e gestito da piattaforme informatiche.

[3] A. MATEESCU - A. NGUYEN, *Algorithmic Management in the Workplace*, in *Data*

© Wolters Kluwer Italia

nagement by algorithm, cioè i problemi provenienti dalla gestione del rapporto di lavoro basata sull'algoritmo. Tale gestione può essere effettivamente fonte di discriminazione allorquando, sotto vari profili, essa entra in conflitto con i diritti fondamentali del lavoratore, fattispecie nella quale si può parlare di "discriminazione algoritmica". Per comprendere il significato di tale espressione sembra utile chiedersi: com'è possibile che un algoritmo, cioè un'operazione matematica automatizzata e quindi incosciente, sia in grado di generare discriminazione?

È stato chiarito, al riguardo, che l'incoscienza dell'algoritmo è irrilevante ai fini dell'insorgenza della discriminazione [4]. La nozione di discriminazione proveniente dalle fonti di matrice unionale precisa, infatti, che ad essere rilevante è l'effetto che determina l'applicazione e l'operatività della regola dettata dall'algoritmo. Inoltre, come insegna il diritto antidiscriminatorio, anche una sequenza di istruzioni apparentemente neutra può generare discriminazione attraverso l'impatto differenziato che può determinarsi a detrimento dei portatori di un fattore di rischio (si parla in questo caso di discriminazione indiretta) [5].

Le forme di discriminazione che si possono configurare nei processi algoritmici sono molteplici e questo dipende anzitutto dalla diversa tipologia di algoritmo utilizzato. In termini generali, per algoritmo si intende la procedura di calcolo connotato da un numero finito di regole che conduce al risultato dopo un numero finito di operazioni. In pratica, si tratta di una sequenza di istruzioni codificate tramite *software* e dirette a un *computer*.

L'algoritmo che regola i sistemi di lavoro tramite piattaforme digitali (come appunto il caso dei *riders*) è chiamato *logic-based*. Ciò in quanto è costituito da un insieme di regole di deduzione logica, scritte in sede di programmazione, che hanno carattere deterministico (ossia: a parità di dati d'ingresso, può condurre ad un solo possibile percorso e ad un solo possibile risultato). Dunque, la regola che viene cristallizzata all'interno dell'algoritmo conduce ad un processo decisiona-

---

& Society Research Institute, 2019; J. Adams-Prassl, *What if Your Boss was an Algorithm?*, in *Comparative Labor Law & Policy Journal*, 41/2019, pp. 131 ss.

[4] M. Peruzzi, *La discriminazione algoritmica,* in *Rivista di diritto antidiscriminatorio*, 1/2024, pp. 7-23.

[5] È questa l'ipotesi che si è verificata nei più noti casi di discriminazione algoritmica, ossia quelli degli algoritmi utilizzati da piattaforme digitali, come *Deliveroo* o *Foodinho*, per la profilazione e il *ranking* dei propri *riders*, nonché per la conseguente organizzazione del sistema di prenotazione degli *slot* di lavoro. Come affermato dai Tribunali di Bologna e di Palermo (Trib. Bologna, ord. 31 dicembre 2020; Trib. Palermo, sent. 17 novembre 2023), l'incoscienza della macchina e l'applicazione indifferenziata dei parametri di valutazione non escludono l'accertamento della discriminazione.

© Wolters Kluwer Italia

le automatizzato che non distingue le diversità. Se la regola è uguale per tutti, è evidente che in questa regola si possono annidare forme di discriminazione [6].

Un altro tipo di discriminazione può essere generato dagli algoritmi *machine learning*, rispetto ai quali il processo decisionale è basato su un metodo statistico/probabilistico. Qui la macchina non dispone di un modello di relazioni logiche precodificato per estrarre e ottimizzare l'*output*, ma piuttosto l'obiettivo del sistema è proprio quello di elaborare un tale modello, individuandone e ottimizzandone i parametri a partire da un'ampia quantità di dati. È quindi la qualità dei dati utilizzati in fase di programmazione, nonché dei dati di *input* in caso di adattabilità e apprendimento continuo della macchina, a incidere non solo sul livello di accuratezza dell'*output* (quindi di funzionalità ed efficienza del processo rispetto all'obiettivo) ma anche sul rischio di *bias* [7], di distorsioni, di discriminazione. Per comprendere meglio la discriminazione generata dall'algoritmo *machine learning*, si pensi al celebre caso *Amazon*, in cui l'algoritmo utilizzato per il *ranking* dei candidati a posizioni di sviluppatori di *software* era stato elaborato sulla base dei *curricula* ricevuti dall'azienda negli ultimi dieci anni, in modo che recepisse i parametri per individuare i soggetti "statisticamente migliori". Avendo registrato, per quella determinata posizione, una percentuale minima di donne, il sistema aveva "imparato" che per tale posizione sarebbe stato meglio scegliere un uomo [8], posizionando di conseguenza ai primi posti della classifica soltanto uomini.

Questo scenario ha allarmato l'Unione europea, rendendo necessaria la creazione di un nuovo quadro di tutele adeguato alle caratteristiche dei rapporti lavorativi nascenti dalle tecnologie digitali e in grado di tenere conto, in modo specifico, delle particolari caratteristiche di tali sistemi.

---

[6] Si pensi ad esempio alla previsione e applicazione di un regolamento aziendale che riduce l'ammontare del premio di produttività in proporzione alle assenze, senza distinguerle in base alle ragioni che le giustificano.

[7] Lo psicologo D. KAHNEMANN definisce i *bias* come "*errori sistematici, dei veri e propri preconcetti che ricorrono in maniera prevedibile in particolari circostanze*". Si tratta di distorsione cognitiva, un costrutto derivante da percezioni errate, automatismi mentali che generano credenze, che inducono a veloci valutazioni e decisioni, che, in ultima analisi, conducono a formare un pensiero che contiene pregiudizi e stereotipi.

[8] Parla al riguardo di "algoritmo «specchio»" A. LO FARO, *Algorithmic Decision Making e gestione dei rapporti di lavoro: cosa abbiamo imparato dalle piattaforme*, in *Federalismi.it*, 25/2022, pp. 189 ss.

© Wolters Kluwer Italia

2. La risposta dell'Unione europea alla discriminazione algoritmica

In tema di IA, il modello di azione euro-unitario promuove un approccio basato sul riconoscimento del rischio oggettivo e sulla necessità di individuare misure di garanzia imprescindibili, riconducibili alla prospettiva antropocentrica, alla trasparenza e alla supervisione umana. Tali scelte metodologiche e di contenuto, già più volte evidenziate in diversi atti di *soft law* dell'Unione europea [9], trovano oggi una specifica declinazione nel regolamento sull'intelligenza artificiale [10], c.d. *AI Act* [11], entrato in vigore il 2 agosto 2024.

L'*AI Act* è una normativa a carattere trasversale in materia di intelligenza artificiale che si applica a vari ambiti, tra cui quello bancario, sanitario e lavoristico.

In riferimento al settore lavoristico, il legislatore europeo mostra piena consapevolezza del potenziale impatto dell'intelligenza artificiale sul mondo del lavoro e, in particolare, delle possibili ripercussioni negative di tale impatto sui diritti fondamentali dei prestatori di lavoro. Tale consapevolezza emerge, in particolare, nel 36° "considerando", che definisce ad alto rischio i sistemi di IA utilizzati per l'assunzione e la selezione di persone, per la gestione dei lavoratori (con riferimento, ad esempio, a decisioni su promozioni e licenziamenti o in tema di assegnazione di compiti) e per l'accesso al lavoro autonomo, come pure per il monitoraggio o la valutazione di persone. Ed infatti tali sistemi possono avere un impatto negativo sui diritti dei prestatori di lavoro, sulla protezione dei dati e sulla *privacy*, perpetuando modelli storici

---

[9] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "*Creare fiducia nell'intelligenza artificiale antropocentrica*", Bruxelles, 8 aprile 2019, COM(2019)168 final, nella quale è stato definito indispensabile l'intervento e la sorveglianza umana sui processi algoritmici come paradigma di riferimento per garantire un clima di fiducia e sicurezza nei confronti dell'IA e prevederne i risultati imprevisti.

[10] 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), in G.U.U.E. L/2024/1689 del 12 luglio 2024, p. 1-144.

[11] A. Adinolfi, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno della loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in A. Pajno - F. Donati - A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol. I, *Diritti fondamentali, dati personali e regolazione*, Bologna, 2022, pp. 127 ss.

© Wolters Kluwer Italia

di discriminazione come quelli nei confronti delle donne, di determinate fasce d'età, di persone con disabilità o di determinate origini razziali, etniche o di orientamento sessuale. In linea generale, infatti, secondo le regole dettate dal nuovo regolamento, il fornitore di un sistema di IA è gravato, *in primis*, dall'obbligo di verificare se il sistema debba essere classificato come "ad alto rischio". Tale classificazione non deriva soltanto dall'inclusione del sistema all'interno di un determinato elenco di aree critiche e casi d'uso, ma anche da una valutazione effettuata dal fornitore circa la sussistenza di un effettivo rischio significativo di danno alla salute, alla sicurezza o ai diritti fondamentali (art. 6, par. 3) [12]. In caso di classificazione "ad alto rischio" del sistema [13], il fornitore sarà gravato, dunque, dall'obbligo di mappare e valutare i rischi e di predisporre un sistema di misure per la loro gestione (art. 9). Trattasi, in particolare, dei rischi noti e ragionevolmente prevedibili in condizioni di corretto utilizzo del sistema ovvero di quelli che potrebbero emergere in caso di un suo uso improprio ragionevolmente prevedibile. Rispetto alla qualità dei dati di addestramento, convalida e prova, al fornitore si richiede di adottare adeguate pratiche di *governance* e gestione, che comprendano, tra gli altri, un esame atto a valutare i possibili *bias* (molto rilevanti, come visto, nell'ottica antidiscriminatoria, soprattutto in caso di *machine learning*), nonché misure volte a localizzarli, prevenirli e mitigarli (art. 10). Si prevede segnatamente che tali pratiche riguardino "*un esame atto a valutare le possibili distorsioni suscettibili di incidere sulla salute e sulla sicurezza delle persone, di avere un impatto negativo sui diritti fondamentali o di comportare discriminazioni vietate dal diritto dell'Unione, specie laddove gli* output *di dati influenzano gli* input *per operazioni future*" (art. 10, par. 2, lett. f) e "*le misure adeguate per individuare, prevenire e attenuare le possibili distorsioni individuate*" (art. 10, par. 2, lett. g). Al riguardo, è interessante segnalare che l'art. 10, par. 5, dell'*AI Act*, autorizza "ecce-

[12] I sistemi utilizzati nel campo dell'occupazione, della gestione dei lavoratori e dell'accesso al lavoro autonomo (punto 4, Allegato III) sono inclusi nell'elenco delle aree critiche. Detti sistemi devono comunque essere sottoposti alla valutazione di rischio effettivo da parte del fornitore. Ai sensi del regolamento, tuttavia, un sistema di IA deve essere sempre considerato ad alto rischio laddove effettui una profilazione di persone fisiche (art. 6, par. 3) e questo è molto probabile che si verifichi in caso di utilizzo di processi automatizzati di monitoraggio o decisionali sul lavoro.

[13] Specifici obblighi di trasparenza, a carico del fornitore o del *deployer*, sono stabiliti – a prescindere dalla qualificazione ad alto rischio – per i sistemi destinati a interagire direttamente con persone fisiche e per quelli a carattere generativo, compresi i sistemi di IA per finalità generali (*General Purpose AI* – GPAI), a tutela di chi sia esposto ai c.d. *deep fakes* (Capo IV, art. 50).

© Wolters Kluwer Italia

zionalmente" (nonché a determinate condizioni) i fornitori a trattare categorie particolari di dati, tra quelli di cui all'art. 9 del regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (regolamento generale sulla protezione dei dati) (GDPR) [14], nella misura in cui sia strettamente necessario per garantire il rilevamento e la correzione delle distorsioni.

Dunque, tutti i *deployer* di sistemi ad alto rischio (qualificazione assunta da un datore di lavoro che faccia uso di sistemi di IA) sono chiamati a monitorare il funzionamento del sistema e a sospenderne l'utilizzo, con informazione al fornitore o distributore e all'organismo di vigilanza nazionale, laddove abbiano ragione di ritenere che l'uso, pur conforme alle istruzioni ricevute, possa determinare un rischio per la salute, la sicurezza e i diritti fondamentali (art. 26, par. 5).

Come spiega il 9° "considerando", il regolamento mira a rafforzare l'efficacia dei diritti e dei rimedi esistenti introducendo requisiti, vincoli e garanzie che possono svolgere un ruolo funzionale, facilitante e abilitante. Il regolamento presenta così una natura orizzontale [15] che, con riguardo alla protezione dei lavoratori, deve armonizzarsi anzitutto con le disposizioni del GDPR, con la legislazione in materia di salute e sicurezza e con il diritto antidiscriminatorio. L'art. 26, par. 9, specifica infatti che il *deployer* utilizza le informazioni ricevute dal fornitore per adempiere all'obbligo di valutazione d'impatto sulla protezione dei dati personali (DPIA), previsto dal GDPR. Sulla medesima linea di raccordo, l'art. 27, par. 4, stabilisce che se uno qualsiasi degli obblighi ivi previsti è già rispettato a seguito della DPIA, la valutazione d'impatto sui diritti fondamentali integra la valutazione condotta a norma del GDPR.

---

[14] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in G.U.U.E. L119 del 4 maggio 2016, p. 1-88.

[15] Nell'art. 26, par. 3, del regolamento è specificato l'obbligo di utilizzare il sistema in conformità alle istruzioni d'uso e alle misure di sorveglianza umana indicate dal fornitore non pregiudica gli obblighi che gravano sul *deployer* ai sensi di altre fonti dell'Unione o interne.

© Wolters Kluwer Italia

2.1. *Le garanzie antidiscriminatorie previste nella proposta di direttiva in materia di lavoro su piattaforma digitale*

L'11 marzo 2024, il Consiglio e il Parlamento europeo hanno trovato un accordo anche sulla proposta di direttiva in materia di lavoro su piattaforme digitali [16].

Tuttavia, poiché neanche dopo il suddetto accordo il complesso procedimento di approvazione può dirsi concluso – atteso che manca un testo ufficiale definitivo – allo stato è solo possibile una ricognizione dei principi e delle linee generali della futura direttiva europea.

La proposta si basa sull'art. 153, par. 1, lett. b), TFUE, che conferisce all'Unione il potere di sostenere e completare l'azione degli Stati membri con l'obiettivo di migliorare le condizioni di lavoro. In tale contesto, l'art. 153, par. 2, lett. b), TFUE, consente all'Unione di stabilire norme minime relative alle condizioni di lavoro delle persone che svolgono un lavoro mediante piattaforme digitali, nonché alla protezione dei lavoratori nel contesto della gestione algoritmica. La proposta di direttiva si basa anche sull'art. 16, par. 2, TFUE, che conferisce al Parlamento europeo e al Consiglio il potere di stabilire norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale. Dunque, detto articolo è qui utile in riferimento alla protezione dei dati personali – trattati mediante sistemi decisionali e di monitoraggio automatizzati – delle persone che svolgono un lavoro mediante piattaforme digitali.

Quanto alle misure antidiscriminatorie, la proposta di direttiva muove da tre principi: obbligo di trasparenza, monitoraggio dei dati, sorveglianza umana.

Esplicativo, con particolare riferimento alla trasparenza, è il 39° "considerando" della proposta di direttiva, che stabilisce, ai sensi dell'art. 88 GDPR, la previsione di "*norme più specifiche in relazione al regolamento (UE) 2016/679 per quanto riguarda l'uso e la trasparenza*

---

[16] Commissione europea, "*Proposta di direttiva del Parlamento europeo e del Consiglio relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali*", Bruxelles, 9 dicembre 2021, COM(2021)762 final. L'iniziativa della Commissione europea del 2021 nasce in un contesto nel quale esistevano già norme europee applicabili anche per la tutela dei lavoratori su piattaforma e quindi soggetti alla gestione del rapporto tramite algoritmo. Oltre al già citato regolamento (UE) 2016/679 sulla protezione dei dati, v. la direttiva (UE) 2019/1152 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa a condizioni di lavoro trasparenti e prevedibili nell'Unione europea, in G.U.U.E. L186 dell'11 luglio 2019, p. 105-121.

© Wolters Kluwer Italia

del processo decisionale automatizzato", nonché "*misure aggiuntive [...] per salvaguardare la protezione dei [...] dati personali, in particolare quando le decisioni sono adottate o sostenute dal trattamento automatizzato di dati personali*". In questo senso, infatti, l'art. 7 della direttiva prevede limitazioni del trattamento dei dati personali mediante sistemi decisionali o di monitoraggio automatizzati, in alcuni casi speculari alle proibizioni previste dall'*AI Act* nell'ambito della categoria dei sistemi ad alto rischio. Si pensi, in particolare, al divieto di trattare dati relativi allo stato emotivo o psicologico ovvero utili a desumere alcune caratteristiche "sensibili", tra cui l'origine razziale o etnica, lo *status* di migrante, le opinioni politiche, le convinzioni religiose. L'art. 5 dell'*AI Act* inserisce, infatti, tra le pratiche di IA vietate i sistemi di riconoscimento delle emozioni sul posto di lavoro, ad eccezione di quelli che riconoscono il dolore o la fatica per motivi medici o di sicurezza, ovvero i sistemi di categorizzazione biometrica delle persone volti a dedurre caratteristiche sensibili come la razza, le opinioni politiche, l'affiliazione sindacale, l'orientamento sessuale e il credo religioso.

Rispetto poi all'uso di sistemi di monitoraggio dei dati, l'art. 9 prevede specifici obblighi di trasparenza anche a tutela dei candidati in fase di *recruitment*: l'informativa include, tra l'altro, le categorie di dati e i parametri utilizzati dall'algoritmo nonché la spiegazione dei motivi alla base di alcune decisioni.

Si stabilisce, quale garanzia di sorveglianza umana aggiuntiva rispetto alla DPIA del GDPR (a sua volta opportunamente oggetto di una normativa di dettaglio a rafforzamento della tutela dei lavoratori, ai sensi dell'art. 8), una periodica valutazione dell'impatto, in particolare sulla parità di trattamento sul lavoro (art. 10, par. 1), delle decisioni individuali prese o (solo) sostenute dai sistemi automatizzati, specificando inoltre che "*qualora dalla sorveglianza o dalla valutazione [...] emerga un elevato rischio di discriminazione sul lavoro nell'uso di sistemi decisionali e di monitoraggio automatizzati [...], la piattaforma di lavoro digitale adotta le misure necessarie, compresa, se del caso, una modifica del sistema decisionale e di monitoraggio automatizzato o la cessazione del suo utilizzo, al fine di evitare tali decisioni in futuro*" (art. 10, par. 3).

3. Riflessioni finali

Oggi la tecnologia non è più soltanto uno strumento per realizzare quanto deciso dall'uomo, ma è diventata essa stessa fautrice di decisioni rilevanti dal punto di vista della dignità e dei diritti degli indivi-

© Wolters Kluwer Italia

dui [17]. Gli algoritmi impattano in vario modo sull'uguaglianza, sia promuovendola, sia causando o consolidando discriminazioni ed esclusioni, rispetto alle quali si rivela necessaria un'adeguata risposta giuridica. Ciò che non si può far a meno di sottolineare è che i sistemi di regolamentazione attuali, così come quelli che si prospettano nel futuro, presentano limiti intrinseci dovuti alla velocità e anche all'imprevedibilità degli sviluppi tecnologici, cosicché il diritto non sempre appare in grado di fornire una risposta pronta e congrua. In un quadro di questo tipo, dominato da complessità e incertezza, i diritti fondamentali degli individui sembrano correre un rischio costante.

Cionondimeno, l'analisi qui svolta, seppur breve, degli strumenti normativi dell'Unione europea dimostra lo sforzo notevole affrontato dalle sue istituzioni per realizzare un bilanciamento tra i benefici dell'innovazione tecnologica e la necessità di proteggere i diritti fondamentali e di prevenire le discriminazioni: tale sforzo pone l'Unione europea all'avanguardia nella regolamentazione etica dell'IA a livello globale. L'intelligenza artificiale, infatti, si ritiene debba essere "addestrata" in modo da prevenire la discriminazione e proteggere la diversità, nel rispetto dei valori fondanti l'Unione stessa. In sintesi, questi valori, che sono parte essenziale dell'identità europea, devono riflettersi anche nel modo in cui vengono utilizzati gli algoritmi e le innumerevoli applicazioni dell'IA.

[17] Sul sovvertimento della relazione tra "agente" e "strumento" che caratterizza il rapporto tra uomini e algoritmi v. A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Biolaw Journal*, 1/2019, pp. 67 ss.

© Wolters Kluwer Italia

LE TECNOLOGIE IMPIEGATE NEI CONTROLLI ALLE FRONTIERE ESTERNE DELL'UNIONE EUROPEA ED IL RELATIVO IMPATTO SULLA TUTELA DEI DIRITTI FONDAMENTALI *

EMILIO ADAMO

SOMMARIO: 1. Premessa. I principali sistemi di informazione su larga scala dell'UE. – 2. Impatto sulla tutela dei diritti fondamentali e interoperabilità dei sistemi. – 3. Recenti iniziative: *iBorderCtrl*. – 4. Considerazioni conclusive.

Abstract: EU policy on the management of external borders aims to "*carrying out checks on persons and efficient monitoring of the crossing of external borders*" and "*the gradual introduction of an integrated management system for external borders*" (Article 77, para. 1, points B and C, TFEU). In order to create an area of freedom, security and justice without internal frontiers, which should be offered to the citizens of the Union, Article 3, para. 2, TEU calls for "*appropriate measures with respect to external border controls*". An important, albeit instrumental, function in this field is provided by the EU large-scale databases, which are consulted both by national authorities and by Frontex when carrying out controls. The best known is the Schengen Information System (SIS). These systems have had the merit of modernising and making border controls more efficient. However, their use affects the fundamental rights of individuals concerned by such controls. The aim of this contribution is to examine these technological solutions and analyse their implications for the protection of individuals' fundamental rights. In this context, some recent initiatives will also be examined which, due to their potential invasiveness, risk opening up hitherto unexplored scenarios with repercussions in terms of

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

the protection of fundamental rights still to be evaluated. These include, in particular, the *iBorderCtrl* (*Intelligent Portable Border Control System*) research project. This project, developed with the aim of speeding up border crossing processes, uses technology based on emotions detection in order to assess the veracity of information provided by travellers. The use of systems based on such technologies opens up new scenarios in the field of border controls, with potential spill-over effects for safeguarding fundamental rights.

1. Premessa. I principali sistemi di informazione su larga scala dell'UE

Gli Accordi di Schengen hanno rappresentato un banco di prova per sperimentare, a livello internazionale, fra un gruppo ristretto di Stati, una cooperazione nelle materie della giustizia e degli affari interni che non era stato possibile avviare in ambito comunitario. L'abolizione dei controlli alle frontiere interne aveva come necessario presupposto il rafforzamento dei controlli alle frontiere esterne al fine di scongiurare rischi per la sicurezza. Tale esigenza ha stimolato, tra l'altro, la creazione di strumenti deputati alla raccolta e allo scambio di informazioni per finalità di controllo delle frontiere esterne, di gestione dei flussi migratori nonché di esame delle domande di protezione internazionale [1]. Tali tecnologie costituiscono un panorama vasto in continua evoluzione nell'ambito del quale assumono un ruolo preponderante i sistemi di informazione su larga scala definiti anche come banche dati o *database* centralizzati.

Il Sistema d'Informazione Schengen (c.d. SIS) ha rappresentato e tuttora rappresenta il sistema di condivisione delle informazioni più esteso e più impiegato per la sicurezza e la gestione delle frontiere in Europa. Il SIS costituisce l'unico sistema informativo su larga scala a svolgere questa funzione ibrida, da un lato, securitaria, e, dall'altro,

[1] Comunicazione della Commissione al Consiglio e al Parlamento europeo, "*Il programma dell'Aia: dieci priorità per i prossimi cinque anni. Partenariato per rinnovare l'Europa nel campo della libertà, sicurezza e giustizia*", Bruxelles, 10 maggio 2005, COM(2005)184 final; Consiglio europeo, "*Programma di Stoccolma-Un'Europa aperta e sicura al servizio e a tutela dei cittadini*", in G.U.U.E. C115 del 4 maggio 2010, p. 1-38.

© Wolters Kluwer Italia

di gestione delle frontiere. Si tratta di un sistema cosiddetto *hit/no hit* tale da consentire di verificare se le informazioni concernenti una persona od un oggetto siano presenti nella banca-dati ed in tal caso di inviare una segnalazione alle autorità competenti. Il sistema prevede specifiche categorie di segnalazioni sia per persone che per oggetti. Tra queste, ai fini del presente contributo, assumono particolare rilevanza le segnalazioni per rifiuto di ingresso e di soggiorno riguardanti i cittadini di Stati terzi. Scopo del SIS è quello di preservare l'ordine e la sicurezza pubblica, compresa la sicurezza dello Stato, all'interno dello spazio Schengen nonché di favorire la circolazione delle persone attraverso lo scambio di informazioni. In vista dell'allargamento dell'Unione del 2004, il sistema è stato ulteriormente sviluppato giungendo ad una seconda generazione (SIS II)[2]. Soltanto nell'aprile del 2013, dopo anni di dibattiti, ritardi e costi esorbitanti dovuti alle difficoltà tecniche di sviluppo, il SIS II divenne operativo[3]. La principale novità fu rappresentata dall'introduzione dei dati biometrici. Successivamente, nel 2018, attraverso tre regolamenti, vennero apportate ulteriori innovazioni, tra le quali, l'inclusione, tra i dati conservabili, delle immagini facciali e dei profili DNA, rendendo il SIS sempre più un sistema biometrico. Il SIS si avvale di un sistema automatico per il riconoscimento delle impronte digitali c.d. AFIS (*Automated Fingerprint Identification System*). Inoltre, il nuovo regolamento "SIS frontiere", oltre ad aver specificato le categorie di dati da segnalare, ha disciplinato le condizioni per l'inserimento ed il trattamento delle segnalazioni riguardanti cittadini di Stati terzi. Per queste ultime è stato esteso l'accesso anche a Frontex ed Europol[4]. A livello strutturale, il SIS è composto da un sistema centrale (SIS centrale) con funzioni di supporto tecnico ed amministrativo, un sistema nazionale (N.SIS.II), in ciascuno Stato membro dello Spazio Schengen, ed un'infrastruttura di comunicazione.

---

[2] Decisione 2007/533/GAI del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II), in G.U.U.E. L205 del 7 agosto 2007, p. 63-84.

[3] J. Parkin, *The Difficult Road to the Schengen Information System II: The legacy of "laboratories" and the cost for fundamental rights and the rule of law*, 1 April 2011, disponibile su: *www.semanticscholar.org*.

[4] Regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006, in G.U.U.E. L312 del 7 dicembre 2018, p. 14-55, artt. 35 e 36; E. Brouwer, *Large-scale databases and interoperability in migration and border policies: The Non-Discriminatory Approach of Data Protection*, in *European Public Law*, 1/2020, pp. 71-92.

© Wolters Kluwer Italia

Il sistema europeo comune di asilo (CEAS) prevede una disciplina specifica per l'individuazione dello Stato competente a decidere sulla domanda di protezione internazionale. In tale ambito, il sistema EURODAC (*European dactylographic system*) ha svolto e continua a svolgere un ruolo fondamentale. EURODAC è un *database* biometrico che supporta il funzionamento del sistema Dublino. In particolare, concorre alla determinazione dello Stato competente per l'esame di una domanda di asilo così contrastando il fenomeno del c.d. *asylum shopping* [5]. Si tratta di un sistema informatizzato e centralizzato che consente la comparazione delle impronte dei richiedenti asilo e di coloro che attraversano irregolarmente le frontiere europee. Ai richiedenti protezione internazionale in uno Stato membro (anche alla frontiera), di età non inferiore ai 14 anni, nonché a coloro che sono fermati in relazione all'attraversamento irregolare di una frontiera esterna, vengono rilevate le impronte digitali. Ogni Stato membro, attraverso il *focal point* nazionale, trasmette i dati al Sistema centrale. Il confronto tra le impronte digitali raccolte con i dati presenti in EURODAC, attraverso il sistema AFIS, consente allo Stato membro di accertare se i richiedenti protezione internazionale o i cittadini di Stati terzi irregolarmente presenti sul territorio dell'Unione abbiano già presentato una domanda di protezione internazionale in altro Stato membro o se l'ingresso sia avvenuto irregolarmente. Al sistema possono accedere le autorità nazionali designate ed Europol. Nel 2013, dopo un percorso travagliato, EURODAC è stato riformato. In particolare, si è assistito ad un significativo allargamento delle finalità per cui i dati venivano raccolti e trattati fino a ricomprendervi la lotta al terrorismo e la repressione di gravi reati. Più di recente, tra i diversi strumenti che compongono il nuovo Patto sulla migrazione e l'asilo è stato inserito il regolamento 2024/1358 (regolamento EURODAC) [6]. Esso amplia ulteriormente le

[5] Regolamento (CE) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'"Eurodac" per il confronto delle impronte digitali per l'efficace applicazione della convenzione di Dublino, in G.U.C.E. L316 del 15 dicembre 2000, p. 1-10.

[6] Regolamento (UE) 2024/1358 del Parlamento europeo e del Consiglio, del 14 maggio 2024, che istituisce l'"Eurodac" per il confronto dei dati biometrici ai fini dell'applicazione efficace dei regolamenti (UE) 2024/1351 e (UE) 2024/1350 del Parlamento europeo e del Consiglio e della direttiva 2001/55/CE del Consiglio e ai fini dell'identificazione dei cittadini di paesi terzi e apolidi il cui soggiorno è irregolare, e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, che modifica i regolamenti (UE) 2018/1240 e (UE) 2019/818 del Parlamento europeo e del Consiglio e che abroga il regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio, in G.U.U.E. L/2024/1358 del 22 maggio 2024, p. 1-69.

© Wolters Kluwer Italia

finalità del sistema prevedendo, tra l'altro, il supporto generale al sistema di asilo nonché l'assistenza nell'applicazione del regolamento in materia di reinsediamento e ammissioni umanitarie. Inoltre, tra i dati trattabili vengono previste anche nuove categorie di dati biometrici oltre alle impronte digitali, in particolare i dati relativi all'immagine del volto. Da segnalare, infine, l'abbassamento del limite di età per la raccolta delle impronte da 14 a 6 anni.

Da ultimo, occorre menzionare il sistema informativo VIS (*Visa Information System*). All'indomani degli attentati dell'11 settembre 2001 la politica comune europea in materia di visti subì una decisa accelerazione. Venne così istituito, nel 2004, un sistema per lo scambio di informazioni sui visti per soggiorni di breve durata, i cui scopi e funzionalità vennero poi definiti con successivo regolamento del 2008 [7]. Tuttavia, il sistema divenne operativo soltanto nel 2011. Il VIS si prefigge l'obiettivo di migliorare l'attuazione della politica comune in materia di visti, la cooperazione consolare e la consultazione tra le autorità centrali competenti per i visti, facilitando lo scambio di dati tra Stati membri. Tale sistema ha consentito di accelerare l'esame delle domande di visto, di contrastare le relative frodi e di prevenire il *visa shopping*. Inoltre, ha consentito di agevolare i controlli alle frontiere esterne, di favorire l'applicazione del regolamento Dublino nonché di prevenire le minacce per la sicurezza interna degli Stati membri. Il VIS raccoglie le domande di visto presentate dai cittadini provenienti dagli Stati terzi elencati dal regolamento 2018/1806 [8]. Inoltre, si compone di un sistema informatico centrale e di un'infrastruttura di comunicazione che collega il sistema centrale con i sistemi nazionali. I dati trattati attraverso il VIS ricomprendono, tra gli altri, le fotografie e le impronte digitali. Le scansioni delle dita non sono richieste per i minori di 12 anni e per coloro i quali è fisicamente impossibile rilevarle. Oltre alle autorità competenti per i visti possono accedere al sistema le

[7] Decisione 2004/512/CE del Consiglio, dell'8 giugno 2004, che istituisce il sistema di informazione visti (VIS), in G.U.U.E. L213 del 15 giugno 2004, p. 5-7; regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (regolamento VIS), in G.U.U.E. L218 del 13 agosto 2008, p. 60-81.

[8] Regolamento (UE) 2018/1806 del Parlamento europeo e del Consiglio, del 14 novembre 2018, che adotta l'elenco dei paesi terzi i cui cittadini devono essere in possesso del visto all'atto dell'attraversamento delle frontiere esterne e l'elenco dei paesi terzi i cui cittadini sono esenti da tale obbligo (codificazione), in G.U.U.E. L303 del 28 novembre 2018, p. 39-58.

© Wolters Kluwer Italia

autorità nazionali competenti in materia di asilo e immigrazione e le autorità deputate ai controlli di frontiera. In specifici casi, anche le autorità nazionali di polizia ed Europol possono consultare il VIS per finalità di prevenzione e lotta al terrorismo ed altri gravi reati. Più di recente, il VIS è andato incontro a diverse modifiche per esigenze connesse alla sicurezza, alla migrazione nonché nell'ottica di rendere maggiormente interoperabili i vari sistemi informativi.

2. Impatto sulla tutela dei diritti fondamentali e interoperabilità dei sistemi

I sistemi sopra esaminati costituiscono uno strumento fondamentale al fine di realizzare una gestione effettivamente integrata delle frontiere esterne. Tuttavia, la raccolta e l'archiviazione di dati personali, inclusi i dati biometrici, in sistemi informativi su larga scala, rischia di configurare un'interferenza con l'esercizio di alcuni diritti fondamentali. In particolare, ciò riguarda i diritti al rispetto della vita privata e alla protezione dei dati personali, come tutelati dall'art. 8 CEDU e dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Come precisato dalla Corte di giustizia dell'Unione europea, tali diritti non costituiscono prerogative assolute ma devono essere considerati in relazione alla loro funzione nella società [9]. Con specifico riferimento all'impatto che le banche dati centralizzate hanno sui diritti fondamentali, sia la Corte di giustizia che la Corte europea dei diritti dell'uomo hanno, in più occasioni, individuato una serie di criteri interpretativi. Come affermato dalla Corte europea dei diritti dell'uomo, la semplice conservazione dei dati riguardanti la vita privata di una persona costituisce già di per sé un'ingerenza ai sensi dell'art. 8 CEDU, indipendentemente dal fatto che le informazioni conservate siano poi effettivamente utilizzate o meno [10]. La Corte di giustizia, chiamata a pronunciarsi sulla validità del regolamento n. 2252/2004, aveva ritenuto legittimi gli scopi volti all'inclusione di dati biometrici nel passaporto. In tale ipotesi, non venne ravvisato il rischio di una loro eventuale conservazione in modo centralizzato e di un loro impiego per fini diversi da quelli previsti dal regolamento [11]. Mentre, con la sentenza

[9] C. giust. UE, 17 ottobre 2013, C-291/12, *Schwarz*, punti 33-34.

[10] C. eur. dir. uomo, 26 marzo 1987, ricorso n. 9248/81, *Leander* c. *Svezia*, punto 48; C. eur. dir. uomo, 16 febbraio 2000, ricorso n. 27798/95, *Amann* c. *Svizzera*, punto 69.

[11] Regolamento (CE) n. 2252/2004 del Consiglio, del 13 dicembre 2004, relativo

© Wolters Kluwer Italia

Digital Rights Ireland, la Corte era giunta a conclusioni del tutto opposte. Nello specifico, venne considerato incompatibile con il diritto dell'Unione la direttiva *data retention* che attuava una sorveglianza di massa realizzando un'ingerenza nei diritti fondamentali della quasi totalità della popolazione europea [12]. Ed ancora, nel caso *S. e Marper* c. *Regno Unito* la Corte europea dei diritti dell'uomo aveva segnalato i rischi di stigmatizzazione connessi alla conservazione, all'interno di banche dati centralizzate, di dati personali di individui non riconosciuti colpevoli di nessun reato e trattati alla stregua di condannati [13].

A seguito degli attentati di Parigi del 2015 e di Bruxelles del 2016, si avvertì l'esigenza di intensificare la condivisione delle informazioni pertinenti, tra l'altro, attraverso l'interoperabilità delle banche dati. La scelta di rendere interoperabili i sistemi di informazione dell'UE relativi alla sicurezza, alle frontiere e alla gestione della migrazione derivava dalla presa d'atto della necessità di potenziare la cooperazione in tali settori. Nell'ambito dei controlli di frontiera (così come in quelli di polizia) la presenza di numerosi sistemi informativi imponeva di consultare un gran numero di banche dati con il rischio di avere informazioni non aggiornate e duplicazione dei dati. Vennero così adottati i regolamenti gemelli sull'interoperabilità 2019/817 e 2019/818 [14]. La struttura delineata dai regolamenti ha dato vita ad un *network* attraverso il quale diverse autorità sono in grado di verificare se le informazioni relative a un particolare soggetto siano disponibili nei vari *database*. I regolamenti sull'interoperabilità si prefiggono l'ambizioso obiettivo di centralizzare i dati archiviati nei principali sistemi informativi. Così facendo si vuole migliorare, tra l'altro, l'efficacia e l'efficienza delle

---

alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri, in G.U.U.E. L385 del 29 dicembre 2004, p. 1-6; C. giust. UE, *Schwarz*, cit.

[12] C. giust. UE, 8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland Ltd*, punto 56.

[13] C. eur. dir. uomo, 4 dicembre 2008, ricorsi nn. 30562/04 e 30566/04, *S. e Marper* c. *Regno Unito*.

[14] Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, in G.U.U.E. L135 del 22 maggio 2019, p. 27-84; regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816, in G.U.U.E. L135 del 22 maggio 2019, p. 85-135.

© Wolters Kluwer Italia

verifiche alle frontiere esterne e contrastare l'immigrazione illegale Ma anche assicurare un elevato livello di sicurezza nello spazio di libertà, sicurezza e giustizia, migliorare l'attuazione della politica comune in materia di visti e supportare l'esame delle domande di protezione internazionale [15]. I regolamenti realizzano un ambiente integrato tra i sistemi, contribuendo alla "*completa tracciabilità della mobilità umana in transito verso le frontiere europee*" [16].

Tuttavia, le criticità connesse all'utilizzo di *database* centralizzati rischiano di amplificarsi. L'interoperabilità consente di aumentare sia il numero degli Stati membri che i *database* centralizzati coinvolti nella raccolta e nel trattamento dei dati, così determinando la condivisione di una vasta quantità di informazioni. Da un lato, la stessa valutazione d'impatto, a corredo delle due proposte di regolamento, assicurava che le innovazioni proposte non avrebbero intaccato l'equilibrio già garantito da ciascuno dei sistemi esistenti. Ma dall'altro, riconosceva un possibile impatto indiretto sui diritti fondamentali [17]. Inoltre, l'interoperabilità pone il problema di un utilizzo dei dati per scopi diversi da quelli che originariamente ne avevano giustificato la raccolta. In particolare, l'operatore sarebbe in grado di consultare tutti i sistemi resi interoperabili attraverso il CIR (l'archivio comune di dati d'identità). Questa ricerca generalizzata per scopi di identificazione potrebbe infatti comportare, come evidenziato sia dal Garante europeo della protezione dei dati (EDPS) che dall'Agenzia dell'Unione europea per i diritti fondamentali (FRA), un impatto sproporzionato, sebbene indiretto, sulla protezione dei dati e sui diritti fondamentali [18]. Da questo punto di vista, l'interoperabilità rischia di porsi in contrasto con uno dei prin-

---

[15] *Id.,* art. 2, par. 1.

[16] D. VITIELLO, *Le frontiere esterne dell'Unione europea*, Bari, 2020, p. 79.

[17] Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE (frontiere e visti) e che modifica la decisione 2004/512/CE del Consiglio, il regolamento (CE) n. 767/2008, la decisione 2008/633/GAI del Consiglio, il regolamento (UE) 2016/399 e il regolamento (UE) 2017/2226, Bruxelles, 12 dicembre 2017, COM(2017)793 final; proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE (cooperazione giudiziaria e di polizia, asilo e migrazione), Bruxelles, 12 dicembre 2017, COM(2017)794 final.

[18] P. HANKE - D. VITIELLO, *High-Tech Migration Control in the EU and Beyond: The Legal Challenges of "Enhanced Interoperability"*, in E. CARPANELLI - N. LAZZERINI (eds.)*, Use and Misuse of New Technologies. Contemporary Challenges in International and European Law*, Cham, 2019, p. 24; EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), *Opinion 4/2018, 16 April 2018*, disponibile su: *www.edps.europa.eu*; EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), *Opinion 1/2018, 19 April 2018*, disponibile su: *www.fra.europa.eu*.

© Wolters Kluwer Italia

cipi fondamentali della tutela dei dati personali, ossia quello della limitazione delle finalità di raccolta [19]. Ed anche i principi di correttezza e trasparenza rischiano di essere compromessi. In particolare, da un meccanismo che amplia il novero delle autorità in grado di accedere ai sistemi, consentendo l'utilizzo dei dati per finalità ulteriori e con modalità diverse rispetto a quelle originarie. Per quanto riguarda il principio di trasparenza, si pongono degli interrogativi in merito alle modalità di funzionamento del modulo MID (*Multiple-Identity Detector*). Tale componente prevede processi automatizzati ma senza specificazione delle modalità di supervisione umana come, invece, imporrebbe il regolamento 2016/679 sulla protezione dei dati (GDPR) in materia di processi decisionali automatizzati relativi a persone fisiche [20]. Sotto altro profilo, occorre evidenziare come l'impianto normativo delineato dai due regolamenti si applichi ai principali sistemi informativi solo con riferimento ai cittadini di Stati terzi. Tale scelta, come spiegato dalla Commissione, dovrebbe accrescere la fiducia dell'opinione pubblica garantendo, maggior sicurezza ai cittadini dell'UE [21]. Tuttavia, nonostante i regolamenti sull'interoperabilità prevedano delle salvaguardie al riguardo, tali accorgimenti non fugano del tutto i dubbi derivanti da un sistema che introduce un trattamento differenziato tra cittadini europei e cittadini di Stati terzi prevedendo per questi ultimi ulteriori controlli di sicurezza [22]. Tale rischio sarebbe accentuato dalla previsione contenuta nell'art. 20 del regolamento 2019/818 in base alla quale le autorità di polizia possono interrogare il CIR anche se l'interessato non è in grado o rifiuta di cooperare [23].

---

[19] G. Caggiano, *L'interoperabilità fra le banche-dati dell'Unione sui cittadini degli Stati terzi*, in *Dir. immigr. citt.*, 1/2020, pp. 170-184.

[20] C. Blasi Casagran, *Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU*, in *Human Rights Law Review*, 2/2021, pp. 433-457.

[21] COM(2017)793 final; COM(2017)794 final.

[22] Meijers Committee, *Comments on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) 12 December 2017, COM(2017)794*, 19 February 2018, disponibile su: *https://www.commissie-meijers.nl*.

[23] E. Brouwer, *Interoperability of Databases and Interstate Trust: a Perilous Combination for Fundamental Rights*, 25 May 2019, disponibile su: *www.verfassungsblog.de*.

© Wolters Kluwer Italia

3. Recenti iniziative: *iBorderCtrl*

Il ricorso a nuove soluzioni tecnologiche ha rivoluzionato le metodologie attraverso le quali venivano tradizionalmente svolti i controlli di frontiera. Ciò ha condotto ad una nuova concezione o, per meglio dire, ad una digitalizzazione della politica migratoria europea [24]. In realtà, in tale ambito, l'impiego dell'intelligenza artificiale avveniva già da tempo. Basti pensare ai sistemi automatizzati di identificazione delle impronte digitali (come il sistema AFIS). Maggiori perplessità sono invece legate all'utilizzo delle c.d. *emotion detection technologies*. Per tali tecnologie al momento non vi è ancora un impiego ai controlli di frontiera ma l'Unione ha iniziato a muovere i primi passi finanziando dei progetti di ricerca. Al riguardo, recente attenzione ha suscitato lo strumento denominato *iBorderCtrl* (*Intelligent Portable Border Control System*), finanziato nell'ambito dell'iniziativa *EU's Horizon 2020*. Scopo principale del progetto, avviato nel 2016 e completato nel 2019, è quello di contribuire allo sviluppo di tecnologie che possano accelerare i processi di attraversamento delle frontiere con particolare riguardo ai c.d. *bona fide travellers*, migliorando nel contempo la sicurezza e l'affidabilità dei controlli. Si tratta di uno strumento che combina in un unico sistema diverse tecnologie [25]. La procedura prevede una fase di pre-registrazione con il coinvolgimento diretto dei viaggiatori chiamati a fornire una serie di informazioni. La componente più discussa è rappresentata dall'*Automatic Deception Detection System* (ADDS). Attraverso tale sistema, sulla base dell'intervista di pre-registrazione, vengono elaborate una serie di domande che verranno poste ai viaggiatori da un *avatar* personalizzato. L'ADDS calcola la probabilità di inganno nelle interviste analizzando le microespressioni non verbali degli intervistati [26]. L'iniziativa ha sollevato un certo scetticismo. In generale, diversi dubbi sono emersi in merito all'affidabilità scientifica della tecnologia basata sul rilevamento delle emozioni. Infatti,

---

[24] P. BONDITTI, *From Territorial Spaces to Networks: A Foucauldian Approach to the Implementation of Biometry*, in *Alternatives: Global, Local, Political*, 29/2004, pp. 465-482; European Commission, *Opportunities and challenges for the use of artificial intelligence in border control, migration and security*, Vol. I, *Main Report*, 2020, disponibile su: *www.op.europa.eu*.

[25] Periodic Reporting for period 2-iBorderCtrl (*Intelligent Portable Border Control System*), 2021, disponibile su: *https://cordis.europa.eu*.

[26] iBorderCtrl (*Intelligent Portable Border Control System*)-Technical Framework, disponibile su: *https://perma.cc/9MKY-GAFC*.

© Wolters Kluwer Italia

secondo alcuni autori, è da ritenersi altamente improbabile che tale tecnologia possa funzionare nella pratica [27].

Per quanto riguarda il potenziale impatto sui diritti fondamentali, va osservato come il rilevamento delle emozioni rappresenti in sostanza uno dei potenziali impieghi della tecnologia basata sul riconoscimento facciale [28]. Pertanto, i criteri giurisprudenziali elaborati in materia sono estensibili anche alle tecnologie basate sul rilevamento delle emozioni.

In primo luogo, il riconoscimento facciale ha ricadute evidenti sia sul diritto al rispetto della vita privata che su quello alla protezione dei dati personali. Al riguardo, sia la Corte di giustizia dell'Unione europea che la Corte europea dei diritti dell'uomo hanno sottolineato come le immagini del volto costituiscano dati personali e, più nello specifico, uno dei principali caratteri distintivi della personalità. La Corte europea dei diritti dell'uomo ha chiarito che il monitoraggio di una persona in un'area pubblica tramite videoripresa non costituisce di per sé una forma di interferenza. Tuttavia, nel caso in cui le immagini vengano registrate, in particolare se la registrazione ha carattere sistematico o permanente, in tal caso possono configurarsi problemi di interferenza con i diritti riconosciuti dall'art. 8 CEDU [29]. Inoltre, il trattamento dei dati personali nell'ambito di procedure amministrative che prevedono l'utilizzo di tecnologie di riconoscimento facciale configura un'interferenza con i diritti di cui all'art. 8, par. 1, CEDU [30].

Sotto altro profilo, il riconoscimento facciale rischia di porsi in contrasto con il principio di non discriminazione. In particolare, il rischio di discriminazione riguarderebbe il funzionamento degli algoritmi. Già nella fase in cui gli algoritmi vengono elaborati o testati si potrebbero configurare degli errori o *bias* da cui potrebbero derivare dei

---

[27] J. Sánchez Monedero - L. Dencik, *The politics of deceptive borders*, in *Information, Communication & Society*, 3/2020, pp. 413-430; Homo Digitalis' input to the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, Athens, 13 May 2020, disponibile su: *www.ohchr.org*.

[28] Il riconoscimento facciale può essere definito come il "*trattamento automatico di immagini digitali che contengono i volti di persone ai fini di identificazione, autenticazione/verifica o categorizzazione di tali persone*", Gruppo di lavoro Articolo 29 per la protezione dei dati, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobili*, 22 marzo 2012, p. 2.

[29] C. giust. UE, *Schwarz*, cit., punti 22, 48-49; C. eur. dir. uomo, 4 luglio 2023, ricorso n. 11519/20, *Glukhin* c. *Russia*, punto 66; European Court of Human Rights, *Guide on Article 8 of the European Convention on Human - Rights Right to respect for private and family life, home and correspondence*, 31 August 2019, par. 138.

[30] C. eur. dir. uomo, *Glukhin* c. *Russia*, cit., punto 73.

© Wolters Kluwer Italia

trattamenti discriminatori in fase attuativa. Inoltre, differenti livelli di *performance* con riferimento a determinate caratteristiche protette potrebbero dar luogo a discriminazioni indirette a seconda del genere e del sesso della persona rappresentata [31]. Le stesse problematiche potrebbero configurarsi anche per coloro che sono affetti da una qualche disabilità del volto o nel caso dei minori e degli anziani, per i quali il trascorrere del tempo potrebbe inficiare l'accuratezza dell'analisi [32].

Da ultimo, va segnalato come le tecnologie basate sul riconoscimento facciale possano determinare un effetto dissuasivo o scoraggiante (il c.d. *chilling effect*). Gli individui, sapendo di poter essere sottoposti a sorveglianza, si astengono dall'esercitare diritti e libertà fondamentali [33]. Tale effetto può influenzare il modo attraverso il quale si sviluppa l'identità della persona e si evolve la società democratica [34].

4. Considerazioni conclusive

L'impiego di nuove tecnologie digitali e dell'intelligenza artificiale ha assunto una sempre maggiore rilevanza nella gestione della migrazione e per garantire la sicurezza nell'area Schengen. Tuttavia, permangono delle criticità per la tutela dei diritti fondamentali. Per quanto riguarda i sistemi informativi su larga scala, la loro iniziale frammentazione aveva in qualche modo fornito maggiori garanzie per i diritti fondamentali. Mentre il percorso verso l'interoperabilità si prospetta segnato da rischi per la tutela di tali diritti in particolare per quelli dei cittadini di Stati terzi. Inoltre, l'interoperabilità realizza un ulteriore stratificazione normativa che rischia di rendere maggiormente complessa la cornice legale in cui questi sistemi operano. Come giustamente rilevato, l'interoperabilità apre nuovi scenari inducendo una rimodulazione dei principi giuridici della materia determinando, in questo senso, "*un punto di non ritorno*" [35]. Allo stesso modo l'impiego delle

---

[31] D. MURRAY, *Facial recognition and the end of human rights as we know them?*, in *Netherlands Quarterly of Human Rights*, 2/2024, pp. 145-152; A. BRIHANE, *The unseen black faces of algorithms*, in *Nature*, 610/2022, pp. 451-452; J. BUOLAMWINI - T. GEBRU, *Gender shades: Intersectional accuracy disparities in commercial gender classification*, 81/2018, pp. 77-91, disponibile su*: www.proceedings.mlr.press*.

[32] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019, pp. 28-29, disponibile su: *www.fra.europa.eu*.

[33] C. eur. dir. uomo, *Glukhin* c. *Russia*, cit., punto 88.

[34] D. MURRAY, *Op. cit.*, p. 147.

[35] Sintesi del parere del Garante europeo della protezione dei dati sulle proposte

© Wolters Kluwer Italia

tecnologie basate sul riconoscimento delle emozioni pone seri interrogativi. Il nuovo *AI Act*, recentemente adottato, contiene espliciti riferimenti ai sistemi di riconoscimento delle emozioni definiti come quei sistemi di intelligenza artificiale "*finalizzati a identificare o inferire emozioni o intenzioni di persone fisiche, sulla base dei loro dati biometrici*" [36]. Salvo specifiche ipotesi, l'*AI Act* qualifica tali sistemi come ad alto rischio [37]. Inoltre, per gli stessi è previsto un divieto di immissione sul mercato e messa in servizio nell'ambito dei luoghi di lavoro e degli istituti di istruzione. Mentre il divieto non riguarderebbe le immissioni sul mercato per motivi medici o di sicurezza [38]. La *ratio* di tale previsione risiederebbe nello squilibrio di potere che caratterizza tali contesti.

Il nuovo regolamento sull'intelligenza artificiale ha sicuramente il merito di aver fornito una prima cornice normativa in materia, prevedendo una disciplina in grado di orientare gli sviluppatori e gli operatori del settore. Tuttavia, con riferimento alle tecnologie di rilevamento delle emozioni sussistono delle perplessità che il legislatore europeo non nasconde di condividere. Al riguardo, viene esplicitamente segnalato come permangano serie preoccupazioni con riferimento alla base scientifica dei sistemi in esame. Il modo di esprimere le emozioni, infatti, può essere influenzato da vari fattori (ad esempio, culturali o situazionali) e produrre effetti discriminatori. Inoltre, il legislatore europeo riconosce come tali tecnologie siano caratterizzate da limitata affidabilità, mancanza di specificità e limitata generalizzabilità. Pertanto, ne viene ammesso il potenziale impatto discriminatorio e lesivo dei diritti e delle libertà degli individui [39]. Inoltre, la deroga prevista per l'utilizzo di tali tecnologie nel campo della sicurezza sembra stridere con la logica che ne esclude l'impiego nei luoghi di lavoro ed in quelli di istruzione. A ben vedere, infatti, anche il settore della sicurezza può essere caratterizzato da situazioni di squilibrio di potere, così come quello dei controlli di frontiera e, a maggior ragione, quando la pubbli-

---

di due regolamenti che istituiscono un quadro per l'interoperabilità tra i sistemi di informazione su larga scala dell'UE (2018/C 233/07).

[36] 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), in G.U.U.E. L/2024/1689 del 12 luglio 2024, p. 1-144, 18° "considerando" e art. 3, par. 1, n. 39.

[37] *Id*., art. 6 e Allegato III.

[38] *Id*., art. 5, lett. f).

[39] *Id*., 44° "considerando".

© Wolters Kluwer Italia

ca autorità si imbatte in cittadini di Stati terzi in condizioni di vulnerabilità. Per quanto riguarda, più nello specifico, l'impiego di tali tecnologie nell'ambito dei controlli di frontiera, le preoccupazioni sopra menzionate pongono ulteriori spunti di riflessione. Innanzitutto, il processo politico che conduce al finanziamento ed all'implementazione di tali iniziative dovrebbe essere improntato ad un'ampia trasparenza ed accessibilità. Tali tecnologie rappresentano una novità, per cui si rende opportuno un ampio coinvolgimento dell'opinione pubblica, degli *stakeholders* e degli esperti dei vari settori interessati, garantendo pur sempre un adeguato bilanciamento dei vari interessi in gioco [40]. In secondo luogo, l'utilizzo di nuove tecnologie impone di valutare attentamente quali possano essere le conseguenze sui diritti e le libertà fondamentali. Pertanto, ogni iniziativa andrebbe preceduta da adeguate analisi di impatto nonché dal monitoraggio da parte di autorità indipendenti già nella fase di progettazione. La fiducia nei confronti del mezzo tecnologico, come strumento volto ad efficientare la gestione integrata delle frontiere esterne, non deve tradursi in un affidamento ingiustificato che dia per scontate le implicazioni sul piano etico e dei diritti umani [41].

[40] C. giust. UE, 17 ottobre 2013, C-135/22P, *Breyer* c. *Agenzia esecutiva europea per la ricerca (REA)*.

[41] E. GUILD - S. CARRERA - A. EGGENSCHWILER, *Informing the Borders Debate*, 18 May 2009, pp.1-4, disponibile su: *https://aei.pitt.edu*.

© Wolters Kluwer Italia

PRINCIPIO DI PRECAUZIONE E INTELLIGENZA ARTIFICIALE *

Domenico Andrea Pisani

Sommario: 1. L'ambito di applicazione del principio di precauzione. – 2. Il rango del principio e la riforma costituzionale del 2022. – 3. Precauzione e intelligenza artificiale.

Abstract: The precautionary principle, developed in the environmental field, has progressively risen to the rank of general principle with respect to situations characterised by scientific uncertainty as well as technological progress. From this transversal perspective, the precautionary principle has been referred to in multiple European soft law instruments relating to the robotics and artificial intelligence sector. As regards artificial intelligence, the adoption of precautionary measures should prevent the risk that the decisions made by a machine learning system, disadvantaging particular categories of subjects, may be discriminatory. This paper aims to study the scope of application of the principle regarding artificial intelligence, with particular reference to the distinction between general precaution and the principle of precaution in an "environmental" version.

1. L'ambito di applicazione del principio di precauzione

Il recente sviluppo di tecnologie basate sull'intelligenza artificiale e, soprattutto, dei sistemi di apprendimento automatico (*machine learning*) ha spinto la dottrina a chiedersi se anche in tale ambito sia applicabile il principio di precauzione [1], un principio di azione destinato a

* Contributo sottoposto a doppio referaggio in forma anonima.

[1] Il tema è stato affrontato da P. Zuddas, *Pregiudizi digitali e principio di precau-*

© Wolters Kluwer Italia

essere impiegato nel momento in cui deve essere assunta una decisione in un contesto connotato da incertezza scientifica. Questa caratteristica lo distingue dal principio di prevenzione, destinato invece a operare in contesti di certezza scientifica [2]. Il fine dell'approccio precauzionale è quello di evitare o mitigare i potenziali danni prodotti, a titolo esemplificativo, dal singolo prodotto, sostanza, procedimento, piano o azione.

Il tema si pone rispetto al rischio che le decisioni formulate da un sistema di intelligenza artificiale (IA), nella specie di apprendimento automatico, sfavorendo particolari categorie di soggetti, risultino discriminatorie, nonché in relazione allo sviluppo di un sistema di intelligenza artificiale. L'applicabilità del principio sembra infatti avvalorata dalla recente comparsa di molteplici richiami ad esso all'interno dei principali documenti dell'Unione europea relativi alle nuove tecnologie [3].

---

zione, in *Consulta online*, 2/2020, pp. 408 ss., per il quale "*[u]no dei rischi più rilevanti, legati al ricorso crescente all'intelligenza artificiale per assumere decisioni*" è rappresentato dalla possibilità che i *software* impiegati "*formulino previsioni errate che penalizzino sistematicamente specifiche categorie di soggetti, generando decisioni discriminatorie*". Secondo l'Autore, il principio di precauzione è applicabile nel settore dell'intelligenza artificiale in quanto "*la nascita all'interno del diritto internazionale ne marca una vocazione «globale», utile per la regolamentazione soprattutto dei sistemi di apprendimento automatico che si alimentano dei* Big data *acquisiti dalla rete* Internet*, mentre la sua qualificazione come principio generale lo rende pienamente applicabile anche al di fuori degli ambiti nei quali è espressamente richiamato*". Sul tema v. anche E. CIBELLA, *Il principio di precauzione nell'ambiente digitale*, in *PA Persona e Amministrazione*, 1/2023, pp. 511 ss.

[2] Osserva F. DE LEONARDIS, *Il principio di precauzione nell'amministrazione del rischio*, Milano, 2005, p. 127, che "*[i]l principio di precauzione esprime qualcosa di assolutamente diverso, di innovativo e di originale rispetto ad altri principi di azione, come quello di proporzionalità e di prevenzione, dal momento che le decisioni assunte in ossequio a questi ultimi si muovevano ancora in un contesto tradizionale di tendenziale certezza e di potere amministrativo delimitato (almeno) all'esterno dalla legge. Il principio precauzionale richiama, invece, direttamente la fragilità della certezza tecnica e, per questo, la sua portata sistematica appare assai più rilevante di quanto esprimano sinora le controversie che ne hanno fatto applicazione*".

[3] V. la risoluzione del Parlamento europeo del 16 febbraio 2017, *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, all'interno della quale il principio di precauzione è citato due volte, rispetto all'immissione sul mercato di sistemi di intelligenza artificiale e di robot (par. 7), e rispetto all'individuazione delle aree in cui testare i robot (par. 23); la risoluzione del Parlamento europeo del 12 febbraio 2019, *Una politica industriale europea globale in materia di robotica e intelligenza artificiale*, per la quale "*la ricerca sull'IA e altre attività correlate dovrebbero essere condotte nel rispetto del principio di precauzione e tutti i soggetti coinvolti nello sviluppo, nell'attuazione, nella diffusione e nell'utilizzo dell'AI dovrebbero [...] anticipare le potenziali conseguenze sulla sicurezza e prendere le dovute precauzioni, in proporzione al livello di protezione, compresa la tempestiva divulgazione di fattori che potrebbero mettere a rischio i cittadini e l'ambiente*" (par. 19). Il principio di pre-

© Wolters Kluwer Italia

In questo contributo si tenterà, dunque, di affrontare la questione relativa messa in atto del principio precauzionale nello sviluppo e nella gestione dei sistemi di IA cercandone di definire più precisamente la portata e il rango.

Una prima problematica riguarda le materie in cui il principio può trovare applicazione. Infatti, per una parte dei commentatori, il principio di precauzione esplicherebbe la sua forza solo nei settori dell'ambiente e della salute [4], essendo stato inizialmente enunciato nei termini in cui oggi è noto all'interno di normative (internazionali o comunitarie, come ad esempio l'art. 174 TCE, oggi art. 191 TFUE) rivolte alla loro protezione, mentre secondo una diversa opinione [5], il principio di precauzione avrebbe travalicato i confini della materia ambientale finendo per assumere un ambito di applicazione più ampio, come principio generale dell'ordinamento [6].

---

cauzione, tuttavia, non viene menzionato espressamente nel regolamento (UE) 2024/1689, del 13 giugno 2024, in materia di regole armonizzate sull'intelligenza artificiale, contenente in ogni caso numerose norme ispirate a una logica precauzionale *in senso lato*, tra le quali si possono citare, a titolo esemplificativo, gli artt. 9 sul "*sistema di gestione dei rischi*" in relazione ai sistemi di IA ad alto rischio; 14 sulla "*sorveglianza umana*"; 27 sulla "*valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio*"; e 60 riguardante le "*prove di sistemi di IA ad alto rischio in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA*". In merito v. C. Casonato, *L'intelligenza artificiale e il diritto pubblico comparato ed europeo*, in *Dir. pubbl. comp. eur. online*, 1/2022, pp. 169 ss.

[4] Così P. Sands - J. Peel, *Principles of International Enviromental Law*, IV ed., Cambridge, 2018, pp. 230 ss., secondo i quali "the precautionary principle aims to provide guidance in the development and application of international environmental law where there is scientific uncertainty". Nello stesso senso v. A. Trouwborst, *Evolution and Status of the Precautionary Principle in International Law*, The Hague, 2002, pp. 303 ss. Se la correlazione tra precauzione e ambiente appare ancora stretta nell'ambito del diritto internazionale, così non si può dire per quanto riguarda l'ordinamento eurounitario e quello interno, dove la concezione trasversale del principio la fa da padrone. In tal senso si esprime anche A. Gragnani, *Il principio di precauzione come modello di tutela dell'ambiente, dell'uomo, delle generazioni future*, in *Riv. dir. civ.*, 1/2003, pp. 35 ss.

[5] Il principio di precauzione è ricostruito dalla dottrina maggioritaria quale principio trasversale e generale, che ha travalicato i confini della materia ambientale. In tale senso, E. Del Prato, *Il principio di precauzione nel diritto privato: spunti*, in *Liber amicorum per Francesco D. Busnelli. Il diritto civile tra principi e regole*, Milano, 2008, p. 547, per il quale "*la precauzione è un atteggiamento necessario in qualsiasi attività amministrativa a prescindere dalla sua formulazione in qualche norma: quella dettata a livello comunitario, in tema di ambiente, non è che una sua esplicazione*".

[6] Per tutte v. Trib. CE, 26 novembre 2002, T-74/00, T-76/00, T-83/00, T-85/00, T-132/00, T-137/00 e T-141/00, *Artedogan GmbH e altri* c. *Commissione*, par. 183-184, per il quale "*[n]onostante sia menzionato nel trattato solamente in relazione alla politica ambientale, il principio di precauzione ha un ambito di applicazione più ampio. Esso è destinato ad applicarsi, al fine di assicurare un livello elevato di protezione*

© Wolters Kluwer Italia

In questo contributo si tenterà di sostenere una prospettiva intermedia, distinguendo tra precauzione in *senso lato*, che non rappresenterebbe altro che un momento applicativo del più generale principio di ragionevolezza, e precauzione in *senso stretto*, che riguarda la protezione dei beni giuridici ambiente e salute. Tale impostazione sembra avvalorata dalla lettera della norma più importante per rango relativa al principio operante nel nostro ordinamento, ossia l'art. 191 TFUE.

In ogni caso la precauzione in *senso stretto* è ricompresa nell'ambito della precauzione in *senso lato*.

Infatti, in generale e in *senso lato*, l'idea di precauzione connessa ai sistemi di IA può giustificare l'adozione di misure limitative dello sviluppo tecnologico e allo stesso tempo di provvedimenti autorizzatori in merito a campi di ricerca connotati da alto rischio con la conseguenza che le misure precauzionali adottate in senso ampliativo o ristrettivo finiscono per essere connotate da un elevato tasso di discrezionalità, sindacabile tramite un giudizio di ragionevolezza.

Nell'ambito della precauzione in *senso stretto*, oltre a ciò, assume un grande rilievo l'aspetto cautelare, volto a impedire possibili compromissioni dei beni ambiente e salute, bilanciato da un obbligo di procedimentalizzazione dell'assunzione della conoscenza scientifica. La precauzione in *senso stretto*, tuttavia, non si limita a questo, ma riveste una rilevanza fondamentale all'interno del processo di riconversione ecologica delle economie umane, in quanto, sul lungo periodo, riguarda il corretto uso delle risorse naturali in rapporto ai bisogni delle popolazioni umane, legandosi strettamente al tema delle generazioni future.

In un'ottica di bilanciamento di diritti costituzionali potenzialmente confliggenti, solo la precauzione in *senso stretto* giustificherebbe l'adozione di misure limitative di altri diritti costituzionalmente tutelati in un contesto di incertezza scientifica e prevalentemente in relazione a una potenziale lesione dei beni ambiente e salute. La precauzione in *senso stretto* può quindi essere considerata come una versione potenziata della precauzione in *senso lato*.

Da questo punto di vista, la precauzione in *senso lato* non sembra trovare copertura costituzionale se non come momento applicativo del principio di ragionevolezza, riguardando per lo più l'incertezza scien-

---

della salute, della sicurezza dei consumatori e dell'ambiente, in tutti gli ambiti di azioni della Comunità [...]. Infatti, essendo le istituzioni comunitarie responsabili, in tutti i loro ambiti di azione, della tutela della salute, della sicurezza e dell'ambiente, il principio di precauzione può essere considerato come un principio autonomo, che discende dalle menzionate disposizioni del Trattato".

© Wolters Kluwer Italia

tifica in merito ai presupposti fattuali delle possibili limitazioni di diritti costituzionali.

Come noto, la dottrina tradizionale riteneva che il principio di ragionevolezza derivasse dal principio di uguaglianza *ex* art. 3 Cost. Infatti, per questa impostazione, dal principio di uguaglianza deriva il principio per cui devono essere trattate in modo uguale situazioni uguali e in modo diseguale situazioni diseguali, interpretazione che la Corte costituzionale. sembra tutt'ora far propria in alcune delle sue più recenti decisioni [7]. La ragionevolezza, in questa prospettiva, rappresenta il principale criterio di raffronto tra le disuguaglianze insite nelle disparità o uniformità delle normative.

Tuttavia, secondo una diversa e sempre più diffusa corrente di pensiero il principio di ragionevolezza si sarebbe emancipato dal principio di uguaglianza guadagnando ormai "*una propria autonomia rispetto al testo della Costituzione*" ed essendo utilizzato "*come complemento e in appoggio a qualunque altro principio costituzionale richiamato a parametro del giudizio della Corte (costituzionale)*" [8].

La ragionevolezza rappresenterebbe dunque un canone di giudizio funzionale al bilanciamento dei diversi interessi coinvolti, che non limita la sua operatività al giudizio di uguaglianza, ma permea nelle fondamenta il ragionamento giuridico.

Bisogna ora occuparsi del rango del principio di precauzione, inteso in *senso stretto*, con un particolare sguardo sulla revisione costituzionale del 2022.

2. Il rango del principio e la riforma costituzionale del 2022

Il principio di precauzione inizia ad entrare nel nostro ordinamento tramite la ratifica di molteplici strumenti internazionali in materia di protezione dell'ambiente, per poi assumere maggiore cogenza tramite

[7] V., ad esempio, la motivazione della sent. della Corte cost. del 22 aprile 2024, n. 67.

[8] Così M. Cartabia, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, relazione svolta nel corso dell'Incontro trilaterale tra la Corte costituzionale italiana, la Corte costituzionale spagnola e il Tribunale costituzionale portoghese tenutosi a Roma, presso la Corte costituzionale, il 25 ottobre 2013, p. 1. Sulla portata costituzionale del principio cfr. almeno G. Scaccia, *Gli strumenti della ragionevolezza nel giudizio costituzionale*, Milano, 2000, e A. Morrone, *Il custode della ragionevolezza*, Milano, 2001.

© Wolters Kluwer Italia

l'inserimento di un'apposita previsione all'interno dell'art. 174 TCE (oggi art. 191 TFUE).

Un percorso parallelo e successivo di riforma ha interessato il testo costituzionale, con specifico riferimento all'interesse ambientale. Nel testo originario della Costituzione non appariva alcuna norma relativa all'ambiente, ma successivamente giurisprudenza [9] e dottrina [10] riconobbero la presenza di un principio costituzionale di tutela dell'ambiente, come principio implicito insito nel sistema costituzionale. In seguito, la revisione costituzionale del Titolo V ha per la prima volta inserito l'espressione "*tutela dell'ambiente, dell'ecosistema*" nell'art. 117 Cost., come materia di competenza esclusiva dello Stato ai sensi del co. 2, lett. s).

La l. cost. 11 febbraio 2022, n. 1, rappresenta il coronamento [11] di questo processo di emersione dell'interesse ambientale e ha interessato gli artt. 9 e 41 Cost. In particolare, la legge di revisione costituzionale ha aggiunto un terzo comma all'art. 9 Cost., secondo il quale "*la Repubblica [...] tutela l'ambiente, la biodiversità e gli ecosistemi, anche nell'interesse delle future generazioni. La legge dello Stato disciplina i modi e le forme di tutela degli animali*" e ha modificato i co. 2 e 3 dell'art. 41 Cost., introducendo la tutela dell'ambiente e della salute tra i limiti espliciti al godimento della libertà di iniziativa economica privata (limiti elencati nel co. 2 dell'art. 41) e menzionato i "*fini ambientali*" tra gli obiettivi di un intervento di indirizzo e coordinamento dell'attività economica pubblica e privata accanto a quelli sociali (co. 3 dell'art. 41).

Se per una parte della dottrina [12] la riforma rappresenterebbe una

---

[9] V. Corte cost., sent. 20 maggio 1987, n. 210, che definisce la salvaguardia dell'ambiente "*come diritto fondamentale della persona ed interesse fondamentale della collettività*". V. anche Corte cost., sent. 13 gennaio 1987, n. 641, secondo la quale "*[l]'ambiente è protetto come elemento determinativo della qualità della vita. La sua protezione [...] è imposta anzitutto da precetti costituzionali (artt. 9 e 32 Cost.), per cui esso assurge a valore primario ed assoluto*".

[10] V. M.S. GIANNINI, "*Ambiente*"*, saggio sui suoi aspetti giuridici*, in *Riv. trim. dir. pubbl*., 1973, pp. 15 ss.; A. PREDIERI, *Paesaggio (ad vocem*), in *Enc. dir.,* vol. XXXI, Milano, 1981, pp. 503 ss.; B. CARAVITA, *Costituzione, principi costituzionali e tecniche di normazione per la tutela dell'ambiente*, in S. GRASSI - M. CECCHETTI - A. ANDRONIO (a cura di), *Ambiente e diritto*, Firenze, 1999, pp. 175 ss.

[11] In questo senso si esprime anche la Corte cost., nella sent. 13 giugno 2024, n. 105, p.t. 5.1.2 dei "considerando" in diritto.

[12] Sul punto v. V. ONIDA, *Ambiente in Costituzione*, in *Corti supreme e salute*, 1/2022, pp. 359-360. Nello stesso senso R. MONTALDO, *La tutela costituzionale dell'ambiente nella modifica degli artt. 9 e 41 Cost.: una riforma opportuna e necessaria?*, in *Federalismi.it*, 13/2022, p. 452.

© Wolters Kluwer Italia

mera ricognizione di quanto già affermato dalla giurisprudenza costituzionale, secondo una differente posizione [13] la revisione avrebbe comportato la costituzionalizzazione del principio della tutela dell'ambiente e dello sviluppo sostenibile (testimoniato dal riferimento alle "*generazioni future*" e dai nuovi limiti alla libertà d'iniziativa economica).

Ora, partendo dal presupposto che la riforma abbia effettivamente esplicitato il valore costituzionale del principio dello sviluppo sostenibile, si può ritenere che ciò sia avvenuto anche riguardo al principio di precauzione in *senso stretto*, quale suo corollario.

Il principio di precauzione in *senso stretto*, infatti, si è sviluppato in un contesto normativo, quello del diritto ambientale, ricco di principi generali, quali quello dello sviluppo sostenibile e della prevenzione.

Il rapporto con il principio dello sviluppo sostenibile potrebbe, infatti, essere ricostruito come di genere a specie. Il principio precauzionale nella sua veste ambientale sembra costituire uno dei corollari del principio dello sviluppo sostenibile [14].

L'opportunità di dare rilevanza alla dimensione intergenerazionale del principio precauzionale è stata, inoltre, sottolineata da attenta dottrina [15].

Se quindi il principio di precauzione in *senso lato* si rivolge a una situazione di incertezza destinata a protrarsi nel breve o nel medio periodo, invece il principio di precauzione di matrice ambientale, in *senso stretto*, sembra destinato a operare anche sul lungo periodo, manifestando le sue massime potenzialità in ordine alla pianificazione economica finalizzata a fini ambientali prevista dalla recente revisione all'art. 41, co. 3.

Così ricostruito, il principio di precauzione *in senso stretto* appare

---

[13] In tal senso R. Bifulco, *Primissime riflessioni intorno alla l. cost. 1/2022 in materia di tutela dell'ambiente*, in *Federalismi.it*, 11/2022, p. 4, e M. Cecchetti, *La revisione degli articoli 9 e 41 della Costituzione e il valore costituzionale dell'ambiente: tra rischi scongiurati, qualche virtuosità (anche) innovativa e molte lacune*, in *Forum di Quaderni Costituzionali*, 3/2021, pp. 297 ss.; così anche F. Fracchia, *L'ambiente nell'art. 9 della Costituzione: un approccio in "negativo"*, in *Dir. Econ.*, 1/2022, p. 18.

[14] In tal senso M.A. Gliatta, *Ambiente e Costituzione: diritti distributivi e riconfigurazione della responsabilità intergenerazionale*, in *Costituzionalismo.it*, 2/2021, pp. 103 ss., la quale osserva che "*l'evoluzione giurisprudenziale dei concetti di «sviluppo sostenibile» e di «precauzione» [...] origina da quelle disposizioni che più strettamente intrecciano un rapporto fra Costituzione e futuro, ovvero quelle sulla scienza e sulla ricerca scientifica (art. 9, primo comma e art. 33 primo comma)*".

[15] Così M. Cecchetti, *Diritto ambientale e conoscenze scientifiche tra valutazione del rischio e principio di precauzione*, in *Federalismi.it*, 13/2023, pp. 48 ss.

© Wolters Kluwer Italia

idoneo a giustificare l'adozione di misure necessarie e urgenti (rafforzando i presupposti fattuali per l'adozione di un d.l. *ex* art. 77 Cost., ad esempio) e allo stesso tempo a incidere profondamente sulla programmazione economica volta alla transizione ecologica.

Grazie a questa lettura della precauzione si potrebbe concretizzare un ampliamento del sindacato del giudice costituzionale sulle leggi tributarie e di bilancio, in quanto l'azione dell'esecutivo e del legislatore in questo settore potrebbe essere ulteriormente limitata dai vincoli derivanti dalla transizione ecologica e dagli interessi delle generazioni future ad essa sottesa.

In quest'ottica, il principio, oltre a fornire una guida per il legislatore nel delineare normative con un adeguato livello di protezione e a porsi come criterio fondamentale nella programmazione economica "verde", assume anche una funzione di criterio guida nell'eventualità che si presenti un'esigenza di bilanciamento tra i beni salute/ambiente e altri beni costituzionalmente garantiti, nella specie la libertà d'iniziativa economica.

Ne conseguirebbe infine che, sul piano costituzionale, risulterebbe più agevole adottare misure anticipatorie e afflittive per altri diritti quando viene in gioco la tutela di beni giuridici afferenti alle sfere della salute e dell'ambiente.

3. Precauzione e intelligenza artificiale

In conclusione, sembra opportuno chiedersi quale applicazione possa trovare il principio di precauzione *in senso stretto* nel campo dell'intelligenza artificiale. Se i riferimenti all'approccio precauzionale presenti nel regolamento europeo 2024/1689 [16] possono essere considerati come un'espressione della precauzione in *senso lato*, prevedendo misure ragionevolmente volte a mitigare od evitare qualsiasi tipo di danno derivante dall'IA, il principio in *senso stretto* troverebbe invece applicazione solo nel caso in cui sia necessario proteggere i beni ambiente/salute, od orientare lo sviluppo di queste tecnologie a favore della transizione ecologica.

Da ciò deriverebbe la legittimità di misure anticipatorie fondate sulla precauzione in *senso stretto*, volte ad esempio a limitare lo sviluppo di sistemi di IA dannosi per ambiente e salute. Le stesse misure, adottate in attuazione del principio in *senso lato*, a protezione di beni

[16] V. nota 3.

© Wolters Kluwer Italia

ulteriori, dovrebbero invece essere giustificate con il più generale principio di ragionevolezza, di cui il principio precauzionale in *senso lato* rappresenterebbe un corollario.

Si possono, in ogni caso, immaginare molteplici spazi applicativi per il principio in *senso stretto* nel settore dell'IA: il profilo della lesione del bene ambiente si pone, principalmente, in relazione alla questione del consumo di energia elettrica da parte dei sistemi di intelligenza artificiale [17]. Vi è poi il tema del potenziale danno per la salute che potrebbe ipoteticamente derivare da un utilizzo eccessivo della tecnologia da parte del consumatore, sfociante in una nuova forma di manipolazione digitale delle masse [18], ma si potrebbe far riferimento anche alla possibile implementazione di armi letali dotate di tecnologia IA [19].

Si pone, inoltre, anche il rischio di discriminazione derivante dalla disomogeneità dei dati su cui l'IA si forma [20]. Ma il principio opera anche in positivo, vincolando il legislatore a favorire uno sviluppo dell'IA nel settore, ad esempio, della ricerca medica, o nel favorire l'efficienza del sistema sanitario tramite l'implementazione di procedure amministrative semplificate tramite l'accorto utilizzo di questi sistemi.

Si può, infine, auspicare che grazie a una lettura intergenerazionale alla precauzione in *senso stretto* lo sviluppo delle tecnologie di IA possa procedere in armonia con la transizione ecologica e supportarla, anche con riferimento alle nuove possibilità offerte da questa tecnologia per la personalizzazione delle cure, l'efficienza della programmazione, la gestione delle risorse e la loro allocazione.

---

[17] Sul punto v. A. De Vries, *The growing energy footprint of artificial intelligence*, in *Joule*, 10/2023, pp. 2191 ss., e J. Li - S. Ma - Y. Qu - J. Wang, *The impact of artificial intelligence on firm's energy and resource efficiency: Empirical evidence from China*, in *Resources Policy*, 5 April 2023.

[18] In relazione ai potenziali danni dell'IA per la salute v. F. Federspiel - R. Mitchell - A. Asokan, *Threats by artificial intelligence to human health and human existence*, in *BMJ Global Health*, 9 May 2023, p. 2.

[19] *Id.*, pp. 3 ss.

[20] Così P. Zuddas, *Intelligenza artificiale e discriminazione*, in *Liber amicorum per Pasquale Costanzo-Diritto costituzionale in trasformazione,* vol. I, *Costituzionalismo, Reti e Intelligenza artificiale*, *Consulta Online*, Genova, 2020, p. 461. Nello stesso senso D. Morana - T. Balduzzi - F. Morganti, *La salute "intelligente": eHealth, consenso informato e principio di non-discriminazione*, in *Federalismi.it*, 34/2022, pp. 145 ss. Sulle possibili applicazioni dell'IA in medicina, v. anche B. Kham - H. Fatima, *Drawbacks of Artificial Intelligenze and Their Potential Solutions in the Healthcare Sector*, in *Biomedical Material Devices*, vol. II, t. II, 8 February 2023.

© Wolters Kluwer Italia

LA PRESUNZIONE DI SUBORDINAZIONE NEL LAVORO TRAMITE PIATTAFORME DIGITALI *

GABRIELLA CATALDI

SOMMARIO: 1. Premessa: l'evoluzione dello stato delle fattispecie legali di lavoro. – 2. Gli orientamenti giurisprudenziali sulla qualificazione del rapporto di lavoro svolto tramite piattaforma digitale. – 3. La presunzione di subordinazione nella proposta di direttiva UE. – 4. Conclusioni e prospettive future.

Abstract: The contribution aims to examine the regulation of work performed through digital platforms. The former has been the subject of careful reflection by national and European legislators in recent years, in light of the implications of the digital transition and its impact both in the industrial and economic world and on the entire structure of human and labour relations. In particular, in the national context, work through digital platforms has been the focus of a wide and rich legal literature, both in terms of the qualification of the employment relationship and from the point of view of the protections applicable to digital workers. On the European side, on the other hand, one cannot ignore a careful reflection on the Proposal for an European Directive on the "improvement of working conditions in work through digital platforms" in the recent text subject to the agreement between the European Parliament and the Council reached on 8 March 2024, aimed to countering distortions in the digital market through the prescription of rules common to the national legal systems of European countries, and with the aim of protecting the social rights of digital workers and promoting the sustainable growth of platforms in the European Union. More specifically, emphasis will be placed on the technique of the "presumption of subordination", the gravitational center of

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

the Proposal, which raises several perplexities with regard to the opportunity of its use in our system for establishing the subordinate or self-employed nature of the employment relationship, also in view of the aporia represented by the presumption of subordination without the euro-union notion of subordination itself.

1. Premessa: l'evoluzione dello stato delle fattispecie legali di lavoro

Il fenomeno della digitalizzazione nel mondo del lavoro ha avuto, tra gli altri effetti, quello di minare le tradizionali categorie dei rapporti di lavoro, mettendo in crisi l'alternativa "*secca*" tra i due poli della subordinazione e della autonomia [1], così come individuata dal Codice civile del 1942 [2].

Al riguardo, degne di attenzione negli ultimi anni sono state le fattispecie del lavoro svolto tramite piattaforme digitali, intese come quelle infrastrutture tecnologiche che abilitano interazioni per svolgere attività economiche ed estrarre dati [3] e che si inseriscono nell'ambito dell'"economia delle piattaforme" [4].

Quest'ultima si configura come un arcipelago molto complesso ed eterogeneo, in cui rientrano diverse fattispecie di lavoro in rete, tra cui la vicenda dei *riders* che, benché nota, rappresenta solo la punta dell'*iceberg*.

Parallelamente all'emersione di nuove fattispecie di lavoro, si è registrato negli ultimi anni uno sviluppo incontrollato di forme di collaborazioni coordinate e continuative, a cui il legislatore ha cercato di

---

[1] Criticata a causa della successiva evoluzione dei modi di produrre e di lavorare, tra gli altri, da R. DE LUCA TAMAJO - R. FLAMMIA - M. PERSIANI, *La crisi della subordinazione e della sua idoneità selettiva nei trattamenti garantistici. Prime proposte per un nuovo approccio sistematico in una prospettiva di valorizzazione del* tertium genus*: il lavoro coordinato*, in *Quad. dir. lav. rel. ind.*, 21/1998, p. 331.

[2] Mentre non prevedeva una specifica considerazione e disciplina per il lavoro autonomo continuativo. Cfr. G. SANTORO PASSARELLI, *Il lavoro parasubordinato*, Milano, 1979.

[3] R. SCIOTTI, *Tecnologia digitale e rapporto di lavoro*, in *Riv. infort.*, 2/2018, p. 167.

[4] B. MARTENS, *An Economic Policy Perspective on Online Platforms*, in *JRC Technical Reports*, *Institute for Prospective Technological Studies Digital Economy Working Paper*, 5/2016.

© Wolters Kluwer Italia

porre un freno, in quanto strumenti troppo spesso usati per celare rapporti di lavoro subordinato.

Ciò è avvenuto, dapprima, con il tipo contrattuale del "*lavoro a progetto*", sottoposto a rigorosi vincoli formali e sostanziali, progressivamente rafforzati, e poi con la disciplina delle "*collaborazioni organizzate*" (e la correlata modifica dell'art. 409, n. 3, c.p.c., disposta dall'art. 15 della l. 22 maggio 2017, n. 81 [5]).

In entrambi i casi, l'ordinamento giuslavoristico ha cercato di presidiare quell'area grigia tra subordinazione e autonomia, al fine di evitare comportamenti elusivi e favorire l'applicazione delle tutele del lavoro subordinato.

Tuttavia, la tecnica normativa utilizzata ha comportato un effetto paradossale, poiché l'obiettivo di contenere la fuga dal lavoro subordinato e la diffusione dei rapporti nell'area grigia tra lavoro e subordinazione è stato realizzato mediante la moltiplicazione delle fattispecie rilevanti in quell'area grigia.

Cosicché, alla semplificazione "*geometrica*" dello schema binario adottato dal Codice del 1942 si è contrapposto un sovraffollamento di fattispecie giuridicamente rilevanti, tale da determinare un "*matassa*" assai difficile da districare.

In particolare, a seguito del d. lgs. 15 giugno 2015, n. 81 – e delle modifiche ad esso apportate con il d.l. 3 settembre 2019, n. 101 – tra i due poli del lavoro subordinato e del contratto d'opera regolato dagli artt. 2222 ss., si collocano ora una serie di fattispecie "*intermedie*", le quali danno rilievo, ciascuna, a diversi elementi compatibili con i due poli originari: dalle collaborazioni organizzate di cui al comma 1 dell'art. 2 del d. lgs. n. 81/2015 [6], a quelle di cui al comma 2 dello stesso articolo; dal lavoro di consegna dei *riders* svolto "*attraverso piattaforme anche digitali*" di cui agli artt. 47-*bis* ss. del d. lgs. n. 81/2015, alle collaborazioni coordinate e continuative [7].

---

[5] Sono le collaborazioni che si concretizzano in prestazioni d'opera prevalentemente personale, oltre che coordinate e continuative. La collaborazione "*si intende coordinata quando, nel rispetto delle modalità di coordinamento stabilite di comune accordo, il collaboratore organizza autonomamente l'attività lavorativa*".

[6] La disciplina del lavoro subordinato qui si applica ai "*rapporti di collaborazione che si concretano in prestazioni di lavoro prevalentemente personali, continuative e le cui modalità di esecuzione della prestazione siano organizzate dal committente. Le disposizioni di cui al presente comma si applicano anche qualora le modalità di esecuzione della prestazione siano organizzate mediante piattaforme digitali*".

[7] Da considerare, inoltre, anche il "*lavoro autonomo continuativo*" (art. 3, comma 1, e art. 14, comma 1, della l. n. 81/2017).

© Wolters Kluwer Italia

Tutto ciò solleva due ordini di problemi.

Il primo è, inevitabilmente, quello della moltiplicazione dei dubbi e delle incertezze legati ai procedimenti di qualificazione, a causa del fatto che, in relazione a ciascuna fattispecie si confrontano diverse teorie interpretative, derivandone il rischio di vere e proprie aporie.

Emblematici, al riguardo, sono proprio i più recenti interventi sollecitati dalla vicenda dei *riders*, nell'ambito dei quali il legislatore, per individuare il campo di applicazione dei "*livelli minimi di tutela per i lavoratori autonomi che – attraverso piattaforme anche digitali – svolgono attività di consegna di beni per conto altrui in ambito urbano*" [8], ha previsto che devono considerarsi "*piattaforme digitali*" quei programmi e quelle procedure informatiche utilizzati dal committente che "*sono strumentali alle attività di consegna di beni, fissandone il compenso e determinando le modalità di esecuzione della prestazione*".

Tale disposizione, invero, se da un lato conferma che la determinazione da parte del committente delle modalità di esecuzione della prestazione è compatibile con il lavoro autonomo, rende ardua, dall'altro lato, l'individuazione dell'elemento discretivo rispetto alla disciplina delle collaborazioni organizzate [9].

Il secondo ordine di problemi è sostanziale, e cioè ammesso che il problema qualificatorio possa essere risolto, è il caso di verificare se la moltiplicazione delle fattispecie legali, così come realizzata, sia idonea a fungere da razionale strumento di distribuzione delle tutele.

Al riguardo, il nostro legislatore si è mostrato diffidente rispetto all'adozione di nuove categorie di classificazione del lavoro, continuando a privilegiare il ricorso a fattispecie che attribuiscono rilievo esclusivamente alla qualificazione del vincolo giuridico tra le parti e delle modalità di esecuzione della prestazione.

Inoltre, la scelta relativa all'estensione tendenzialmente integrale delle tutele del lavoro subordinato sembra non tenere conto che quella scelta, oltre a scoraggiare e sanzionare il lavoro autonomo fittizio, colpisce anche il vero lavoro autonomo, e che quest'ultimo, quando è

---

[8] E "*con l'ausilio di velocipedi o veicoli a motore di cui all'art. 47, comma 2, lett. a), del codice della strada, di cui al decreto legislativo 30 aprile 1992, n. 289*" (art. 47-*bis*, comma 1, del Capo V-*bis* del d. lgs. n. 81/2015).

[9] Le tutele di cui agli artt. 47-*bis* ss. "*non presuppongono la continuità del rapporto di lavoro, a differenza di quanto accade nell'ipotesi prevista dall'art. 2, comma 1, che contempla espressamente i rapporti continuativi*". Cfr. G. SANTORO PASSARELLI, *Sui lavoratori che operano mediante piattaforme anche digitali, sui riders e il ragionevole equilibrio della Cassazione 1663/2000*, in *Lav. dir. eur.*, 1/2020, pp. 2-13.

© Wolters Kluwer Italia

svolto personalmente, in modo continuativo e coordinato, presenta sì elementi in comune con il lavoro subordinato, ma per definizione è diverso da esso.

Cosicché, al posto di una equiparazione di tutele, sarebbe più ragionevole, e coerente con i richiamati principi costituzionali, operare in una prospettiva di applicazione gradualistica e selettiva [10].

Ciò *a fortiori* ove si consideri che l'altra modifica al primo periodo del comma 1 dell'art. 2, rappresentata dall'eliminazione del riferimento nelle "*collaborazioni organizzate*" alla esclusiva personalità della prestazione ed alla organizzazione dei "*tempi*" e del "*luogo*" di lavoro, ha comportato il venire meno di due condizioni che invece sarebbero state coerenti con un disegno di assimilazione di trattamento con la posizione del lavoratore subordinato [11].

2. Gli orientamenti giurisprudenziali sulla qualificazione del rapporto di lavoro svolto tramite piattaforma digitale

Sulla scorta delle opinioni espresse in dottrina, sul piano della qualificazione dei rapporti di lavoro svolto su piattaforma, la giurisprudenza ha in un primo tempo optato per l'accertamento della natura autonoma [12], sulla base della possibilità per i *riders* di scegliere se e quando lavorare.

In una successiva pronuncia della Corte d'Appello di Torino del 4 febbraio 2019, n. 4, è stata invece accertata la natura etero-organizzata della prestazione, ravvisando nella fattispecie del lavoro svolto dai *riders* un "*tertium genus*" tra lavoro subordinato e collaborazioni coordinate e continuative.

Sennonché, è intervenuta l'unica (sinora) sentenza di Cassazione in argomento [13] che, confermando la suddetta sentenza di appello di Torino, ha ricollegato questi rapporti di lavoro alle fattispecie delle collaborazioni organizzate dal committente ai sensi dell'art. 2 del d. lgs. n. 81/2015, ravvisando come "*nella fase funzionale, di esecuzione del rapporto*" il lavoratore non sia autonomo per via delle "*modalità di*

---

[10] Cfr. M. Persiani, *Note sulla disciplina di alcune collaborazioni coordinate*, in *Arg. dir. lav.*, 6/2015, pp. 1257 ss.

[11] C. Pisani, *Le nuove collaborazioni etero-organizzate, il lavoro tramite piattaforme digitali e gli indici presuntivi della subordinazione*, in *Arg. dir. lav.,* 6/2019, p. 1202.

[12] Trib. Torino, 7 maggio 2018, n. 778; Trib. Milano, 10 settembre 2018, n. 1853.

[13] Cass., Sez. Lavoro, 24 gennaio 2020, n. 1663.

© Wolters Kluwer Italia

prestazione determinate in modo sostanziale da una piattaforma multimediale e da un applicativo per smartphone" [14].

La medesima qualificazione del rapporto di lavoro è avvenuta anche in successive pronunce di merito [15], o ai fini dell'applicazione della disciplina relativa alla salute e sicurezza, o dei diritti sanciti dallo Statuto e, in particolare, dell'azione di cui all'art. 28 St. lav. [16], o infine per estendervi la disciplina relativa ai profili previdenziali [17].

In altre pronunce di merito, invece, i giudici si sono orientati accertando il carattere subordinato di tali rapporti di lavoro: ciò è avvenuto, ad esempio, nella sentenza del Tribunale di Palermo del 24 novembre 2020, n. 3750, in cui il giudice ha rinvenuto la sussistenza del potere direttivo, sulla base del fatto che la piattaforma disciplini tutti gli aspetti che riguardano la consegna, come ad esempio il percorso che deve seguire il *rider*. È stato altresì rinvenuto il potere di controllo nel monitoraggio che la piattaforma riesce ad effettuare proprio attraverso l'applicazione, ed il potere disciplinare nel meccanismo del *rating*, che premia o punisce i lavoratori con riferimento alla scelta dei turni e alla loro assegnazione [18].

3. La presunzione di subordinazione nella proposta di direttiva UE

Nella prospettiva *de iure condendo* relativa alla regolamentazione giuridica dei *platform workers*, non si può prescindere da una attenta riflessione sulla proposta della Commissione europea del 9 dicembre 2021, relativa al "*miglioramento delle condizioni di lavoro nel lavoro*

---

[14] F. CARINCI, *Il percorso giurisprudenziale sui* rider*. Da Tribunale Torino 7 maggio 2018 a Tribunale Palermo 24 novembre 2020*, in *Arg. dir. lav.*, 1/2021, pp. 1-25; L. BATTISTA, *I lavoratori delle piattaforme digitali tra diritto, tecnologia e giustizia*, ivi, 6/2021, pp. 1455 ss.; M. BIASI, *Tra fattispecie ed effetti: il "*purposive approach*" della Cassazione nel caso Foodora*, in *Lav. dir. eur.*, 1/2020, pp. 2 ss.; A. PERULLI, *La prima pronuncia della Corte di Cassazione sull'art. 2, co. 1, d. lgs. n. 81/2015: una sentenza interlocutoria*, ivi, pp. 3 ss.; M. PERSIANI, *Note sulla vicenda giudiziaria dei* riders, ivi, pp. 2 ss.

[15] Trib. Firenze, 5 maggio 2020, n. 886; Trib. Bologna, 14 aprile 2020, n. 745.

[16] Trib. Milano, 28 marzo 2021; Trib. Bologna, 30 giugno 2021; App. Palermo, 23 settembre 2021; Trib. Firenze, 24 novembre 2021, n. 781.

[17] Trib. Milano, 9 ottobre 2023.

[18] Nel senso della qualificazione subordinata del rapporto di lavoro anche Trib. Torino, 18 novembre 2021 (confermata da App. Torino 13 settembre 2022); Trib. Milano, 20 aprile 2022, n. 1018; Trib. Milano, 28 settembre 2023; Trib. Milano, 19 ottobre 2023, n. 3237.

© Wolters Kluwer Italia

mediante piattaforme digitali" [19] a cui, nel corso dell'*iter* legislativo, il Parlamento europeo e il Consiglio hanno proposto una serie di emendamenti, raggiungendo da ultimo un accordo provvisorio in data 8 marzo 2024 [20].

In linea generale, l'obiettivo della proposta consiste nel miglioramento delle condizioni di lavoro e dei diritti sociali dei soggetti che svolgono la propria attività tramite piattaforme digitali, anche al fine di favorire la crescita sostenibile delle piattaforme nell'Unione europea.

Più in particolare, la suddetta proposta è articolata in sei Capi, in cui sono chiarite preliminarmente le finalità, l'ambito di applicazione dell'iniziativa e le definizioni dei termini utilizzati.

In secondo luogo, si propongono dei meccanismi finalizzati al corretto accertamento della natura dei rapporti di lavoro svolti mediante piattaforme digitali, con l'introduzione di una presunzione legale. In terzo luogo, la direttiva appresta una serie di tutele contro i rischi derivanti dalla gestione algoritmica.

Inoltre, è posto l'accento sulla necessità della trasparenza delle informazioni acquisite dalle autorità pubbliche e, nel Capo V, sull'esigenza di garantire ai lavoratori il diritto di accedere alla tutela giurisdizionale sotto vari profili. Infine, sono introdotte una serie di misure rimediali, individuali e collettive.

Il tema centrale riguarda il meccanismo di accertamento della natura subordinata della prestazione, prevista nel Capo II. La disposizione intende contrastare il fenomeno della c.d. "*misclassification*", cioè del lavoro autonomo fittizio, imponendo agli Stati di adottare procedure adeguate al fine di prevenire ed affrontare la corretta "situazione occupazionale" dei lavoratori coinvolti [21].

Rileva, in tal senso, il principio del primato dei fatti secondo cui è irrilevante ai fini qualificatori la volontà delle parti e dunque il modo in cui il rapporto è definito nel contratto, ma l'esistenza dello stesso si fonda sui fatti relativi all'effettiva esecuzione del lavoro, conformemente alla raccomandazione dell'Organizzazione internazionale del lavoro (OIL) n. 198 del 2006 sul rapporto di lavoro.

---

[19] Proposta di direttiva del Parlamento europeo e del Consiglio relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali, Bruxelles, 9 dicembre 2021, COM(2021)762 final.

[20] Comunicato stampa del Consiglio, "*Lavoratori delle piattaforme digitali: il Consiglio conferma l'accordo su nuove norme volte a migliorare le loro condizioni di lavoro*", 11 marzo 2024.

[21] COM(2021)762 final, 26° "considerando".

© Wolters Kluwer Italia

Tuttavia, la direttiva non intende solo combattere la falsa qualificazione di un rapporto di lavoro che nei fatti è subordinato, avendo peraltro un'altra prospettiva, che è la promozione di diritti per il vero lavoro autonomo [22]: in altri termini, non guarda solo alla subordinazione come "porto sicuro" per l'applicazione delle tutele ordinamentali, ma anche al lavoro autonomo genuino, bisognoso di specifiche tutele.

Più in particolare, ai sensi dell'art. 2, par. 1, la direttiva si applica nei confronti di tutti i lavoratori che svolgono una prestazione tramite piattaforme digitali che abbiano "*un contratto di lavoro o si ritiene che abbiano un rapporto di lavoro quali definiti dal diritto, dai contratti collettivi o dalle prassi in vigore negli Stati membri, tenuto conto della giurisprudenza della Corte di giustizia*".

Il centro gravitazionale della proposta risiede, come anticipato, nel meccanismo della presunzione semplice di subordinazione [23]. Più in particolare, ai sensi dell'art. 5, alla presenza di fatti che indicano "*un potere di controllo o direzione, conformemente al diritto nazionale*", si presume la natura subordinata del rapporto di lavoro.

Ciò a dispetto della versione iniziale, in cui era invece necessario che ricorressero almeno due indici dei cinque previsti ai fini della configurazione di un potere di controllo della piattaforma sull'esecuzione del lavoro. Nella specie, essi consistevano nel potere unilaterale della piattaforma di determinare il livello di retribuzione; nell'obbligo per il lavoratore di rispettare regole vincolanti sull'aspetto o sul comportamento nei confronti del destinatario del servizio; nel potere di controllo sui risultati del lavoro, sempre per mezzo della piattaforma; nel potere organizzativo della piattaforma, cioè nella possibilità di limitare, anche tramite sanzioni, la libertà e l'autonomia del lavoratore di scegliere l'orario di lavoro o i periodi di assenza e di accettare o rifiutare incarichi; nel divieto espresso per il lavoratore di crearsi una propria clientela o di svolgere lavori per altri committenti [24].

La qualificazione del *platform worker* come lavoratore subordinato determina evidentemente il riconoscimento di una serie di tutele rappresentate dal salario minimo, dal diritto a godere di ferie retribuite, dall'indennità di malattia e disoccupazione, dall'accantonamento di

---

[22] *Id*., 30° "considerando".

[23] E. MENEGATTI, *Ragionando sulla presunzione di subordinazione di cui dalla proposta di Direttiva sul lavoro mediante piattaforme digitali*, in *Federalismi.it*, 14/2023, p. 234.

[24] Impostazione criticata da una parte della dottrina, in virtù dell'ampliamento del campo di applicazione del lavoro subordinato. Cfr. P. TULLINI, *La Direttiva Piattaforme e i diritti del lavoro digitale*, in *Labour & Law Issues*, 1/2022, p. 49.

© Wolters Kluwer Italia

contributi previdenziali e da un migliore accesso alle tutele contro gli infortuni sul lavoro, con conseguente inevitabile ricadute applicative in termini di aumento dei costi dei servizi a carico dei consumatori.

L'articolo introduce, inoltre, un ulteriore strumento che si ricollega alla predetta presunzione e che consiste nell'inversione dell'onere probatorio, che in tal caso ricade sulla piattaforma, la quale sarà chiamata a dimostrare che quel rapporto contrattuale non si configura come rapporto di lavoro subordinato, sulla base degli indicatori di ciascuno Stato [25].

Quel che è certo è che l'efficacia applicativa della suddetta presunzione sarà rimessa interamente alla capacità attuativa dei singoli Stati membri [26].

4. Conclusioni e prospettive future

La tecnica regolativa della presunzione di subordinazione è ad oggi ampiamente dibattuta: da una parte, vi è chi vi ravvisa un efficace strumento per garantire la certezza del diritto per i soggetti coinvolti [27]; dall'altra, vi è chi ne evidenzia invece l'incertezza rappresentata proprio dalla valutazione dell'interprete nel procedimento di qualificazione [28].

Infatti, la disciplina della presunzione eurounitaria risulta essere interamente rimessa alle tradizioni normative e alle scelte dei singoli Stati [29].

Un ulteriore punto controverso è poi rappresentato dall'esclusione del meccanismo della presunzione per le "*questioni fiscali, penali e di sicurezza sociale*", come si evince dall'art. 5, anche se gli Stati membri "*possono applicare la presunzione legale in tali procedimenti in base*

---

[25] Sulle criticità sollevate dalla tecnica della presunzione cfr. B. Caruso - R. Del Punta - T. Treu, *Il diritto del lavoro nella giusta transizione. Un contributo "oltre" il manifesto*, 2023, p. 68.

[26] M. Giovannone, *Il lavoro tramite piattaforma nell'ordinamento europeo*, in M. Biasi (a cura di), *Diritto del lavoro e intelligenza artificiale*, Milano, 2024, p. 508.

[27] M. Kullmann, *Platformisation's of Work: An EU Perspective on Introducing a Legal Presumption*, in *European Labour Law Journal*, 1/2021, pp. 66-80.

[28] M. Giovannone, *La proposta di direttiva UE sui* platform workers*: tecniche regolative ed effettività delle tutele per i lavoratori autonomi*, in *Federalismi.it*, 25/2022, pp. 135 ss.

[29] M. Barbieri, *Prime osservazioni sulla proposta di direttiva per il miglioramento delle condizioni di lavoro nel lavoro con piattaforma*, in *Labour & Law Issues*, 2/2021.

© Wolters Kluwer Italia

al diritto nazionale". È dunque dubbio l'atteggiamento che l'ordinamento nazionale adotterà in merito a tale aspetto, e cioè se propenderà per un'interpretazione minimale o meno della disposizione.

Quanto alle possibili ricadute della futura direttiva sulla questione qualificatoria nell'ordinamento italiano, si ritiene che la disposizione che più di altre potrebbe consentire l'applicazione della disciplina del lavoro subordinato sia proprio l'art. 2 del d. lgs. n. 81/2015, alla luce della sua attitudine a poter ricomprendere anche fattispecie che non rientrano nella nozione di cui al 2094 c.c. [30]

[30] G. BANDELLONI, *Il lavoro tramite piattaforma nel diritto interno*, in M. BIASI (a cura di), *Diritto del lavoro e intelligenza artificiale*, cit., p. 496; A. DONINI, *Alcune riflessioni sulla presunzione di subordinazione della Direttiva Piattaforme*, in *Labour & Law Issues*, 1/2022, p. 39.

© Wolters Kluwer Italia

IL LAVORO CHE CAMBIA E SI ADEGUA ALL'ERA DELLA TRASFORMAZIONE DIGITALE *

Melania Carteri

Sommario: 1. Premessa. La persona del lavoratore negli scenari attraversati dall'innovazione tecnologica. – 2. Il lavoro nell'organizzazione, nei ruoli, nei risultati. – 3. Le tipologie applicative del lavoro digitale: lavoro agile e artigianato digitale. – 4. Tecnologia e tutela costituzionale del lavoro. – 5. Conclusioni. Il diritto del lavoro verso un adeguamento normativo necessario.

Abstract: The contribution will propose a study on the evolving nature of labour law driven by technological advancements and will assess its "positive" impacts on domestic labour law. First, it will examine the transformations in labour organisation, roles, and outcomes. The study will also briefly analyse the applications of digital labour, specifically focusing on remote work and digital craftsmanship. It will then highlight the potential of technology to enhance managerial advantages in labour management, improve the recognition of individual personality, and automate both manual and cognitive tasks, regardless of the type of work and categories of workers involved. Moreover, the intrinsic tendency of digital labour towards equality and social dignity will be emphasised. Constitutional protection of labour (Article 4 of the Constitution) is guaranteed to all workers, irrespective of the type of work performed. Furthermore, in the current digital age, new forms of labour enable the implementation of Article 35 of the Constitution, which promises protection for labour in all its forms and applications. Finally, conclusions will be drawn regarding traditional labour law, which is struggling to address the new demands for worker protection. It will be argued that labour law needs to be adaptable according to the va-

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

rying degrees of contractual weakness of workers. This approach will consider the increased aspirations for spatial, temporal, and existential autonomy of workers, who rediscover their identity as independent producers and creators within technologically advanced environments.

1. Premessa. La persona del lavoratore negli scenari attraversati dall'innovazione tecnologica

"*Abbiamo bisogno, in parte, di nuovi sentieri perché siamo cambiati*" [1]. Così, scrive il filosofo americano Charles Taylor nel suo celebre libro "*Questioni di senso nell'età secolare*", per illustrare una complessa età post-moderna investita da grandi trasformazioni sociali, economiche ed umane. La rivoluzione tecnologica ha incentivato queste trasformazioni. Anche il diritto partecipa *naturaliter* a questa fase storica, inaugurando, in particolare, il diritto del lavoro, una nuova *way of working* [2], che cerca di equilibrare le tre autonomie, spaziale, temporale ed esistenziale ricercate dal lavoratore [3] con il potere regolatorio del datore di lavoro. Tale nuovo paradigma segue una logica di cooperazione tra datore di lavoro e lavoratore, che ha sullo sfondo, una logica "*win win*" tra persona e intelligenza artificiale. In tal modo, tutti traggono vantaggio dallo sviluppo digitale: la persona del lavoratore "aumentata" dalla tecnologia, l'impresa ed il datore di lavoro che sperimentano gli effetti fertili della gestione positiva del lavoro digitalizzato [4].

La tecnologia è, dunque, intesa quale primo vettore di accelerazione di un processo sociale operante un profondo cambiamento morfologico del lavoro che coinvolge il lavoratore e prima ancora la persona, "*con le sue capacitazioni, qualunque siano i luoghi di lavoro e gli sce-*

[1] C. TAYLOR, *Questioni di senso nell'età secolare*, Milano, 2023, p. 68.

[2] F. BUTERA, *Dal lavoro agile alla new way of working*, in G. MARI - F. AMMANNATI - S. BROGI - T. FAITINI - A. FERMANI - F. SEGHEZZI - A. TONARELLI (a cura di), *Idee di lavoro e di ozio per la nostra civiltà*, Firenze, 2024, p. 1555.

[3] B. CARUSO - L. ZAPPALÀ, *Un diritto del lavoro "tridimensionale": valori e tecniche di fronte ai mutamenti dei luoghi di lavoro*, in R. DEL PUNTA (a cura di), *Valori e tecniche nel diritto del lavoro*, Firenze, 2022, p. 49.

[4] Così, L. ZAPPALÀ, *Informatizzazione dei processi decisionali e diritto del lavoro: algoritmi, poteri datoriali e responsabilità del prestatore nell'era dell'intelligenza artificiale*, in *Biblioteca "20 Maggio"*, 2/2021, pp. 116 ss.

© Wolters Kluwer Italia

nari in cui esplica la sua personalità" [5], qualunque siano i luoghi attraversati dall'innovazione tecnologica.

Ci si avvia ad un "nuovo" diritto del lavoro che "*quasi ritrova sé stesso, come disciplina che ha ragion d'essere proprio nella relazione tra le innovazioni tecniche (e tecnologiche) e l'attività lavorativa*" [6]. Un lavoro che può avvalersi delle capacità tecnologiche per favorire ed esaltare le straordinarie potenzialità ed aspirazioni (prima) della persona (e poi) del lavoratore.

La tecnologia include tutti i lavoratori, riscoprendosi la sua naturale inclinazione al soddisfacimento delle promesse costituzionali di uguaglianza e al "*pieno riconoscimento della dignità dei lavoratori all'interno della formazione sociale impresa*" [7], qualunque forma di lavoro venga svolto, manuale, intellettuale (art. 35 Cost.) tecnico, organizzativo, esecutivo (art. 2060 c.c.). Si sperimenta, così, un diritto del "*lavoro permeabile con la vita personale*" [8], in quanto edificante un nuovo ordine giuridico fatto di "*relazioni con le persone e con la tecnologia*" [9], con al "*centro il benessere e la crescita della persona*" [10].

Questo nuovo paradigma dà valore alla "persona" del lavoratore nel progetto di protezione e promozione dello sviluppo tecnologico, rispettando le conoscenze e competenze acquisite dal lavoratore che ottiene "*un riconoscimento in grado di superare il proprio status di subordinazione*" [11].

2. Il lavoro nell'organizzazione, nei ruoli, nei risultati

Il cambiamento del lavoro parte dall'organizzazione, nella quale ruoli e risultati si modificano.

---

[5] B. Caruso - L. Zappalà, *Op. cit*., p. 46.

[6] U. Gargiulo, *Intelligenza Artificiale e poteri datoriali: limiti normativi e ruolo dell'autonomia collettiva*, in *Federalismi.it*, 29/2023, p. 172.

[7] R. Del Punta, *Il diritto del lavoro e il lavoro postfordista*, in G. Mari - F. Ammannati - S. Brogi - T. Faitini - A. Fermani - F. Seghezzi - A. Tonarelli (a cura di), *Idee di lavoro e di ozio per la nostra civiltà*, cit., p. 1483.

[8] F. Butera, *Dal lavoro agile alla new way of working*, cit., p. 1561.

[9] *Ibid*.

[10] F. Butera, *Organizzazione 5.0 e una nuova idea di lavoro*, in G. Mari - F. Ammannati - S. Brogi - T. Faitini - A. Fermani - F. Seghezzi - A. Tonarelli (a cura di), *Idee di lavoro e di ozio per la nostra civiltà*, cit., p. 1509.

[11] M.G. Militello, *L'impresa sostenibile tra riconoscimento e redistribuzione. Dialogando con Bruno Caruso*, in *Trasformazioni dell'impresa e diritto del lavoro*, in *Biblioteca "20 Maggio"*, Collective volumes, 2024, p. 25.

© Wolters Kluwer Italia

L'organizzazione, quale spazio delle regole e del diritto, oggi diviene un luogo dematerializzato, che si consegna al contesto digitale, uno spazio sempre più ubiquo tra la sede fisica del lavoro e la casa, personalizzato in base a bisogni, ambizioni e competenze di un lavoratore "potenziato" dalla tecnologia. Il lavoro di nuova concezione apre a diverse dimensioni dell'organizzazione, in particolare, al "cosa" ed al "chi" del cambiamento [12]. Quanto al primo profilo, ci si riferisce al contenuto della prestazione lavorativa e delle organizzazioni. La logica di cooperazione tra datore di lavoro e lavoratore favorisce uno snellimento della subordinazione classica, sganciando il lavoratore dalle attività lavorative scandite da un tempo fisso in presenza nella sede di lavoro e sotto il controllo della gerarchia. Il lavoro agile è l'esempio più evidente di accesso e funzionamento della tecnologia tanto nell'impresa quanto nella pubblica amministrazione. Il cambiamento nell'organizzazione riguarda soprattutto, il "chi", ossia i prestatori di lavoro che hanno modellato le proprie attività vestendo nuovi ruoli responsabili di risultati, plasmati sulle specificità delle persone, sempre più formate, creative, competenti, professioniste, formalmente dipendenti, che sperimentano un tempo di libertà nel lavoro, con miglioramento della vita personale e lavorativa.

Così, parallelamente all'impresa e all'amministrazione, si evolve la figura datoriale imperniata tradizionalmente sull'esercizio dei tre poteri: direttivo, di controllo e disciplinare. In particolare, il potere direttivo, che trova il suo tratto distintivo nell'essere il lavoro intellettuale o manuale prestato alle "dipendenze" e "sotto la direzione" dell'imprenditore (art. 2094 c.c.), assume nel lavoro digitale nuovi contorni. L' "*elemento costitutivo della fattispecie del lavoro subordinato è l'eterodirezione della prestazione lavorativa, che consiste nella collaborazione svolta alle dipendenze e sotto la direzione del datore di lavoro*" [13]. Perciò, la sua caratteristica principale "*non consiste nel tipo di attività svolta, quindi, manuale o intellettuale [...], risiede nell'essere l'esecuzione della prestazione «alle dipendenze» del datore di lavoro, e quindi comporta una limitazione delle libertà del lavoratore*" [14]. Si tratta di una limitazione di libertà "tecnico-funzionale" esclusivamente finaliz-

[12] La sperimentazione del lavoro di nuova concezione sviluppata nelle dimensioni del cambiamento è così descritta da F. BUTERA, *Dal lavoro agile alla new way of working*, cit., pp. 1554 ss.

[13] C. PISANI, *Norme fondamentali commentate di diritto del lavoro, Ordinamento sistematico*, Torino, 2023, p. 10.

[14] *Ibid*.

© Wolters Kluwer Italia

zata all'esecuzione della prestazione, "*diversa ed ulteriore rispetto a quella che comporta un adempimento delle obbligazioni di fare o non fare degli altri contratti*" [15]. Infatti, il vincolo di subordinazione determina una ulteriore limitazione riguardante l'esecuzione della prestazione lavorativa oggetto del contratto secondo modalità che contemplano il dove, il quando ed il come della prestazione, e che limitano la libertà del lavoratore nell'adempimento della obbligazione da svolgersi "sotto la direzione" e "alle dipendenze del datore". Con l'avvento dell'era digitale, al contrario, il lavoratore riscopre una libertà nel lavoro (e non dal lavoro), che lo rende "*un autonomo artefice della propria vita*" [16], in quanto può scegliere la gestione del proprio tempo e del proprio spazio, pur dipendendo formalmente dal datore. Così, si assiste ad un allentamento del tradizionale vincolo della subordinazione, in quanto il lavoratore dispone di una "diversa libertà" nell'adempiere la sua obbligazione, secondo un tempo e un luogo che può concordare con il datore di lavoro. Dunque, l'importanza delle categorie lavoristiche classiche del tempo e dello spazio si riduce [17]. Ed ancora, la figura datoriale modella il suo potere di organizzazione "allineandosi ed alleandosi" alla figura del lavoratore che ottiene dalla tecnologia una professionalizzazione, cioè "*un aumento di valore e professionalità dei ruoli, dei mestieri e delle professioni e delle relative competenze a ogni livello*" [18]. Di conseguenza, il lavoro subordinato risulta modificato nei tratti tipici delle mansioni, ossia comando, gerarchia, controllo, e si avvale della nuova figura del lavoratore che restituisce all'organizzazione responsabilità di risultati, innovazione, servizio [19]. Il lavoro della conoscenza apre, dunque, a nuovi ruoli, "«*ruoli aperti» [...] «ruoli agiti» allorché vengono animati*, *interpretati e arricchiti dagli attori reali, vale a dire dalle persone vere all'interno delle loro organizzazioni o dei loro contesti*" [20]. La digitalizzazione ha importato una trasformazione "positiva" del lavoro con "*l'avvento nell'impresa di metodi di ideazione, produzione e collaborazione che sono altrettanti metodi di*

---

[15] *Ibid*.

[16] R. Del Punta, *Valori del diritto del lavoro ed economia di mercato*, in *Biblioteca "20 Maggio"*, 2/2019, p. 121.

[17] Così, A. Levi, *Il potere di organizzazione nell'economia digitale e i suoi limiti*, in A. Bellavista - R. Santucci (a cura di), *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, Torino, 2022, p. 13.

[18] F. Butera, *Dal lavoro agile*, cit., p. 1563.

[19] F. Butera, *Organizzazione 5.0*, cit., p. 1511.

[20] *Id*., p. 1510.

© Wolters Kluwer Italia

pensiero, di lavoro e di organizzazione" [21]. Il lavoro digitale è, dunque, il risultato di un progetto di cambiamento in cui tecnologia, organizzazione e lavoro progettano e operano congiuntamente.

3. Le tipologie applicative del lavoro digitale: lavoro agile e artigianato digitale

L'economia digitale ha favorito la proliferazione sul mercato del lavoro di tipologie applicative molto variegate e disomogenee. Tra queste rilevano il lavoro agile e l'artigianato digitale. La loro caratteristica comune risiede nella particolare valorizzazione della personalità e professionalità del lavoratore, che "*ancor prima di esser tale, è un utente della rete*" [22], molto formato e partecipativo, che trae dalla frequente consultazione del *web*, la fonte di un apprendimento costante ed in continua crescita.

Il lavoro agile o *smart working* o lavoro a distanza è un esempio utile di lavoro vincente nell'ambito dei c.d. "*istituti generativi del rapporto di lavoro perché mettono al centro la qualità del lavoro, la persona e la sua responsabilità*" [23], ed ha interessato sia le imprese che le pubbliche amministrazioni.

L' art. 18, l. 22 maggio 2017, n. 81, individua nel lavoro agile una modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa. Il lavoro a distanza rappresenta un utile strumento di conciliazione vita-lavoro, favorita dalla personalizzazione dell'orario di lavoro e del luogo di lavoro individualmente concordati. Ciò rende lo *smart working* una tipologia di lavoro che ben si inserisce nei programmi di lavoro sostenibile. Da un lato, la scelta dell'orario e del luogo di lavoro assicura la sostenibilità sociale. Il lavoratore, attraverso un'impostazione dell'attività lavorativa da svolgersi in modo conciliante con i tempi di vita personali e familiari, riesce a costruirsi la realizzazione del suo potenziale e al contempo vede appagate le sue

---

[21] A. PERULLI - V. SPEZIALE, *Dieci tesi sul diritto del lavoro*, Bologna, 2022, p. 142.

[22] A. LEVI, *Il potere di organizzazione nell'economia digitale e i suoi limiti*, cit. p. 13.

[23] B. CARUSO, *Capability e diritto del lavoro: non solo teoria. Dialogando con Riccardo del Punta*, WP CSDLE "Massimo D'Antona".IT – 479/2024, p. 14.

© Wolters Kluwer Italia

legittime pretese di riappropriazione di bisogni materiali e spirituali da attuarsi dentro e fuori il lavoro. Dall'altro lato, il lavoro agile consente di perseguire la sostenibilità ambientale, in quanto l'assenza di vincoli di orari e luoghi di lavoro, svincola il lavoratore sia dagli spostamenti tra la propria abitazione e la sede fisica del lavoro, riducendosi così le emissioni di carbonio, che dall'uso di grandi spazi di lavoro, riducendosi anche i costi ambientali.

Inoltre, il lavoro agile consente di ottenere il miglioramento della qualità del lavoro erogato in termini di rendimento-produttività. Il lavoro da remoto innesca nei lavoratori positivi meccanismi di rendimento predisponendoli a restituire le migliori *performance* possibili, in quanto dettate dal riconoscimento della fiducia investita dal datore di lavoro secondo una logica di cooperazione finalizzata alla crescita del lavoratore, al miglioramento della qualità della vita e del lavoro, in una parola sola, al benessere.

Accanto al lavoratore agile, merita considerazione la figura dell'artigiano digitale assimilabile a quella classica del piccolo imprenditore (art. 2083 c.c.). L'artigianato digitale rappresenta una forma di lavoro tecnico-manuale, in cui il tempo e lo spazio in cui lavora sono suoi alleati. In particolare, secondo il Manifesto dei nuovi artigiani del XXI secolo, il luogo di lavoro è considerato per l'artigiano "*molto più di un luogo di lavoro: è parte integrale e integrante del territorio in cui l'attività artigiana è ubicata e racchiude un pezzo della vita di chi ci lavora*" [24] e l'arco temporale necessario alla realizzazione dell'opera racchiude uno spazio temporale che dura nel tempo: "*il rapporto fra l'artigiano e ciò che produce continua nel tempo: riparazione, recupero, rigenerazione, rinnovamento sono espressioni tipiche del vocabolario artigiano*" [25].

L'artigiano, da un lato, è legato alla tradizione e ad un sapere frutto dell'abilità artistica delle sue mani, dall'altro è aperto all'innovazione tecnologica. "*La figura dell'artigiano è dunque una realtà «bifronte», che guarda al futuro ma non dimentica il passato [...] con un piglio creativo e sensibile al contesto in cui opera, [...] usa le nuove tecnologie non per sostituire l'uomo con la macchina ma per potenziare il suo operato e la sua capacità trasformativa*" [26]. Nell'artigianato digitale si mescolano due attitudini: alla stabilità e

---

[24] DNA dei Giovani Imprenditori di Confartigianato, *Manifesto dei nuovi artigiani del XXI secolo*, disponibile su *www.giovanimprenditori.confartigianato.it*, p. 5.

[25] *Ibid*.

[26] A. Granelli, *Artigianato digitale*, in G. Mari - F. Ammannati - S. Brogi - T.

© Wolters Kluwer Italia

alla conservazione dei valori del passato, egli infatti padroneggia la "*techne*", "*maestria che sfocia in arte*" [27], e al cambiamento, "*l'artigiano è un imprenditore che rispetta la tradizione ma è fortemente attratto dall'innovazione*" [28].

L'artigianato digitale sperimenta molteplici effetti positivi della tecnologia. L'artigiano, infatti, si serve "*di nuovi strumenti dall'anima sempre più digitale*" [29], ma ne mantiene il controllo in quanto "*l'uso e soprattutto la progettazione degli strumenti digitali richiede un'attitudine sempre più artigiana*" [30]. La figura dell'artigiano digitale sembra ben allinearsi con l'approccio di un'intelligenza artificiale da gestire "sotto il controllo umano". Un simile approccio, infatti, assicura che "*le decisioni finali che influenzano il lavoro*" [31] vengano assunte dall'uomo e non dalla macchina. Pertanto, l'utilizzo, da parte dell'artigiano, della tecnologia, fa dell'artigiano un creatore creativo ed un produttore autonomo della sua opera, in quanto specializzato "*con l'«intelligenza nelle mani»*" [32], grazie ad una tecnica "*alleata del lavoro, generata dal pensiero umano*" [33] e "*con un alto livello di generazione di valore simbolico, estetico, economico*" [34].

4. Tecnologia e tutela costituzionale del lavoro

Dallo studio finora effettuato, emerge con chiarezza il facile approdo dell'Intelligenza artificiale in tutti lavori, qualunque forma o tipologia di lavoro venga svolto dal lavoratore. Dal lavoro intellettuale, quale quello di un dipendente pubblico in regime di *smart working*, al lavoro tecnico-manuale, quale quello di un artigiano digitale che realizza prodotti artigianali "*made in Italy*", utilizzando anche le tecnologie.

Con l'avvento della robotica e dell'automazione, tutte le mansioni, a cui il lavoratore è adibito, possono essere automatizzate, non soltanto

---

FAITINI - A. FERMANI - F. SEGHEZZI - A. TONARELLI (a cura di), *Idee di lavoro e di ozio per la nostra civiltà*, cit., p. 1536.

[27] *Ibid*.

[28] *Manifesto dei nuovi artigiani del XXI secolo*, cit., p. 5.

[29] A. GRANELLI, *Op. cit.*, p. 1537.

[30] *Ibid*.

[31] Commissione mondiale sul futuro del lavoro, *Lavorare per un futuro migliore*, Ginevra, 22 maggio 2019, disponibile su: *www.ilo.org*, p. 15.

[32] F. BUTERA, *Organizzazione 5.0 e una nuova idea di lavoro*, cit. p. 1507.

[33] Sommo Pontefice Giovanni Paolo II, Lettera enciclica *Laborem exercens*, disponibile su: *www.vatican.va*.

[34] F. BUTERA, *Organizzazione 5.0 e una nuova idea di lavoro*, cit., p. 1513.

© Wolters Kluwer Italia

quelle manuali, ma anche quelle di concetto, attraverso l'impiego della tecnologia più sofisticata [35].

La tutela del lavoro in tutte le sue forme ed applicazioni di cui all'art. 35 Cost., unitamente a quanto disposto dall'art. 2060 c.c. che specifica la tutela del lavoro prestato nelle forme organizzative ed esecutive, intellettuali, tecniche e manuali, è stimolo cogente per l'ordinamento verso il compimento, oggi più che mai, nell'era digitale, di "*un'opera di costante costituzionalizzazione del lavoro*" [36].

La Carta fondamentale attraverso la sua impostazione lavoro-centrica consegna all'ordinamento giuridico una singolarità esemplare imperniata su un esteso riconoscimento dei diritti sociali dei lavoratori. Ad essi il progetto costituzionale di uguaglianza (art. 3 Cost.) si rivolge, promettendo che "*lo sviluppo della personalità venga attuato essenzialmente mediante il lavoro tanto da far parlare di glorificazione teoretica del lavoro*" [37].

Lo svolgimento del lavoro di nuova concezione è, dunque, "*un'occasione storica per dare finalmente attuazione all'art. 35 cost. che promette la tutela del lavoro in tutte le sue forme e applicazioni*" [38].

Nonostante le possibili ricadute negative della digitalizzazione [39], il lavoro digitale offre una grande *chance* ai lavoratori: promette la dignità sociale a cui ogni uomo è chiamato a prescindere dalla mansione, manuale ed intellettuale cui siano adibiti. Così, parificando i lavoratori, il lavoro di nuova concezione "*dà valore economico e sociale e qualità alla vita delle persone*" [40] ed evoca il principio secondo cui "*il primo fondamento del valore del lavoro è l'uomo stesso, il suo soggetto*" [41], oggi più che mai potenziato dalla tecnologia ed innovato dal suo risultato fruttuoso: la circolazione dell'informa-

---

[35] Così, U. Gargiulo, *Intelligenza Artificiale e poteri datoriali: limiti normativi e ruolo dell'autonomia collettiva*, cit. p. 172.

[36] C. Salazar, *La Costituzione interpretata dalle parti sociali*, in *Costituzionalismi.it*, 2/2018, p. 12.

[37] C. Pisani, *Dignità del lavoro e reddito di cittadinanza: un'antitesi*, in *Mass. giur. lav.*, 1/2019, p. 118.

[38] A. Perulli - V. Speziale, *Dieci tesi sul diritto del lavoro*, cit., 135.

[39] Tra questi si segnalano la paura per la scomparsa di alcuni lavori e il rischio di sostituzione dell'uomo con la macchina. Sul punto, sostiene F. Butera, *Organizzazione 5.0 e una nuova idea di lavoro,* cit. p. 1507: "*Il mondo del lavoro di qui al 2030 cambierà profondamente: circa il 45-50% delle future occupazioni oggi non esiste. Quelle che oggi esistono saranno profondamente modificate*".

[40] F. Butera, *Organizzazione 5.0 e una nuova idea di lavoro*, cit., p. 1508.

[41] Lettera enciclica *Laborem exercens*, cit.

© Wolters Kluwer Italia

zione, "*condizione preliminare per l'attuazione dei principi propri dello Stato democratico*" [42].

Dunque, il diritto del lavoro è chiamato adeguarsi alle regole del gioco dettate da un sistema in continua evoluzione ed ai nuovi lavoratori dalla mentalità sempre più digitale.

5. Conclusioni. Il diritto del lavoro verso un adeguamento normativo necessario

La sfida per il diritto del lavoro sarà dunque valorizzare il lavoro digitale a partire dalla sua prima casa, la Costituzione.

La presentazione del lavoro nel dettato costituzionale quale strumento di garanzia della pari dignità sociale, consente di riconoscervi una preesistente inclinazione della Carta fondamentale a riconoscere nel lavoro, quindi, anche in quello digitale, uno "*strumento di avanzamento nell'uguaglianza*" [43] e di celebrazione della persona del lavoratore.

Si tratta di un diritto del lavoro che esalta la dignità e le libertà fondamentali della persona, investe nelle sue capacità e promuove una valorizzazione sociale e identitaria del lavoratore.

A questo disegno costituzionale il diritto del lavoro è chiamato a conformarsi attraverso un'opera di adeguamento normativo necessario.

Il diritto del lavoro è oggi impegnato a dare "*valore economico e sociale a tutti i lavori, di assicurare un alto livello di occupazione e una buona qualità della vita di lavoro*" [44] e, soprattutto, a riconoscere nella rivoluzione tecnologica non la grande paura per la scomparsa del lavoro, ma "*la grande chance di una sua definitiva valorizzazione, in quanto lavoro a elevata intensità di conoscenza, e, come tale, sempre meno «dipendente» nel senso tradizionale del termine*" [45]. Così, il lavoro di nuova concezione darà rilievo, negli scenari attraversati dalla tecnologia, ad una "diversa" debolezza contrattuale del lavoratore che ha la sua genesi in una "diversa libertà" nell'esecuzione della prestazione lavorativa. Tale nuovo paradigma aprirà a nuovi orizzonti che renderanno necessaria una rivisitazione della disciplina lavoristica, at-

---

[42] C. cost., 12 aprile 2005, n. 151.

[43] R. DEL PUNTA, *Valori del diritto del lavoro ed economia di mercato*, in *Biblioteca "20 Maggio"*, 2/2019, p. 119.

[44] F. BUTERA, *Organizzazione 5.0 e una nuova idea di lavoro*, cit., p. 1508.

[45] B. CARUSO - R. DEL PUNTA - T. TREU, *Manifesto per un diritto del lavoro sostenibile*, in *Riv. dir. lav. rel. ind.*, 168/2020, p. 14.

© Wolters Kluwer Italia

traverso l'esaltazione del lavoro secondo una logica relazionale che riempia di contenuti collaborativi il rapporto di lavoro, avendo a cuore i diritti primari e universali della persona.

Così, si sperimenta un tempo in cui "*la tecnologia dà vita a diverse vie di fuga. È al sublime tecnologico che il corpo* (*del lavoratore) è consegnato*" [46] e "*le società lasci(a)no libere le persone di decidere della loro vita e s(o)no al contempo garantite le concezioni personali di vita buona (secondo le proprie possibilità e preferenze)*" [47].

[46] A.C. Amato Mangiameli, *Natur@. Dimensioni della Biogiuridica*, Torino, 2021, p. 254.

[47] *Id*., p. 137.

© Wolters Kluwer Italia

DECISIONI AUTOMATIZZATE: IL FUTURO DEI DIRITTI NELLA SOCIETÀ DIGITALE *

GIANLUCA FASANO

SOMMARIO: 1. Introduzione. – 2. La nozione normativa di decisione automatizzata: l'art. 22 del regolamento (UE) n. 2016/679 (GDPR). – 3. L'interpretazione espansiva della Corte di giustizia dell'Unione europea (C-634/21, *SCHUFA Holding*). – 4. Conclusioni.

Abstract: The development of automated individual decision-making has received a strong boost thanks to machines with large computational capabilities related to huge amounts of data and to the development of profiling algorithms and artificial intelligence systems. These systems are transforming many aspects of our society, significantly influencing the way in which crucial decisions are taken in everyday life.

The recent judgment of the Court of Justice of the European Union (C-634/21, *SCHUFA Holding*) offers the opportunity to redefine the legal notion of "automated decision-making" in a perspective that considers such decisions as the result of complex "decision-making systems", rather than mere automated processes. This perspective goes beyond the rigid dichotomy between "solely automated" decisions and human decisions, instead valorising the human-machine dialogue and the ethical and social implications of computational delegation.

1. Introduzione

Lo sviluppo di "*processi decisionali automatizzati*" (*Automated*

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

Decision-Making) [1] ha ricevuto un forte impulso grazie a macchine dotate di ampie capacità di calcolo riferite a enormi quantità di dati, grazie allo sviluppo di algoritmi di profilazione e sistemi di intelligenza artificiale. Essi vengono utilizzati in una vasta gamma di settori dove è necessario analizzare una grande quantità di informazioni al fine di valutare, prevedere e prendere decisioni. Si pensi al settore bancario e finanziario [2], ove sono diffusi per valutare il rischio di credito di un individuo o di un'azienda, indirizzando la decisione sul se concedere un prestito, a quale tasso di interesse e a quali condizioni. Di impieghi ne troviamo anche nel settore assicurativo [3], ove le compagnie possono utilizzarli per determinare i premi assicurativi, nel settore immobiliare, dove i proprietari possono valutare la solvibilità dei potenziali inquilini, nel mercato del lavoro, in cui i datori di lavoro possono utilizzarli nel processo di *screening* dei candidati, sia per il reclutamento che per la progressione professionale, e perfino nel settore pubblico, ove possono esser impiegati per decidere l'erogazione di servizi [4]. Per citarne solo alcuni.

Questi sistemi stanno influenzando in maniera significativa le modalità con cui vengono prese decisioni cruciali nella vita di tutti i giorni e saranno sempre più integrati nelle nostre vite man mano che la tecnologia continuerà ad evolversi. Rappresentano una tappa significativa nell'evoluzione degli strumenti digitali e delle pratiche decisionali, per cui diventa essenziale comprendere le implicazioni che ciò comporta sul piano della tutela dei diritti fondamentali.

Sul piano regolatorio il principale riferimento è rappresentato dall'art. 22 del regolamento (UE) n. 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (d'ora in poi anche GDPR), che ha introdotto il concetto di "non esclusività" della decisione automatizzata: l'interessato ha il

---

[1] Per seguire il lessico contenuto nel *General Data Protection Regulation*, Reg. (UE) 2016/679, all'art. 22.

[2] G. BIFERALI, *Big data e valutazione del merito creditizio per l'accesso al peer to peer lending*, in *Dir. inform.*, 2018, pp. 487 ss.

[3] D. PORRINI, *Big data, personalizzazione delle polizze ed effetti nel mercato assicurativo*, in V. FALCE - G. GHIDINI - G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2018, pp. 319 ss.

[4] Sull'uso di sistemi decisionali automatizzati nel settore dei pubblici servizi è noto il caso SyRI, sistema automatizzato progettato nei Paesi Bassi per combattere le frodi in materia di previdenza sociale, giudicato dal Tribunale distrettuale dell'Aia (*Rechtbank Den Haag* 5 febbraio 2020, C-09-550982-HA 18-388) in contrasto con l'art. 8 CEDU.

© Wolters Kluwer Italia

diritto di non essere sottoposto a una decisione basata "unicamente" sul trattamento automatizzato.

Gli strumenti di tutela previsti dal GDPR si fondano sul bilanciamento tra automazione e intervento umano, imponendo all'interprete di indagare le diverse dinamiche che caratterizzano i processi decisionali automatizzati, alla ricerca di evidenze circa la prevalenza dell'uno o dell'altro fattore. Ebbene, una siffatta indagine non risulta per nulla scontata in contesti, oggi sempre più frequenti, formati da reti complesse di *input*, algoritmi e interventi umani. Inoltre, anche laddove potrebbe apparire rilevante l'intervento umano è alto il rischio che tale intervento rappresenti una mera "presa d'atto" della decisione elaborata della macchina. In tal senso, la decisione confezionata dalla macchina verrebbe assunta come propria dell'uomo, umanizzandola e sottraendola alle tutele del GDPR.

Le difficoltà sull'interpretazione e applicazione di tale disciplina sono state già messe in luce in letteratura [5] ma oggi possiamo registrare sull'argomento una prima interpretazione della Corte di giustizia dell'Unione europea (C-634/21, *SCHUFA Holding*), decisione che merita attenzione per le sue implicazioni non soltanto sulla protezione dei dati personali ma per la tutela delle libertà nel loro complesso.

2. La nozione normativa di decisione automatizzata: l'art. 22 del regolamento (UE) n. 2016/679 (GDPR)

Il principale riferimento normativo in materia è rappresentato dall'art. 22 GDPR, il quale introduce una tutela per le persone fisiche sulla base del concetto di non esclusività della decisione automatizzata: "*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*" [6].

Sul piano applicativo, al fine di poter invocare la tutela normativa,

---

[5] S. Wachter - B. Mittelstadt - L. Floridi, *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017.

[6] Art. 22, par. 1, GDPR. Secondo le *Linee guida sulle decisioni automatizzate individuali adottate il 7 ottobre 2017 dal Gruppo di lavoro sulla protezione degli individui con riguardo al trattamento dei dati personali istituito dall'art. 29 della direttiva 95/46/EC (c.d. A29WP)*, anche un annuncio pubblicitario "personalizzato" può essere una decisione agli effetti dell'art. 22.

© Wolters Kluwer Italia

occorre individuare l'esatto confine della fattispecie di divieto, compito che non risulta affatto agevole alla luce dei due parametri normativi che fondano il divieto stesso: da un lato, il legame della decisione con il trattamento automatizzato di informazioni personali, che deve esser qualificato da una connessione forte come risulta dall'espressione "*unicamente*"; dall'altro, l'efficacia della decisione che può manifestarsi nella produzione di "*effetti giuridici*" ovvero nell'incidere "*significativamente*" sulla persona.

Già dalla lettera della norma emerge un ambito applicativo caratterizzato da sfumature che sollevano numerose questioni interpretative e, in ultima analisi, invitano a riflettere sulla sua effettiva portata applicativa. Guardiamo al primo parametro, quello dell'intervento umano: il divieto scatta qualora la decisione sia basata "*unicamente sul trattamento automatizzato, compresa la profilazione*". La norma vuole ricercare una connessione univoca tra l'elaborazione automatizzata – di aspetti personali – e l'atto decisionale, tale da poter giudicare quest'ultimo come frutto diretto ed esclusivo della prima. Ma proprio la ricerca di questo legame poggia su elementi sfuggenti e complessi da individuare, tanto per il titolare del trattamento, a cui la logica dell'*accountability* che informa l'intera disciplina del GDPR rimette la discrezionalità di tale *assesment*, quanto per l'interessato in sede di tutela *ex post*. Indagare la misura in cui il calcolo computazionale sia prevalente sull'elemento umano è essenziale per poter invocare le tutele normative avverso le decisioni basate esclusivamente sul trattamento automatizzato e che potrebbero avere conseguenze significative per le proprie vite. Eppure un'indagine circa la prevalenza dell'uno o dell'altro fattore in contesti molto complessi, fatti di reti di *input*, algoritmi, dati e influenze umane, rischia di dissolvere le tutele stesse.

Anche il parametro dell'incidenza significativa della decisione sulla persona non è di facile valutazione. Anzitutto, la stessa formula della norma non offre criteri oggettivi attraverso cui valutare quando una decisione sia destinata ad incidere "*significativamente*" sulla persona dell'interessato [7]. Ancora una volta, la mancanza di criteri ogget-

[7] Un'indicazione viene fornita nel 71° "considerando", laddove si cita a titolo esemplificativo "*il rifiuto automatico di una domanda di credito* online *o pratiche di assunzione elettronica senza interventi umani*". Anche il Gruppo di lavoro "Articolo 29", *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., 24, è intervenuto sull'argomento, enucleando quali situazioni significative quelle che influenzano le condizioni finanziarie di una persona (ammissibilità al credito), ovvero l'accesso ai servizi sanitari, che negano un'opportunità di impiego o pongono tale persona in una posizione di

© Wolters Kluwer Italia

tivi sarà supplita da criteri soggettivi, cioè, affidando siffatta valutazione al titolare del trattamento, nella logica dell'*accountability*. Tuttavia, la sua valutazione sarà comprensibilmente rivolta ad uno *standard* in cui non tutte le persone (interessati) potrebbero identificarsi, per via dei loro differenti gradi di vulnerabilità e per via del fatto che il concetto di dignità della persona non è comprimibile in *standard* omogenei. Per tali ragioni, l'interessato si troverebbe costretto a dover eccepire le proprie ragioni opponendosi alla decisione automatizzata, soltanto *ex post*, a decisione assunta e sacrificio ormai prodotto.

Per di più, ci sono casi in cui la incisività della decisione automatizzata è celata agli occhi dell'interessato per cui viene a mancare anche quell'ultimo baluardo di garanzia rappresentato dall'autodifesa. Si pensi alla pubblicità mirata che, apparentemente non incisiva dal momento che può essere ignorata, influenza il punto di vista e la libertà di scelta degli utenti. Attraverso messaggi inviati ai singoli individui, e personalizzati grazie a sofisticati modelli predittivi computazionali di *micromarketing* [8], di cui la maggior parte degli utenti ignora l'esistenza e il funzionamento, si creano delle vere e proprie *filter bubbles* [9], ovvero delle bolle in cui l'utente viene rinchiuso ricevendo soltanto informazioni conformi alle proprie opinioni e pregiudizi.

La consapevolezza che si tratti di una previsione di difficile interpretazione ha spinto l'interprete, da più fronti, ad individuare elementi o *standard* che ne potessero agevolare l'interpretazione.

Il Gruppo di lavoro "Articolo 29", per esempio, ha identificato almeno due elementi da considerarsi rappresentativi di un intervento umano: che il coinvolgimento umano sia opera di "*una persona che dispone dell'autorità e della competenza per modificare la decisione*" e che "*tale persona dovrebbe prendere in considerazione tutti i dati pertinenti*" [10]. Di certo la specifica circa la capacità della persona di poter assumere e sindacare il risultato del modello computazionale è da intendersi come requisito necessario in vista di quel controllo umano

notevole svantaggio; decisioni che influenzano l'accesso di una persona all'istruzione, ad esempio le ammissioni universitarie.

[8] Il *micro-targeting* è una tecnica che analizza i dati personali per prevedere gli interessi di un pubblico specifico: una pratica che costituisce il modello di *business* fondamentale di diverse grandi piattaforme di *social media* e che è diventata nota al grande pubblico con lo scandalo Cambridge Analytica del 2016.

[9] E. Longo, *Dai big data alle "bolle filtro": nuovi rischi per i sistemi democratici*, in *Percorsi costituzionali*, 2/2019, pp. 29 ss.

[10] Gruppo di lavoro "Articolo 29", *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., p. 23.

© Wolters Kluwer Italia

che si vuol assicurare. Dubbi residuano, invece, relativamente all'ulteriore elemento, quello inerente a una persona che, per quanto autorevole e competente, possa "*prendere in considerazione tutti i dati pertinenti*", cioè tutti quei dati che sofisticati sistemi di calcolo sono in grado di analizzare ed elaborare, al di là e oltre la capacità inferenziali dell'uomo.

Tutti gli sforzi interpretativi muovono dall'idea di fondo che l'uomo debba poter conservare un controllo e per questa ragione si tende a enfatizzare il ruolo di supporto o strumentale che le decisioni automatizzate debbono assumere rispetto alla decisione presa dall'agente umano. Tuttavia, il problema resta il come, come assicurare siffatto ruolo strumentale, come evitare che da strumento diventi esso stesso padrone delle decisioni attraverso un uso conformativo delle risultanze del sistema automatizzato.

Questo è l'aspetto fondamentale. Anche quando la decisione non è basata unicamente sul trattamento automatizzato di aspetti personali, cioè quando il ruolo del soggetto umano appare rilevante ai fini dell'assunzione della decisione, quando il divieto *ex* art. 22 non troverebbe applicazione, proprio allora ci possiamo attendere che la "*travolgente forza pratica dell'algoritmo*" [11] prevalga, di fatto, sulla valutazione dell'uomo.

Sebbene venga prestata notevole attenzione affinché le decisioni non siano affidate soltanto all'algoritmo ma contemplino anche un coinvolgimento umano non è da sottovalutare quella capacità dell'algoritmo di indurre il decidente ad affidarsi all'esito computazionale e ad assumere la decisione recependo passivamente l'esito computazionale. Anche perché gli sviluppi esponenziali delle capacità di calcolo delle nuove tecnologie, in particolare delle macchine intelligenti, presenteranno sempre più spesso artefatti con capacità di analisi e inferenziali indispensabili per l'uomo.

E le ragioni per affidare alcune attività a sistemi automatizzati saranno sempre più sostenute e predominanti: vantaggi di elaborazione dati su larga scala, velocità, volume e aspettative di tassi di errore inferiori rispetto agli esseri umani. Di fondo, viene riconosciuta alle macchine una maggiore efficienza rispetto alle capacità analitiche umane: gli algoritmi sono infatti in grado di analizzare quantità elevatissime di

[11] A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1/2019, p. 81, che puntualizza come tale forza non dipenda da ragioni di valore scientifico, di accuratezza predittiva o di affidabilità tecnica dell'automatismo, ma – appunto – da mera convenienza pratica.

© Wolters Kluwer Italia

dati, anche fra loro eterogenei sotto il profilo qualitativo, individuandone preziose correlazioni, rapporti, inferenze che nessuna valutazione umana sarebbe in grado di rilevare [12]. In siffatto scenario sarà sempre più difficile rinunciare a tanto, sarà sempre più difficile separare e tenere distinti così nitidamente l'atto decisionale dall'elaborazione automatizzata di aspetti personali, sarà sempre più arduo, in definitiva, attuare quel paradigma disegnato dall'art. 22 che fa leva sul rapporto tra atto decisionale ed elaborazione automatizzata di aspetti personali.

3. L'interpretazione espansiva della Corte di giustizia dell'Unione europea (C-634/21, *SCHUFA Holding*)

La recente pronuncia della Corte di giustizia (C-634/21, *SCHUFA Holding*) [13] riguarda il c.d. *credit scoring*, tecnica attraverso cui la SCHUFA Holding, società privata di diritto tedesco, fornisce ai suoi *partner* contrattuali informazioni sul merito creditizio di terzi, in particolare di consumatori. Il *credit scoring* è un pronostico sulla probabilità di un comportamento futuro di una persona (*score*), come il rimborso di un prestito. La solvibilità della persona viene calcolata grazie a procedure matematiche e statistiche, utilizzando dati e caratteristiche personali che provengono da svariate fonti, quali conti bancari, cronologia degli acquisti *online* e informazioni pubbliche, come le decisioni pubblicate nelle procedure di insolvenza. Sulla base di tale profilazione individuale viene rilasciato un certificato che attesta un punteggio di merito. Chi ha un punteggio alto è considerato un buon debitore ed è considerato affidabile in caso di concessione di ulteriori obbligazioni

[12] Contraria è la posizione del TAR Lazio, sent. 10 settembre 2018, n. 9227, il quale ha relegato l'uso di decisioni completamente automatizzate nell'ambito dell'istruttoria amministrativa ad un "*ruolo strumentale e meramente ausiliario dell'attività dell'uomo*" stabilendo che "*le procedure informatiche, finanche ove pervengano al loro maggior grado di precisione e addirittura alla perfezione, non possano mai soppiantare, sostituendola davvero appieno, l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere*". Sul rapporto tra PA e IA, D.U. Galetta - J.G. Corvalán, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it*, 3/2019. Sia consentito infine richiamare G. Fasano, *L'intelligenza artificiale nella cura dell'interesse generale*, in *Giorn. dir. amm.,* 6/2020.

[13] C. giust. UE, 7 dicembre 2023, C-634/21, *SCHUFA Holding AG*, ECLI:EU:C:2023:957. Nell'occasione la Corte ha pronunciato una seconda sentenza che pertiene alle cause riunite C-26/22 e C-64/22 ove viene indagato il tema della liceità del trattamento dei dati una volta raccolti nella banca dati SCHUFA.

© Wolters Kluwer Italia

come prestiti, mutui bancari, locazione di case e anche per accedere a servizi telefonici e *Internet*.

Come venga calcolato il punteggio effettivo, tuttavia, non è argomento noto e la decisione in oggetto deriva proprio dal rifiuto della SCHUFA Holding di fornire informazioni sui loro metodi di attribuzione del punteggio. Ne è scaturito, dapprima, un reclamo dinanzi all'autorità tedesca per la protezione dei dati e, poi, un ricorso dinanzi al *Verwaltungsgericht* (Tribunale amministrativo) di Wiesbaden (Germania), il quale ha deciso di sospendere il procedimento e di sottoporre alla Corte di giustizia la seguente questione pregiudiziale: la decisione di negare il credito da parte di una banca sulla base del punteggio di credito elaborato dalla SCHUFA Holding rientra nel campo di applicazione dell'art. 22 GDPR?

La particolarità del caso discende dalla circostanza che il processo decisionale ha coinvolto più attori: da un lato, la SCHUFA Holding che ha calcolato il punteggio di merito; dall'altro, la banca che ha deciso di negare il credito sulla base di tale punteggio. In considerazione di ciò, la questione pregiudiziale assume contorni più articolati, involgendo il dibattito sul se costituisce una decisione automatizzata, ai sensi dell'art. 22 GDPR, il punteggio in sé, considerato che la sua elaborazione una volta comunicata a un soggetto terzo (nella fattispecie una banca), fonda la decisione di questi di stipulare, eseguire o cessare un rapporto contrattuale.

La ricostruzione della Corte procede per gradi. Dapprima, viene chiarita la nozione giuridica di "decisione" che, seppur non contenuta nel regolamento, trae dalla formulazione della norma una prima indicazione: è decisione qualsiasi attività atta a produrre "*effetti giuridici [...] o che incida in modo analogo significativamente sulla [...] persona*". Tale lettura trova il conforto nel 71° "considerando", ai sensi del quale una decisione può consistere anche in "*una misura, che valuti aspetti personali [...] e che produca effetti giuridici [...] o incida in modo analogo significativamente sulla sua persona*". Per di più, il medesimo "considerando" procede con esempi specifici, riferendosi proprio al "*rifiuto automatico di una domanda di credito* online *o pratiche di assunzione elettronica senza interventi umani*". In considerazione di ciò, la Corte sposa una lettura sufficientemente ampia della nozione di "decisione", di guisa da poter "*includere diversi atti che possono incidere sulla persona interessata in vari modi*" (punto 46).

E così la Corte giunge ad affermare che "*il risultato del calcolo della solvibilità di una persona sotto forma di tasso di probabilità relativo alla capacità di tale persona di onorare impegni di pagamento in futuro*" rappresenta espressione di un momento decisionale (punto

© Wolters Kluwer Italia

46). Questa prima conclusione consente di mettere in luce che l'elaborazione dell'algoritmo di *scoring* non si riduce ad una mera raccolta di informazioni, riguardanti dati e aspetti personali, assunti da svariate fonti (pubbliche e private), che, opportunamente analizzate e computate, portano a disvelare l'attitudine comportamentale di una persona, bensì appartiene essa stessa al *genus* delle decisioni.

D'altronde, nella progettazione degli algoritmi la modellazione prende avvio con la scelta degli obiettivi e in tal senso potremmo dire che gli algoritmi sono ideologicamente orientati, secondo *target* di efficienza in linea con gli interessi di sviluppatori e progettisti piuttosto che di giustizia, equità o di interesse della comunità [14]. Peraltro, occorre considerare che essi non riflettono in modo incorrotto la realtà anzi, essendo progettati allo scopo di ottenere determinati risultati attesi, si fondano su una predeterminata rappresentazione della realtà, sotto forma di problemi da risolvere, di variabili incidenti e di parametri opportunamente categorizzati [15].

Tanto ci consente di argomentare, in via generale, che l'atto decisionale può assumere anche la veste formale dell'algoritmo di *scoring* ed è facile intuire come tale prospettiva verrà ad incidere sulla ripartizione della responsabilità delle organizzazioni coinvolte. Basti solo pensare alle differenti posizioni che esse dovranno assumere, a seconda del caso specifico, con riferimenti ai ruoli *privacy* definiti dal GDPR.

Nell'indagine sugli ulteriori parametri normativi, la Corte si giova, per un verso, del concetto di profilazione *ex* art. 4, par 4, GDPR, che lo stesso legislatore ha classificato nella categoria delle decisioni basate "*unicamente sul trattamento automatizzato*" (art. 22, par. 1, GDPR); per altro verso, sugli accertamenti di fatto del giudice del rinvio, da cui risulta che in caso di domanda di mutuo rivolta da un consumatore a una banca, un tasso di probabilità insufficiente comporta, in quasi tutti i casi, il rifiuto di quest'ultima di concedere il prestito richiesto.

Quest'ultimo aspetto assume particolare rilievo nella prospettiva di analisi che si intende seguire poiché fonda l'interpretazione espansiva della nozione giuridica di "decisione automatizzata", necessaria per valutare il contesto specifico caratterizzato da una pluralità di agenti. La Corte rileva come l'azione del terzo, al quale è trasmesso il tasso

---

[14] Osserva R. Borusso, Computer *e diritto*, Milano, 1978, p. 30, che il *computer*, potendo svolgere le funzioni più diverse, "*può servire a tutto come a niente, nella misura in cui è stato istruito*".

[15] A.C. Amato Mangiameli, *Algoritmi e big data. Dalla carta sulla robotica*, in *Riv. fil. dir.*, 1/2019, pp. 109 ss.

© Wolters Kluwer Italia

di *scoring*, è guidata da tale tasso in maniera decisiva: "the action of the third party to whom the probability value is transmitted draws «strongly» on that value". Un accertamento di fatto cui segue un'interpretazione della norma che ha riflessi rilevanti su una serie di questioni fondamentali legate alla tutela dei dati personali, alla certezza del diritto, alle dinamiche del potere decisionale e alla ripartizione della relativa responsabilità.

4. Conclusioni

L'interpretazione offerta dalla Corte di giustizia offre l'occasione per ripensare la nozione giuridica di "decisione automatizzata" avvalorando una prospettiva omnicomprensiva che consideri le decisioni assunte con l'ausilio di strumenti di automazione come il frutto di "sistemi decisionali" piuttosto che meri processi decisionali. Questo cambio di prospettiva consentirebbe di analizzare le decisioni automatizzate come il frutto di un complesso di interazioni tra differenti componenti, umane e computazionali, volgendo così lo sguardo al percorso, al contesto, alle componenti e alle dinamiche del decidere i cui elementi finiscono per combinarsi tra loro fino a fondersi l'un l'altro, senza possibilità di individuarne una prevalenza o una esclusività. Lo sguardo unitario consentirebbe di superare il paradigma scriminante della decisione "unicamente automatizzata", foriera di complessità interpretative e difficoltà applicative.

La prospettiva proposta consentirebbe, altresì, di dare maggior peso alle ragioni che dovrebbero fondare il ricorso ai sistemi decisionali automatizzati e a quelle che, invece, dovrebbero spingere a preservare una decisione umana. In effetti, non possiamo non riconosce alle nuove tecnologie il vantaggio di espandere i confini della cognizione umana, determinando la liberazione della persona dai propri limiti cognitivi e assicurando alla società intera una profonda innovazione. Questo progresso non dovrebbe essere sottovalutato né sacrificato.

Per altro verso, il dibattito sulla delega computazionale si intreccia inevitabilmente con la tutela delle libertà individuali, sollevando questioni fondamentali su quanta parte di queste libertà siamo disposti a cedere e per quali imperative ragioni. Se, ad esempio, l'obiettivo dell'automazione fosse prevenire crimini, attacchi terroristici o cyberattacchi, oppure migliorare diagnosi mediche e piani terapeutici, potremmo essere più inclini ad accettare una limitazione parziale della nostra libertà. Se invece lo scopo è quello di dirci ciò che possiamo fare (aprire un mutuo, fittare casa, avere un lavoro, ecc.) e, quindi, ciò che pos-

© Wolters Kluwer Italia

siamo essere, allora ci rendiamo conto di come la delega computazionale comprima la persona nel proprio vissuto, decidendo il suo futuro in base al suo passato, e si avvertirebbe forte il bisogno di un diritto all'oblio comportamentale. Ed è in questa prospettiva che potrebbe esser letto, e rinvigorito, il divieto di decisioni automatizzate, la cui *ratio* dovrebbe collegarsi alla preoccupazione che l'efficientismo della tecnica possa compromettere la comprensione dell'essere laddove non lasci spazio alla imprevedibilità e alla complessità emotiva dell'essere umano, laddove non assicuri una rappresentazione veramente autentica dell'esistenza ma finisca per replicarla nel tempo.

Non si propone, dunque, una lettura soltanto in termini di pericolo di discriminazione nell'uso dei sistemi decisionali automatizzati. Sarebbe riduttivo. Non si tratta dell'esigenza di tutela di gruppi marginali o minoritari, bensì di tutelare tutti valorizzando le differenze, in quanto necessarie per garantire il pluralismo, la pari dignità sociale (art. 3, comma 1, Cost.), il perseguimento dell'uguaglianza (art. 3, comma 1, Cost.) e il pieno sviluppo della persona umana (art. 3, comma 2, Cost.). E, in un'epoca in cui l'accesso a molti servizi, sia pubblici che privati, è disposto sulla base di una delega computazionale la cui complessità rende fragili le tutele normative vigenti, il diritto all'oblio appare un rimedio necessario a garantire il pieno sviluppo della persona umana.

© Wolters Kluwer Italia

Sezione Quinta

STRUMENTI DIGITALI E PROBLEMI DI RESPONSABILITÀ

RESPONSABILITÀ PENALE DELL'UOMO PER L'UTILIZZO DI SISTEMI DI INTELLIGENZA ARTIFICIALE * **

ORIANA LOMBARDI

SOMMARIO: 1. Introduzione. – 2. Condotte colpose. – 2.1. Obblighi positivi specifici. – 2.2. Obbligo di *human oversight*. – 3. Il problema dell'accertamento causale. – 4. Un possibile scenario: tra colpa dell'utilizzatore e *responsibility gap*. – 5. Considerazioni conclusive.

Abstract: The adoption by the EU of the first legally binding Regulation on artificial intelligence calls upon all legal practitioners to draw conclusions from it. Artificial intelligence systems (*id est* their functioning mechanisms) constitute a Copernican revolution that pushes the criminalists to inquire, in case of a damaging event, how human-machine collaboration can acquire criminal relevance in compliance with the principle of legality, its corollaries and in accordance with the traditional categories of the field. The greatest uncertainties are to be found on the side of negligent behaviours, in relation to which the question arises as to how human use of artificial intelligence affects the possibility of being charged with culpability, the very notion of negligence in the light of the obligations just introduced by the AI Act as well as the correct reconstruction of the causal link.

---

* Contributo sottoposto a doppio referaggio in forma anonima.

** Desidero ringraziare il Professor L. PICOTTI, Ordinario di Diritto Penale presso l'Università degli Studi di Verona, per la disponibilità e la fiducia mostratami condividendo suggerimenti e contenuti preziosi che hanno guidato la stesura del presente elaborato.

© Wolters Kluwer Italia

1. Introduzione

L'*AI Act* adottato il 13 giugno 2024 dal Parlamento europeo e dal Consiglio reca la prima definizione vincolante di intelligenza artificiale [1]. In buona sostanza, con la locuzione intelligenza artificiale (d'ora in poi IA) ci si riferisce alla capacità di una macchina di operare, quasi di ragionare, in modo non dissimile dalla mente umana elaborando grandi quantità di dati sulla base di istruzioni fornite da algoritmi capaci di aggiornarsi in modo automatico, c.d. *machine learning* [2]. Tali sistemi sono impiegati ormai da decenni in numerosi settori per delegare alle macchine compiti specifici affinché vengano svolti più velocemente e in modo più accurato (auspicabilmente) rispetto a quanto l'uomo potrebbe fare, consentendogli nel frattempo di concentrarsi su quanto invece non è delegabile [3]. Del resto, quando si parla di progresso l'obiettivo è sempre lo stesso: permettere all'uomo una vita più agevole. Tuttavia, ogni attività umana, specialmente se svolta con l'ausilio di tecnologie avanzate e come tali molto spesso poco intellegibili, espone la collettività a dei rischi più o meno elevati rendendoci tutti beneficiari di un'evoluzione che ci mette inevitabilmente in pericolo. Per le attività pericolose, ma consentite e dunque regolamentate poiché socialmente utili, il legislatore e gli amministratori sono sempre alla ricerca di una normazione che individui un punto di equilibrio fra mas-

---

[1] Ai sensi dell'art. 3, co. 1, del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, per sistema di intelligenza artificiale si intende "*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*".

[2] Secondo la Commissione europea: "[m]achine learning (ML) is a subset of AI, where algorithms are trained to infer certain patterns based on a set of data in order to determine the actions needed to achieve a given goal", v. il *White Paper on Artificial Intelligence – A European approach to excellence and trust* della Commissione europea del 19 febbraio 2020. Per un ulteriore approfondimento sul tema, v. S. RUSSEL - P. NORVIG (eds.), *Artificial Intelligence: A Modern Approach*, New York, 2020, pp. 634 ss.; e H. SURDEN, *Machine Learning and Law*, in *Washington Law Review*, 1/2014, pp. 87 ss.

[3] Si pensi al campo delle *self-driving cars*, in cui l'impiego dell'IA potrebbe ridurre notevolmente il rischio di sinistri o al suo impiego in ambito medico, dove, minimizzato il rischio di *bias*, si potrebbe effettuare uno *screening* oncologico più accurato grazie alla diagnostica per immagini dotata di sistemi di IA, utilizzare tecniche di prevenzione di malattie cardiovascolari e ricorrere ai cc.dd. *surgical robotics*. Su quest'ultimo aspetto, v. E. SANTORO, *Intelligenza artificiale in medicina: qual è il suo impatto?*, in *www.marionegri.it*, 28 giugno 2023.

© Wolters Kluwer Italia

simizzazione dei vantaggi e minimizzazione dei rischi. A fronte di un rischio incerto, questo bilanciamento avviene tradizionalmente in base al principio di precauzione in virtù del quale "*la fissazione del livello di protezione prescelto incombe sui responsabili politici e deve tenere conto dei valori che prevalgono in quella società in un determinato momento storico*" [4].

Il legislatore europeo ha trovato questo punto di equilibrio graduando gli obblighi incombenti sui soggetti coinvolti nella produzione e nell'utilizzo di sistemi di IA proprio in base al livello di rischio che questa tecnologia è in grado di ingenerare, introducendo, in particolare, delle regole specifiche per i cc.dd. sistemi ad "*alto rischio*" [5].

Questo scritto, che per ragioni di economicità affronta unicamente gli aspetti relativi ai fatti storici dannosi realizzati con colpa, si ripropone di individuare i relativi nodi da sciogliere [6] e di tentarne una cauta ricostruzione. Segnatamene, alla luce della nuova regolamentazione, ci si chiede che ruolo giochino gli obblighi appena introdotti in eventuali addebiti per colpa e nei confronti dei produttori e nei riguardi dell'utilizzatore. Inoltre, si cerca di capire come far fronte ai problemi che la collaborazione uomo-macchina può causare in relazione all'accertamento della causalità materiale.

2. Condotte colpose

Visto il largo impiego dei sistemi intelligenti nelle attività lecite svolte dall'uomo, è molto probabile che di qui a breve nelle aule dei

---

[4] V. D. Franzone, *Il principio di precauzione in diritto comunitario*, in A. Bianchi - M. Gestri (a cura di), *Il principio precauzionale nel diritto internazionale e comunitario*, Milano, 2006, pp. 8 ss.; A. Massaro, *Principio di precauzione e diritto penale: nihil novi sub sole?*, in *www.penalecontemporaneo.it.*, 9 maggio 2011; F. Giunta, *Il diritto penale e le suggestioni del principio di precauzione*, in *www.discrimen.it*, 19 dicembre 2018; G. Forti, *"Accesso" alle informazioni sul rischio e responsabilità: una lettura del principio di precauzione*, ivi, 18 dicembre 2018, p. 163. Per un inquadramento sociologico, v. per tutti U. Beck, *La società del rischio. Verso una seconda modernità*, Roma, 2013.

[5] Per le regole di classificazione dei sistemi ad alto rischio, v. l'art. 6 dell'*AI Act*.

[6] Nodi che la dottrina penalistica internazionale più esperta in materia ha individuato e sta sciogliendo in questi anni. Il riferimento, rispetto alle questioni di diritto penale sostanziale, è agli interventi tenuti da K. Ligeti - L. Picotti - J. Walther - X. Wang - S. Beck - S. Aires De Sousa - C.E. Japiassù - F. Mirò Linarès - M. Nord-Wagner - A. Gullo - N. Grofu - A. Khalifa, nelle Sezioni I e II, del XXI Congresso internazionale di diritto penale organizzato dall'*Association Internationale de Droit Pénal* (AIDP).

© Wolters Kluwer Italia

tribunali si dovrà stabilire se, e in che misura, possa essere mosso un addebito colposo nei confronti di taluno per un evento nefasto realizzatosi in occasione della collaborazione uomo-macchina.

Si pensi, all'ipotesi paradigmatica delle *self-driving cars*, visti i precedenti [7], o ai casi in cui la tecnologia offra ai medici, e soprattutto alla collettività, strumenti innovativi per migliorare le capacità di diagnosi e di cura [8]. Ma si pensi anche all'attività di produzione e messa in commercio degli stessi sistemi di IA. In queste circostanze potrebbe verificarsi un evento avverso non voluto dal soggetto agente. Ma allora perché è accaduto? E soprattutto, per colpa di chi? [9]

2.1. *Obblighi positivi specifici*

L'*AI Act* ha indirizzato degli obblighi positivi specifici (artt. 8 ss.) agli operatori economici coinvolti nella produzione e nello sviluppo dei sistemi cc.dd. ad "*alto rischio*". Ove questi non dovessero bastare ad evitare eventi avversi, per ragioni di prossimità rispetto all'eventuale causazione di un danno, è rivolto un generale obbligo di "*human oversight*" (art. 14) all'utilizzatore.

Quanto agli obblighi specifici, ci si domanda se si tratta di regole di condotta la cui violazione è idonea ad integrare l'elemento norma-

---

[7] In Florida, una *Tesla modello S* si infilava sotto ad un camion bianco causando la morte del conducente, il 7 maggio 2016; in Arizona, una vettura *Uber* completamente autonoma investiva un pedone, provocandone la morte, il 18 marzo 2018; in California, una donna è stata colpita e uccisa da un veicolo di prova *Uber*, il 23 marzo 2018.

[8] Merita menzione il *software* italiano "THAITI" che nell'ambito dell'*imaging* medico relativo alla risonanza magnetica cardiaca è in grado di calcolare il valore ottimale del c.d. "tempo di inversione", un parametro necessario per l'acquisizione di immagini mirate a identificare l'eventuale presenza di tessuto cicatriziale nel cuore a seguito di somministrazione di un mezzo di contrasto, per un approfondimento: *www.unimib.it/comunicati.*

[9] Per ragioni di completezza, si consideri che sul versante delle fattispecie dolose il quadro giuridico di riferimento potrebbe essere presto innovato nella direzione prospettata dal d.d.l. n. 1146 approvato il 23 aprile 2024 dal CdM. Infatti, l'art. 25 del menzionato d.d.l. n. 1146/2024 si ripropone di introdurre una nuova fattispecie incriminatrice riguardante le condotte integranti il c.d. reato di *deep-fake* nonché una serie di circostanze aggravanti che tengano conto del maggior grado di offensività del reato allorquando venga posto in essere con l'impiego dell'IA. Per quanto concerne invece le condotte assistite dall'elemento soggettivo della colpa, queste non state prese in considerazione nell'atto d'iniziativa legislativa. Per un approfondimento v. S. DE FLAMMINEIS, *Fattispecie penali nel contesto dell'intelligenza artificiale. Lo spunto del d.d.l. 1146/2024*, in *Sist. pen*., 9/2024.

© Wolters Kluwer Italia

tivo della colpa specifica. Sono tutte connotate dalla finalità preventiva di riduzione del rischio o molte di esse hanno una finalità diversa, quella appunto di dettare regole uniformi per il commercio dell'IA nel mercato interno?

Forse, sarebbe prudente affermare che ove dovesse accadere un evento dannoso in occasione della violazione di uno degli obblighi previsti agli artt. 8 ss., andrebbe verificato caso per caso se la regola violata fosse genuinamente connotata da finalità preventiva, cioè che questa fosse finalizzata a ridurre il rischio di verificazione di quello specifico evento e che non fosse, al più, una prescrizione indirizzata agli operatori economici per garantire un *fair play* nel mercato interno. Certo, non è da escludere che alcune regole di condotta possano perseguire contestualmente più di una finalità [10].

Da alcune recenti pronunce di legittimità emerge la tendenza all'abbandono della teoria del c.d. "rischio consentito" in base alla quale la previsione di regole di condotta scritte costituisce un limite alla possibilità di muovere un rimprovero per colpa generica. Rimanendo nel campo delle attività pericolose ma lecite e regolamentate perché socialmente utili, la Suprema Corte di Cassazione in una recente pronuncia in materia di lesioni colpose cagionate nell'esercizio di un'attività sportiva, ha reputato non soddisfacente l'impostazione in base alla quale il limite fra illecito sportivo e illecito penale fosse rappresentato, appunto, dall'area di rischio consentito. Piuttosto, ha ritenuto che lo sportivo di una pratica "di contatto", accanto al dovere di rispettare le regole dello sport intrapreso, sia tenuto al più generale onere di osservanza delle regole cautelari, prudenziali e di diligenza [11].

Non è improbabile che anche per la produzione e messa in circolazione dell'IA, attività regolamentata ora dall'*AI Act,* il rapporto fra colpa specifica e colpa generica sia visto in un'ottica di integrazione piuttosto che di esclusione [12].

---

[10] Il 3° "considerando" indica l'art. 114 TFUE quale base giuridica del regolamento e contestualmente dichiara che è scopo dell'atto tutelare altri interessi pubblici quali la salute, la sicurezza e la protezione dei diritti fondamentali come riconosciuti e tutelati dal diritto dell'Unione.

[11] Cass. pen., sez. IV, 21 ottobre 2021, n. 3284, oltre alla tematica del rischio consentito, si addentra anche sulla dicotomia regole di condotta e regole cautelari; dello stesso segno v. anche, sulla questione del rischio consentito, Cass. pen., sez. IV, 28 ottobre 2021, n. 8609.

[12] Per un approfondimento del rapporto fra colpa generica e colpa specifica v. G. Civello, *Colpa stradale, affidamento e autoresponsabilità: una sentenza esemplare*, *Nota a Cass., sez. IV, sent. 14 dicembre 2023 (dep. 20 dicembre 2023), n. 50816, pres. Piccialli, rel. Mari,* in *Sist. pen.,* 2/2024, p. 42; con riferimento al rapporto tra colpa

© Wolters Kluwer Italia

A ciò si aggiunga che proprio l'*AI Act* offre, in parte, una base normativa per questo tipo di interpretazione. Infatti, l'art. 9, rubricato "*Sistema di gestione dei rischi*", nel suo par. 4, lett. a), impone che i soggetti produttori individuino le misure di gestione del rischio garantendo "*l'eliminazione o la riduzione dei rischi* [per quanto possibile] *attraverso un'adeguata progettazione e fabbricazione*". Pertanto, sarebbe tutt'altro che privo di fondamento ritenere che, quanto meno nel momento in cui sono chiamati ad individuare le misure di gestione del rischio, la condotta dei soggetti che producono e commercializzano i sistemi di IA sia raffrontabile al parametro dell'*homo eiusdem condicionis et professionis,* rendendo ancora più concreta l'ipotesi che il rispetto delle regole cautelari scritte non escluda nei loro confronti un addebito per colpa generica [13].

2.2. *Obbligo di* human oversight

L'art. 9 dell'*AI Act*, al suo par. 4, definisce accettabili i rischi che, nonostante l'adozione delle misure di gestione di cui al par. 2, lett. d), residuano per la salute, la sicurezza e per i diritti fondamentali e prevede che questa circostanza sia comunicata all'utente. Insomma, quando l'IA passa dal soggetto che l'ha prodotta al soggetto che ne fa uso, su quest'ultimo è allocato il rischio incerto residuo. In effetti, in base all'art. 14, è l'utilizzatore ad essere tenuto ad un obbligo di *human oversight* "*in particolare quando tali rischi persistono nonostante l'applicazione di altri requisiti di cui al presente capo*". Ma che ruolo svolge, *rectius* potrebbe svolgere, questo obbligo sul terreno della responsabilità penale? Più schiettamente, l'art. 14 dell'*AI Act* fonda una posizione di garanzia oppure introduce una regola cautelare?

Nel primo caso, in virtù dell'art. 40, co. 2, c.p., l'uomo-supervisore risponderebbe dell'evento dannoso non solo quando lo ha cagionato,

---

generica e colpa specifica nella responsabilità per colpa medica, v. C. CUPELLI, *Lo statuto penale della colpa medica e le incerte novità della legge Gelli-Bianco*, in *Dir. pen. con.,* 4/2017, p. 206, secondo cui: "*[p]iù esauriente – rispetto alle attività rischiose, giuridicamente autorizzate – è la moderna concezione della c.d. duplice dimensione o misura dell'imputazione colposa: a) la dimensione oggettiva, consistendo il primo elemento essenziale nella condotta violatrice della preesistente regola cautelare di condotta, volta a salvaguardare i beni giuridici; b) la dimensione soggettiva, consistendo il secondo elemento essenziale nell'esigibilità dell'osservanza di tale regola da parte dell'agente (e, quindi, nell'attribuibilità al medesimo dell'inosservanza)*".

[13] In questa direzione anche B. FRAGASSO, *La responsabilità penale del produttore di sistemi di intelligenza artificiale*, in *Sist. pen.*, 13 giugno 2023, p. 15.

© Wolters Kluwer Italia

ma anche quando non lo abbia impedito [14]; ove invece si intenda la norma quale fonte di una regola cautelare, l'*human in the loop* [15] sarebbe responsabile se con condotta commissiva colposa ha cagionato il danno.

Potremmo sostenere che il riportato inciso contenuto nell'art. 14, par. 2, lasci intendere che ove diligenza, prudenza e perizia possano ridurre la possibilità di verificazione di rischi ulteriori, queste accortezze debbono essere prestate dal soggetto utilizzatore secondo quanto ci si può ragionevolmente aspettare.

Del resto, con riferimento ai diversi gradi di automazione del sistema in materia di *autonomous driving*, è condivisibile l'opinione in base alla quale si potrebbe rinvenire nell'obbligo di sorveglianza umana la fonte di una posizione di garanzia "*soltanto quando la macchina è del tutto automatica e non quando il contributo umano resta assolutamente necessario*" [16].

V'è da aggiungere che secondo la concezione formale, affinché una certa norma possa essere reputata fonte di una posizione di garanzia, fra gli altri requisiti, essa deve essere dotata di un sufficiente grado di specificità sì da rendere prevedibile per il soggetto agente che il non fare, in un certo contesto, viene equiparato al fare [17]. La dicitura "*human oversight*" non sembra presentare i necessari caratteri di specificità.

Ma in cosa si sostanzia quindi la sorveglianza umana? La sola richiesta di "*human oversight*" suggerisce poco. Sulla scorta di quanto è già accaduto per gli *autonomous vehicles* in Germania e in Francia [18], si potrebbe ragionevolmente ritenere che in questa parte il regolamento

---

[14] Propende per questa ricostruzione L. Picotti, *Categorie tradizionali del diritto penale e intelligenza artificiale: crisi o palingenesi?*, in *Sist. pen.*, 31 luglio 2024.

[15] Espressione traducibile con "l'uomo al centro dell'algoritmo". Per un approfondimento sul tema, v. A. Giannini, *Intelligenza artificiale, human oversight e responsabilità penale,* in *www.discrimen.it*, 21 novembre 2020, p. 16; B. Green - A. Kak, *The false Comfort of human oversight as an antidote to AI*, in *Slate.com*, 15 June 2021.

[16] In base al più diffuso *standard* J3016 della *SAE International* (*Society of Automotive Engineers*), è possibile distinguere sei livelli di automazione complessiva dell'auto automatica da 0 a 5. Per un approfondimento sul tema, v. A. Cappellini, *Profili penalistici delle self-driving cars*, in *Dir. pen. con.*, 2/2019, p. 325.

[17] Nella manualistica tradizionale, v. G. Marinucci - E. Dolcini - G.L. Gatta, *Manuale di Diritto Penale. Parte generale*, IX ed., Milano, pp. 270 ss. Sui requisiti della fonte della posizione di garanzia, v. F. Mantovani - G. Flora, *Diritto Penale. Parte Generale,* XII ed., Padova, p. 160.

[18] In Germania e in Francia il codice della strada è stato modificato dal legislatore per disciplinare le ipotesi in cui il conducente si avvalga di un veicolo a guida semi-autonoma o completamente autonoma.

© Wolters Kluwer Italia

abbia lasciato agli Stati membri la possibilità di disciplinare gli aspetti riguardanti la posizione dell'utilizzatore, il che è apprezzabile, dal momento che il legislatore europeo, giova ribadirlo, è intervenuto sulla base dell'art. 114 TFUE a tutela del mercato interno.

Con tale intervento, avvenuto con una fonte normativa direttamente applicabile, si può dire che questi abbia legiferato nel pieno rispetto dei principi di sussidiarietà e di proporzionalità [19] concentrandosi sulla posizione degli operatori economici ma senza ignorare il ruolo svolto poi in concreto dagli utilizzatori dei sistemi di IA, obbligando anche questi ultimi quanto meno a sorvegliare il sistema di IA quando questo è in uso.

In definitiva, si potrebbe affermare che la prescrizione di "*human oversight*" abbia la natura giuridica di norma cautelare, pur nella sua generalità, ferma restando la possibilità di una futura introduzione di obblighi positivi che specifichino in che cosa consista la sorveglianza dell'utilizzare nel singolo settore di riferimento [20].

Interventi di questo tipo aprirebbero la strada ad un possibile rimprovero per colpa specifica nei riguardi dell'utente-sorvegliante riproponendosi anche rispetto a quest'ultimo le stesse incertezze applicative relative al rapporto fra colpa generica e colpa specifica esaminate in riferimento ai soggetti produttori.

3. Il problema dell'accertamento causale

Non ci sono particolari controindicazioni affinché il tradizionale procedimento di accertamento della causalità materiale possa ritenersi applicabile. Al più, il giudizio causale avverrà secondo le specificità proprie della materia: per la spiegazione del rapporto causa-effetto dovranno essere ricercate le regole di spiegazione scientifica relative al funzionamento dell'IA [21]. Tuttavia, il rinvio al funzionamento dei sistemi di IA causa qualche incertezza.

In primo luogo, il fatto che l'IA possa essere dotata di un più o meno spiccato livello di autonomia nel *decision making process* comporta l'eventualità che l'evento dannoso verificatosi in occasione della

[19] Principi previsti dall'art. 5 TUE, rispettivamente ai parr. 3 e 4.

[20] Risvolto auspicato da S. BECK - S. GERNDT, *German report on traditional criminal law categories and AI*, in L. PICOTTI - B. PANATTONI (eds.), *Traditional Criminal Law Categories and AI: Crisis or Paligenesis?*, Verona, 2023.

[21] L. PICOTTI, *Categorie tradizionali del diritto penale e intelligenza artificiale*, cit., p. 9.

© Wolters Kluwer Italia

collaborazione uomo-macchina possa essere causalmente legato ad un *output* del sistema non esattamente corrispondente all'*input* ricevuto dall'utilizzatore-sorvegliante [22]. In altre parole, si deve tenere in considerazione il fenomeno della *black box*, cioè le incertezze legate alla ricostruzione dei passaggi compiuti dal sistema. Questi, infatti, potrebbero non essere totalmente ripercorribili attraverso un giudizio controfattuale compiuto *ex post*.

Tuttavia, ciò "*non preclude di per sé la possibilità d'imputazione oggettiva, secondo criteri normativi che sono – almeno metodologicamente – da tempo condivisi, non occorrendo mai la spiegazione di ogni singolo passaggio della catena causale da cui si produce l'evento finale, potendo soccorrere anche correlazioni statistiche od ipotetiche ragionevolmente plausibili*" [23].

4. Un possibile scenario: tra colpa dell'utilizzatore e *responsibility gap*

Quando dall'uso di una macchina che non presenta malfunzionamenti deriva un evento dannoso, questo potrebbe essere riconducibile ad una insufficiente sorveglianza da parte del soggetto utilizzatore [24]. Se si volesse portare a conseguenze la ricostruzione dell'obbligo di *human oversight* di cui all'art. 14 del regolamento quale norma cautelare, intanto il danno sarà attribuibile al soggetto sorvegliante in quanto, al posto suo, l'agente modello lo avrebbe previsto ed evitato. Infatti, si potrebbe osservare che molto spesso ciò che sembra in linea di principio meglio conoscibile da chi programma e costruisce una certa cosa, sia in realtà più familiare a chi si cimenta quotidianamente nel suo uso. Questa riflessione può valere tanto per il *driver* mediamente esperto che in certe condizioni di tempo e di luogo sa quali imprevisti possono rilevarsi di difficile gestione se la guida dell'auto è in modalità semiautonoma, quanto per il medico mediamente esperto che abbia alle spalle una casistica tale da permettergli di rendersi conto che l'*output* prodotto dalla macchina perfettamente conforme ai requisiti richiesti dall'*AI Act*, in quel caso specifico non è calzante.

In sede di accertamento della responsabilità colposa, bisogna veri-

---

[22] Il riferimento è al *machine learning*, per il quale si rimanda alla nota n. 2.

[23] L. Picotti, *Categorie tradizionali del diritto penale e intelligenza artificiale*, cit., p. 9.

[24] Anche l'*AI Act* all'art. 14, par. 4, lett. b), prende in considerazione il rischio di *overreliance* da parte dell'utilizzatore sull'*output* prodotto dal sistema di IA.

© Wolters Kluwer Italia

ficare che il *driver*-agente modello o il medico-agente modello, al posto delle persone concretamente coinvolte, avrebbero previsto ed evitato l'evento in base al grado di competenza ed esperienza che ci si può ragionevolmente attendere. Se così non fosse, l'evento dannoso non sarebbe attribuibile né alla catena di sviluppo del sistema intelligente, essendo lo stesso perfettamente funzionante, né al sorvegliante, avendo egli prestato l'accortezza possibile. Questa è l'ipotesi in cui un fatto dannoso penalmente rilevante non è ascrivibile a nessuna persona fisica. Allo stato dell'arte, il c.d. *responsibility gap* [25] è un rischio congenito all'impiego dell'IA nelle attività lecite con cui il legislatore e i tribunali non hanno ancora fatto i conti.

5. Considerazioni conclusive

Forse un giorno l'ipotesi di una responsabilità diretta dell'IA [26] diventerà realtà. Fino ad allora, quello che ci si augura è che la presa sul principio di personalità della responsabilità penale resti ben salda e che nonostante la tendenza dell'animo umano sia, per natura, quella di cercare qualcuno cui attribuire la responsabilità di un evento nefasto, il legislatore sappia trovare il punto di equilibrio fra costi e benefici derivanti dall'impiego dell'IA senza trasmodare dal principio di precauzione al "precauzionismo" [27].

---

[25] Per un approfondimento sul tema, v., per tutti, F. SANTONI DE SIO - G. MECACCI, *Four responsibility gaps with Artificial Intelligence, Why they matter and how to address them*, in *Philosophy and technology*, 4/2021.

[26] Per tutti, v. R. ABBOT - A. SARCH, *Punishing Artificial Intelligence: Legal Fiction or Science Fiction?*, in *UC Davis Law Review*, 1/2019, pp. 323 ss., disponibile su: *papers.ssrn.com.*

[27] Per un'analisi dei pericoli connessi al "precauzionismo", v. A. MASSARO, *Op. cit*.

© Wolters Kluwer Italia

LA RESPONSABILITÀ DELLE DECISIONI AMMINISTRATIVE AUTOMATIZZATE *

FEDERICA PALOMBA

SOMMARIO: 1. L'uso della tecnologia dalla fase istruttoria alla fase decisoria dell'attività amministrativa: vantaggi e rischi. – 2. La soggettività delle decisioni. – 3. La riserva di umanità nell'organizzazione amministrativa. – 4. L'effettività del controllo amministrativo sulle decisioni automatizzate.

Abstract: This paper aims to examine the administrative power in the context of algorithmic decision-making. It focuses on human oversight obligations and possible legal remedies to overcome the opacity of the AI systems. The general principles of transparency and reasoning remain crucial in order to guarantee a balance between technical efficiency and responsibility of the Public Administration.

1. L'uso della tecnologia dalla fase istruttoria alla fase decisoria dell'attività amministrativa: vantaggi e rischi

L'utilizzo della tecnologia nelle decisioni pubbliche contribuisce alla realizzazione degli obiettivi di efficienza ed economicità dell'azione amministrativa, in applicazione del principio costituzionale del buon andamento [1].

---

* Contributo sottoposto a doppio referaggio in forma anonima.

[1] F. CARDARELLI, *L'uso della telematica*, *Commento dell'art. 3-bis della legge n. 241 del 1990*, in M.A. SANDULLI (a cura di), *Codice dell'azione amministrativa*, Milano, 2017, p. 509; F. COSTANTINO, *Uso della telematica nella pubblica amministrazione*, in A. ROMANO (a cura di), *L'azione amministrativa*, Torino, 2016, p. 242; S. DETTORI, *Articolo 3-bis. Uso della Telematica*, in N. PAOLANTONIO - A. POLICE - A. ZITO (a cura

© Wolters Kluwer Italia

Il rapporto strumentale tra tecnologia e interesse pubblico emergeva già nel 1979, quando, nella relazione al Parlamento, Massimo Severo Giannini evidenziava che "*gli elaboratori elettronici, che erano all'inizio apparecchi di semplice registrazione di dati complessi, sono divenuti poi apparecchi di accertamento e verificazione, di calcolo, di partecipazione a fasi procedimentali di istruttoria, e infine di decisione*" [2].

Oltre quarant'anni dopo, la linea evolutiva tracciata resta attuale. È necessario, quindi, approfondire come l'uso della tecnologia nelle decisioni finali vada declinato con le ordinarie regole di responsabilità.

Nella fase istruttoria, l'algoritmo rappresenta una regola tecnica presupposta e servente rispetto alla valutazione amministrativa [3]: seguendo lo schema ipotetico "*if-then*", il *computer* esegue istruzioni umane al ricorrere di condizioni predeterminate [4].

Le nuove tecnologie consentono inoltre, oggi, di elaborare decisioni autonome, astrattamente in grado di sostituirsi al provvedimento [5], anche di natura discrezionale [6].

L'estensione dell'uso della tecnologia dalla fase istruttoria a quella decisoria segna un passaggio cruciale, vantaggioso in termini di efficienza e celerità, ma anche rischioso per la tutela degli interessati e per la stessa effettività dell'intervento pubblico.

---

di), *La pubblica amministrazione e la sua azione: saggi critici sulla legge n. 241/1990 riformata dalle leggi n. 15/2005 e n. 80/2005*, Torino, 2005, p. 173; A. MASUCCI, *L'atto amministrativo informatico. Primi lineamenti di una ricostruzione*, Napoli, 1993.

[2] Per un inquadramento del "*Rapporto sui principali problemi dell'Amministrazione dello Stato*", presentato nel 1979 alle Camere dal Ministro per la Funzione Pubblica Giannini, cfr. G. MELIS, *Storia dell'amministrazione italiana 1861-1993*, Bologna, 1996.

[3] TAR Lazio-Roma, Sez. III-*bis*, 19 settembre 2018, n. 9230.

[4] V. NERI, *Diritto amministrativo e intelligenza artificiale: un amore possibile*, in *Urbanistica e appalti*, 5/2021, p. 581.

[5] Nella legislazione settoriale emergono diversi casi in cui la decisione è automatizzata, come le aste elettroniche e le gare telematiche, le sanzioni del Codice della strada, le procedure concorsuali preselettive. Per una rassegna v. G. AVANZINI, *Decisioni amministrative e algoritmi informatici. Predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Napoli, 2019.

[6] L'orientamento iniziale escludeva il ricorso alla decisione automatizzata nell'attività discrezionale della P.A. Il Consiglio di Stato, a partire dalle sentenze 13 dicembre 2019, n. 8472 e 4 febbraio 2020, n. 881, ha affermato che non vi sono ragioni "*per limitare l'utilizzo all'attività amministrativa vincolata piuttosto che discrezionale, entrambe espressione di attività autoritativa svolta nel perseguimento del pubblico interesse*". Per un esame sull'impiego dell'IA nelle decisioni discrezionali, A. POLICE, *Scelta discrezionale e decisione algoritmica*, in R. GIORDANO - A. PANZAROLA - A. POLICE - S. PREZIOSI - M. PROTO (a cura di), *Il diritto nell'era digitale: persona, mercato, amministrazione, giustizia*, Milano, 2022.

© Wolters Kluwer Italia

Non sempre, infatti, soprattutto nelle tecnologie fondate sulla rielaborazione dei dati e sull'adeguamento progressivo ai fenomeni conosciuti, è agevole ricostruire l'*iter* logico della scelta automatizzata [7] e la correlazione tra *input* e *output* [8].

Il bilanciamento tra vantaggi e rischi non può che essere garantito dall'interazione della macchina con l'essere umano [9]. Imputazione e responsabilità dell'atto alla P.A. costituiscono, quindi, le condizioni di ammissibilità dei processi di digitalizzazione dell'attività amministrativa [10].

2. La soggettività delle decisioni

Il principale problema della tutela del danneggiato dall'errore della tecnologia ruota intorno all'adeguatezza dei criteri di imputazione della responsabilità [11].

Il quadro normativo vigente, anche nel diritto civile, non è sufficiente a determinare la responsabilità per i danni causati da un *robot*, in quanto non consente di identificare il soggetto imputabile, né di esigere da tale soggetto la riparazione dei danni causati [12].

Resta prematuro il riconoscimento di una personalità giuridica autonoma, in ragione dell'impossibilità di riferire alla macchina una capacità di intendere e volere [13], alla luce dei concetti di diritto naturale di coscienza e libero arbitrio, e in ragione dell'assenza di un patrimonio separato aggredibile ai fini del risarcimento del danno [14].

---

[7] D.U. Galetta - J.G. Corvalán, *Intelligenza Artificiale per una pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it*, 3/2019.

[8] È la c.d. "*black box*". V., sul punto, F. Pasquale, *The Black Box Society. The secret algorithms that control money and information*, London, 2015.

[9] Cons. St., Sez. VI, 4 febbraio 2020, n. 881, richiama il modello matematico *human in the loop*, affermando che "*è necessario che la macchina interagisca con l'essere umano*".

[10] V. Neri, *Op. cit.*, p. 591.

[11] Per una ricostruzione in ambito civilistico, cfr. T. De Mari Casareto dal Verme, *Intelligenza artificiale e responsabilità civile. Uno studio sui criteri di imputazione*, Napoli, 2024; C. Scognamiglio, *Responsabilità civile ed intelligenza artificiale: quali soluzioni per quali problemi?*, in *Resp. civ. prev.*, 4/2023, p. 1082.

[12] Carta della Robotica, risoluzione del Parlamento europeo del 16 febbraio 2017.

[13] G. Pesce, *Funzione amministrativa, intelligenza artificiale e blockchain*, Napoli, 2021.

[14] Il rischio di una deresponsabilizzazione del programmatore, del produttore, del proprietario o dell'utilizzatore è evidenziato da U. Ruffolo, *La "personalità elettroni-*

© Wolters Kluwer Italia

Occorre dunque individuare quale soggetto, tra l'utilizzatore o "custode" della tecnologia, ovvero l'ideatore dell'algoritmo, sia responsabile per i danni cagionati e possa essere direttamente citato in giudizio dal danneggiato.

In assenza di regole specifiche, la dottrina civilistica ha ipotizzato una responsabilità oggettiva in capo ai produttori di sistemi informatici, secondo il modello dell'art. 2050 c.c., o della responsabilità, di matrice eurounitaria [15], per danno da prodotti difettosi.

Nel diritto amministrativo, tuttavia, l'individuazione della responsabilità per danni provocati dalla tecnologia non può prescindere dall'imputazione delle decisioni unicamente alla Pubblica Amministrazione.

Il regime di responsabilità delineato dalla Costituzione, nel solco del principio di legalità nell'attribuzione del potere, presuppone la personalizzazione dei rapporti con il cittadino e l'imputazione dell'attività a singoli funzionari e, in virtù del rapporto di immedesimazione organica, all'Amministrazione [16].

L'art. 28 Cost. sancisce la responsabilità civile diretta dell'Amministrazione per i danni cagionati dai propri funzionari [17], i quali non assumono soggettività autonoma, ma sono chiamati a esprimere la capacità di agire della P.A.

In materia di decisioni algoritmiche, la giurisprudenza afferma senza riserve che la volontà imputabile all'Amministrazione deve necessariamente provenire da un essere umano [18].

---

ca", in U. RUFFOLO (a cura di), *Intelligenza artificiale: il diritto, i diritti, l'etica,* Milano, 2020, p. 214, secondo il quale "*responsabilizzare la macchina, ed essa sola, comporterebbe, di fatto, la limitazione della responsabilità patrimoniale ad uno specifico patrimonio di rischio*". Cfr., sul punto, anche G. ALPA, *L'intelligenza artificiale. Il contesto giuridico*, Modena, 2021.

[15] La disciplina remediale della responsabilità per danno da prodotti difettosi è da ultimo richiamata nel regolamento (UE) 2024/1689, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale.

[16] M.C. CAVALLARO, *Imputazione e responsabilità delle decisioni amministrative automatizzate*, in *European Review of Digital Administration & Law-Erdal*, 1/2020, p. 69.

[17] Cass. Civ., Sez. III, 10 maggio 2005, n. 9741, secondo cui "*[l]'art. 28 della Costituzione, nel sancire che i funzionari e i dipendenti dello Stato sono «direttamente» responsabili degli atti compiuti in violazione di diritti, non postula un'antinomia fra responsabilità diretta (e cioè ricollegata a fatto proprio) e responsabilità indiretta (scaturente, cioè, da fatto altrui), volendo, viceversa, intendere soltanto che essi rispondono «personalmente» di tali atti, senza che ciò elida la responsabilità dell'Amministrazione*". Più di recente, Cass. Civ., Sez. III, 5 novembre 2018, n. 28079; Cass. Civ., SS.UU., 9 marzo 2020, n. 6690.

[18] Cons. Stato, Sez. VI, 13 dicembre 2019, n. 8472: "*sul versante della verifica*

© Wolters Kluwer Italia

Un'interpretazione alternativa propone di estendere la teoria dell'immedesimazione all'intelligenza artificiale, la quale opererebbe alla stregua di un "*organo virtuale*" [19], titolare di una specifica competenza delegata [20].

In questo modo, il vizio o il pregiudizio dell'algoritmo è comunque imputabile all'organo e la responsabilità resta ascritta al funzionario umano, non diversamente dai casi in cui cagioni danni con altre risorse materiali o finanziarie in dotazione all'ufficio. Resta salva, in ogni caso, la configurabilità di una responsabilità erariale in capo ai soggetti privati che progettano o forniscono le tecnologie all'Amministrazione [21].

Al di là della mutuabilità, sotto il profilo teorico, dell'immedesimazione organica, il principio personalista impone di considerare l'Amministrazione quale unico centro di imputazione e fonte di responsabilità diretta dei danni cagionati dalle decisioni algoritmiche.

Si applicheranno, pertanto, le regole ordinarie in tema di responsabilità civile [22] per il danno prodotto a terzi dall'illecito della P.A. e amministrativo-contabile per danno erariale.

---

degli esiti e della relativa imputabilità deve essere garantita la verifica a valle, in termini di logicità e di correttezza degli esiti. Ciò a garanzia dell'imputabilità della scelta al titolare del potere autoritativo, individuato in base al principio di legalità, nonché della verifica circa la conseguente individuazione del soggetto responsabile".

[19] E. Picozza, *Politica, diritto amministrativo and* Artificial Intelligence, in *Giur. it.*, 7/2019, p. 1763.

[20] N. Paolantonio, *Il potere discrezionale della pubblica automazione. Sconcerto e stilemi (sul controllo giudiziario delle "decisioni algoritmiche")*, in *Dir. amm.*, 4/2021, pp. 813 e ss.; P. Forte, *Diritto Amministrativo e Data Science. Appunti di intelligenza amministrativa artificiale (AAI)*, in *Persona e Amministrazione*, 1/2020, p. 285.

[21] Sulla responsabilità erariale da servizio algoritmico, P. Del Vecchio - V. Bignoli, *Le responsabilità amministrative da algoritmo e intelligenza artificiale. La responsabilità da provvedimento algoritmico sia ai fini del risarcimento del danno in sede civilistica che in sede contabile come responsabilità erariale*, in A. Pajno - F. Donati - A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?,* vol. II, *Amministrazione, responsabilità, giurisdizione*, Bologna, 2022, p. 341.

[22] Il riferimento è al modello generale dell'art. 2043 c.c., senza escludere la responsabilità per attività pericolosa dell'art. 2050 c.c. e da cosa in custodia dell'art. 2051 c.c. Sul punto, U. Ruffolo, *La responsabilità da* artificial intelligence*, algoritmo e* smart product*: per i fondamenti di un diritto dell'intelligenza artificiale* self-learning, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, p. 93.

© Wolters Kluwer Italia

3. La riserva di umanità nell'organizzazione amministrativa

Al fine di rendere compatibile il processo di digitalizzazione dell'attività amministrativa con le garanzie ineludibili del diritto amministrativo, le decisioni assunte mediante automazione rispettano i principi di: *a*) conoscibilità e comprensibilità, per cui l'interessato ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino e, in tal caso, a ricevere informazioni significative sulla logica utilizzata; *b*) non esclusività della decisione algoritmica [23], per cui comunque esiste nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatizzata; *c*) non discriminazione algoritmica, per cui il titolare mette in atto misure tecniche e organizzative adeguate al fine di impedire effetti discriminatori nei confronti degli operatori economici.

Nel solco della dottrina e della giurisprudenza in materia di decisioni automatizzate, tali principi sono oggi espressamente recepiti nel Codice dei contratti pubblici [24].

I tre canoni enunciati costituiscono le garanzie di legalità algoritmica, per cui la decisione automatizzata costituisce uno strumento organizzativo che non comporta una delega di potere [25].

La regola tecnica che governa ciascun algoritmo resta pur sempre una regola amministrativa generale, costruita dall'uomo e non dalla macchina, per essere poi (solo) applicata da quest'ultima [26].

Secondo l'assetto attuale, l'algoritmo rappresenta un mezzo a sostegno dell'attività amministrativa, inidoneo a esprimere la decisione

---

[23] Il primo ancoraggio normativo del principio di non esclusività è rappresentato dall'art. 22 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), secondo il quale "*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato*".

[24] M. FAVIERE, *Art. 30-Uso di procedure automatizzate nel ciclo di vita dei contratti pubblici*, in R. GIOVAGNOLI - G. ROVELLI (a cura di), *Codice dei contratti pubblici*, Milano, 2024, pp. 322 ss.; G.M. RACCA, *Trasformazioni e innovazioni digitali nella riforma dei contratti pubblici*, in R. CAVALLO PERINI - M. LIPARI - G.M. RACCA, *Contratti pubblici e innovazioni nel nuovo Codice. Trasformazioni sostanziali e processuali*, Napoli, 2024.

[25] L. TORCHIA, *Lo Stato digitale. Una introduzione*, Bologna, 2023; ID., *Lo Stato digitale e il diritto amministrativo*, in *Liber Amicorum per Marco D'Alberti*, Torino, 2022.

[26] A. POLICE, *Scelta discrezionale e decisione algoritmica*, in R. GIORDANO - A. PANZAROLA - A. POLICE - S. PREZIOSI - M. PROTO (a cura di), *Op. cit.*, p. 499.

© Wolters Kluwer Italia

in via definitiva. In questa prospettiva, non occorrerebbe nemmeno una fonte regolamentare che disciplini il ricorso all'algoritmo, riducendosi il relativo apporto a una scelta di tipo organizzativo propria dell'Amministrazione [27].

L'art. 12 del d.lgs. 7 marzo 2005, n. 82, recante il Codice dell'Amministrazione digitale, stabilisce, in via generale, che la P.A. deve "*organizzare autonomamente*" la propria attività, servendosi delle nuove tecnologie [28]. È così garantita una base legale per la scelta di ricorrere all'algoritmo *ex ante*, ma manca una disciplina volta a precisare i confini e l'intensità del controllo esercitato *ex post* dal responsabile umano del procedimento.

4. L'effettività del controllo amministrativo sulle decisioni automatizzate

La necessità di garantire la sorveglianza umana sul risultato della decisione algoritmica impone di interrogarsi sul tipo di controllo spettante al dirigente o al funzionario amministrativo responsabile del procedimento.

Occorrerebbe precisare, anzitutto, se esso sia interamente devolutivo, ovvero limitato alla non manifesta irragionevolezza dell'esito stesso.

Appare subito il caso di escludere che sia esigibile un controllo sostitutivo, esteso all'intera istruttoria e a tutti i profili di discrezionalità e di opportunità che il provvedimento richiede di valutare. Il riesame umano del risultato informatico, infatti, azzererebbe i vantaggi di celerità ed efficienza perseguiti con la scelta di automatizzare la procedura [29].

Il problema dell'efficacia del controllo umano sull'esito della procedura automatizzata si è posto, peraltro, anche negli altri ordinamenti. In Francia, il *Conseil d'État* ha suggerito di specificare a livello legislativo che l'intervento umano deve essere sostanziale e non solo for-

---

[27] S. Foà, *Intelligenza artificiale e cultura della trasparenza amministrativa. Dalle "scatole nere" alla "casa di vetro"?*, in *Dir. amm.*, 3/2023, p. 515.

[28] Sulla limitata considerazione dell'organizzazione amministrativa nella prospettiva dei rapporti con i terzi, cfr. A. Police, *Il principio di responsabilità*, in M. Renna - F. Saitta (a cura di), *Studi sui principi del diritto amministrativo*, Milano, 2012, p. 223.

[29] N. Durante, *Brevi considerazioni in tema di amministrazione algoritmica e di giustizia predittiva*, in *www.giustizia-amministrativa.it*, 2024.

© Wolters Kluwer Italia

male e, quindi, di stabilire con un successivo strumento di *soft law* i criteri per garantire l'effettività del controllo [30].

In primo luogo, la persona preposta deve essere in grado di "*comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese*" [31]. In questi termini, si richiede una diligenza qualificata dei dipendenti pubblici, con conseguenti profili di *culpa in eligendo* in capo a chi abbia nominato un soggetto privo della professionalità richiesta e di *culpa in vigilando* qualora il responsabile ometta di individuare e affrontare tempestivamente le anomalie nella fase del monitoraggio [32].

Andrebbe quindi promosso uno sviluppo delle competenze interne al fine di assicurare una maggiore padronanza della tecnologia. Si ipotizza, al riguardo, l'introduzione di procedure o linee guida di *Algorithmic Impact Assessment*, che orientino i funzionari pubblici sulla scelta, a monte, di ricorrere all'intelligenza artificiale, sui vantaggi e i rischi connessi ai diversi sistemi utilizzati e sulle implicazioni in termini di responsabilità [33].

Più delicata è la perimetrazione del controllo successivo al risultato ottenuto, che implica un affidamento sull'*output* prodotto dal sistema automatico. La valutazione della legittimità dell'affidamento riposto si scontra con la naturale deferenza del funzionario nei confronti di un procedimento automatizzato predisposto da un soggetto qualificato, vista la sproporzione delle cognizioni tecniche tra chi ha impostato lo strumento tecnologico e chi è chiamato a recepirne i risultati. Il rischio è che il funzionario tenda a conformarsi al risultato informatico, limi-

---

[30] CONSEIL D'ÉTAT, *Le numérique et les droits fondamentaux*, Paris, 2014, p. 343. Successivamente, è stato previsto un ricorso amministrativo, dinanzi a un decisore umano, avverso la decisione automatizzata. V., sul punto, *Conseil Constitutionnel*, n. 2018-765, riportata da S. TRANQUILLI, *Rapporto pubblico-privato nell'adozione e nel controllo della decisione amministrativa algoritmica*, in *Dir. soc.*, 2/2020, p. 281.

[31] Art. 14, co. 4, del regolamento (UE) 2024/1689 sull'intelligenza artificiale. La nozione di "persona dedicata" o "*deployer*" è definita, al 13° "considerando", come "*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*".

[32] S. FOÀ, *Op. cit.*, p. 527.

[33] B. MARCHETTI, *La garanzia dello Human in the Loop alla prova della decisione amministrativa algoritmica*, in *BioLaw Journal*, 2/2021, p. 367.

© Wolters Kluwer Italia

tandosi a una supervisione solo apparente e a un contributo solo formale alla riserva di umanità [34].

Al fine di individuare un punto di equilibrio tra automazione e umanità, la dottrina ha avanzato una soluzione fondata sull'art. 6, co. 1, lett. e), della l. 7 agosto 1990, n. 241, il quale impone un obbligo di motivazione rafforzata qualora l'organo competente per l'adozione del provvedimento finale intenda discostarsi dalle risultanze dell'istruttoria.

Il funzionario è quindi tenuto, di regola, a recepire il risultato algoritmico nel contenuto del provvedimento finale, salva la possibilità di discostarvisi previa specifica motivazione, prescritta a pena di illegittimità [35].

L'automazione della fase procedimentale sarebbe ammissibile e rispettosa della riserva di umanità solo se compensata dalla garanzia di un controllo sulla motivazione, ispirato a criteri della *full jurisdiction* [36].

Il controllo umano riguarda quindi l'attendibilità dell'*output*, tenendo conto che l'algoritmo è fallibile e può dare "*esiti abnormi, irragionevoli o illogici, con necessità di una correzione della base casistica (*data lake*) o delle variabili o delle regole assunte con l'algoritmo*" [37].

Del resto, il Giudice Amministrativo, esigendo le garanzie di trasparenza e conoscibilità dell'algoritmo, rivendica il proprio sindacato sull'algoritmo e sulla correttezza di tutti i passaggi della procedura informatica [38]. Tale controllo, *a fortiori*, deve poter essere esercitato ancor prima, nel corso del procedimento, dalla stessa Amministrazione [39].

I funzionari pubblici sono tenuti a correggere la decisione informatica: nel caso di attività vincolata la revisione riguarda le variabili

---

[34] D. Simeoli, *L'automazione dell'azione amministrativa nel sistema delle tutele di diritto pubblico*, in A. Pajno - F. Donati - A. Perrucci (a cura di), *Op. cit.*

[35] A. Cassatella, *La discrezionalità amministrativa nell'età digitale*, in Aa.Vv., *Diritto amministrativo: scritti per Franco Gaetano Scoca*, vol. I, Napoli, 2021, p. 675.

[36] A conclusione di uno studio sulla riserva di umanità, G. Gallone, *Riserva di umanità e funzioni amministrative,* Milano, 2023, afferma l'esigenza di recuperare, con un controllo giurisdizionale pieno, le garanzie fisiologicamente sacrificate nel corso del procedimento automatizzato.

[37] R. Cavallo Perin, *Ragionando come se la digitalizzazione fosse data*, in *Dir. amm.*, 2/2020, p. 323.

[38] Cons. St., Sez. VI, 8 aprile 2019, n. 2270.

[39] M.C. Cavallaro, *Op. cit.*, p. 73.

© Wolters Kluwer Italia

selezionate; nel caso di attività discrezionale il controllo avverrà nei limiti del giudizio di logicità e ragionevolezza [40].

L'intervento umano sull'algoritmo si sostanzia quindi, essenzialmente, nel vaglio di ragionevolezza, che assicuri la coerenza del risultato ottenuto con la decisione da assumere nell'interesse pubblico.

In conclusione, è possibile contenere i rischi legati alla fallibilità dell'algoritmo con l'applicazione delle garanzie di trasparenza del procedimento amministrativo, reputando irrinunciabile un intervento umano capace di controllare, validare ovvero smentire la decisione automatizzata.

Le nuove tecnologie consentono, in astratto, di elaborare decisioni autonome, ma mai sostitutive del potere pubblico, improntato alla personalizzazione dei rapporti tra Amministrazione e cittadino [41].

---

[40] R. CAVALLO PERIN, *Op. cit.*, p. 323.

[41] I.M. MARINO, *Prime considerazioni su diritto e democrazia*, in E. FOLLIERI - L. IANNOTTA (a cura di), *Scritti in ricordo di Francesco Pugliese*, Napoli, 2010, p. 165, nel tracciare l'evoluzione storica del modello di Stato, sottolinea la progressiva personalizzazione del rapporto con il cittadino, evidenziando che "*la Costituzione repubblicana paleserà e consoliderà [...] la personalizzazione dei rapporti fra chi svolge funzioni pubbliche ed i cittadini, con le relative conseguenze giuridiche: a partire dall'art. 28, con la responsabilità diretta dei funzionari e dipendenti pubblici secondo le leggi penali, civili e amministrative, per gli atti compiuti in violazione di diritti. E con l'articolo 97, comma 2, secondo cui nell'ordinamento degli uffici sono determinate le competenze e le responsabilità proprie dei funzionari, ma anche lo stesso art. 67, secondo il quale ad esercitare le funzioni senza vincolo di mandato e a rappresentare la Nazione non è il Parlamento, ma «Ogni membro del Parlamento»*".

© Wolters Kluwer Italia

I CRITERI DI IMPUTAZIONE DELLA RESPONSABILITÀ DA REATO DEGLI AGENTI NON UMANI: *MACHINA DELINQUERE POTEST*? *

ARIANNA GIACCHINO

SOMMARIO: 1. Premessa. – 2. Sull'imputazione diretta della responsabilità penale. – 3. Sull'imputazione indiretta della responsabilità penale. – 3.1. La causalità materiale. – 3.2. La colpevolezza. – 3.3. Le posizioni di garanzia. – 4. Considerazioni conclusive.

Abstract: The purpose of this paper is to understand whether the current criteria for the indictment of criminal liability may, hypothetically speaking, be considered eligible in case of a criminal offense where the perpetrator is an AI system. The development of new technologies has led to the advent of AI systems capable of acting autonomously, namely able to make and implement their own decisions, which cannot be foreseen by their programmers since they cannot be traced back to previously given commands; hence, it becomes appropriate to rethink the theory of liability to the purpose of take into consideration the decision-making autonomy margin available to the AI systems. As of today, considering that the new intelligences seem capable of learning and making decisions independently, regardless of the contribution of their own creators, a new question comes to mind: *machina delinquere potest*? Even assuming that an affirmative answer can be given, the interpreter would be at a crossroad: to solve the problem of the indictment by means of traditional institutions (and, in particular, through the position of guarantee and culpable cooperation), although remodeled according to the specifics of the case, or to resort to the introduction of new legal categories, going so far as to suppose the existence of the legal personality of the IA. In the end, in

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

consideration of the relentless progress of the AI in our legal system and due to the silence of the Legislator in relation thereof, the purpose is now to identify viable solutions in a criminal system of law essentially built on the pillar of the personal and culpable reprimand.

1. Premessa

Con il presente contributo ci si propone di indagare se gli attuali criteri di ascrizione della responsabilità penale possano, in ipotesi, ritenersi applicabili a fattispecie penalmente rilevanti nelle quali la condotta venga posta in essere da un sistema di IA che agisce quale autore nella commissione del reato.

Lo sviluppo di nuove tecnologie ha condotto all'avvento di sistemi di IA capaci di agire in autonomia, assumendo ed attuando decisioni proprie, non prevedibili dai loro programmatori in quanto tali azioni non sono riconducibili a comandi precedentemente impartiti; di talché, si rende opportuno vagliare la tenuta della teoria della responsabilità, di modo da ricomprendervi il margine di autonomia decisionale di cui dispongono i sistemi di IA.

In particolare, in via ricostruttiva, ci si chiede se: *i*) sia possibile parlare di una vera e propria capacità di agire, giuridicamente rilevante, in capo ai sistemi di IA, sulla quale basare una loro diretta responsabilità penale; *ii*) possa esser mosso un rimprovero, da un lato, coerente con la nozione personalistica di colpevolezza, dall'altro, in assenza di una "persona" da risocializzare mediante la pena; *iii*) sia possibile parlare di una responsabilità penale indiretta con riferimento alle persone o alle entità giuridiche nel cui interesse o vantaggio agisce il sistema di IA.

Tracciando un parallelismo, simili quesiti erano in precedenza sorti in relazione all'introduzione nel nostro ordinamento della *corporate liability*; quesiti risolti con l'introduzione di un apposito corpo normativo (come noto, il d. lgs. 8 giugno 2001, n. 231) sulla scorta del quale si era giunti all'affermazione per la quale *societas delinquere potest*.

Ad oggi, avendo riguardo alla circostanza per la quale le nuove intelligenze sembrano essere in grado di apprendere e decidere autonomamente, indipendentemente dal contributo del suo ideatore, viene in rilievo un nuovo quesito: *machina delinquere potest*?

Pur ammettendo che possa rispondersi in senso affermativo, l'in-

© Wolters Kluwer Italia

terprete si troverebbe dinanzi ad un bivio: risolvere il problema dell'imputazione mediante l'utilizzo degli istituti tradizionali, in specie quelli della causalità, della colpa, delle posizioni di garanzia, della responsabilità da reato delle persone giuridiche benché rimodulati secondo le peculiarità del caso, ovvero ricorrere all'introduzione di nuove categorie giuridiche, spingendosi sino ad ipotizzare una personalità giuridica dell'IA.

L'approccio penalistico tradizionale sembra entrare in crisi: il paradigma della responsabilità vicaria o indiretta proprio delle ipotesi in cui vengono in rilievo azioni compiute da *res mechanicae* vacilla tanto da giungere a domandarsi se, a fronte di sistemi di IA ontologicamente imprevedibili, sia compito del diritto penale, da sempre imperniato su una logica ascrittiva classificatoria, offrire risposte ai numerosi quesiti.

Delimitando il campo d'indagine, il tema dell'allocazione della responsabilità penale oggetto del presente lavoro prescinderà dall'esame dei sistemi di IA sottoposti al controllo umano [1] (per i quali, sebbene con qualche difficoltà, sembrano esser state raggiunte adeguate soluzioni), per focalizzarsi sugli algoritmi di *machine learning* che, pur non replicando le fattezze del sistema cognitivo umano, sono tuttavia in grado di implementare la propria *performance* quanto ai compiti futuri, dopo avere osservato la realtà [2].

Ci si propone, in via preliminare, di chiedersi se possa ritenersi ammissibile una capacità di agire penalmente rilevante e, in caso di risposta affermativa, quale armamentario sanzionatorio possa conseguire al riconoscimento di una responsabilità diretta della macchina.

In caso di risposta negativa, invece, occorrerà domandarsi quali siano i criteri di attribuzione della responsabilità penale alle persone, fisiche e giuridiche, che "stanno dietro" ai sistemi di IA e come ven-

---

[1] Materia sulla quale, da ultimo, è stato presentato dal Presidente del Consiglio dei Ministri e dal Ministro della Giustizia e comunicato alla Presidenza del Senato il 20 maggio 2024 il disegno di legge n. 1146, contenente "*Disposizioni e delega al Governo in materia di intelligenza artificiale*", il cui testo è rinvenibile in *https://www.senato.it*.

[2] M.B. Magro, *Decisione umana e decisione robotica, un'ipotesi di responsabilità da procreazione robotica*, in *Leg. pen*., 10 maggio 2020, p. 20; U. Ruffolo, *Per i fondamenti di un diritto alla robotica self-learning; dalla* Machinery *produttiva, all'auto* Driverless*: verso una "responsabilità da algoritmo"?*, in U. Ruffolo (a cura di), *Intelligenza artificiale e responsabilità*, Milano, 2017, pp. 18 ss., il quale evidenzia il rischio di improntare l'analisi giuridica del problema dell'intelligenza artificiale *self learning* sul piano meramente etico, "*così denunciando l'esistenza di un preteso vuoto normativo e trascurando la capacità di risposte sistemiche, sia interpretative che del lefigerare*".

© Wolters Kluwer Italia

gano in rilievo la causalità materiale, la colpevolezza, le posizioni di garanzia. Infine, si guarderà alle interferenze con la responsabilità da reato delle persone giuridiche.

Dinanzi al procedere incessante dell'IA nel nostro ordinamento e nel silenzio del legislatore, ci si propone dunque di ipotizzare le soluzioni attuabili in un sistema penale essenzialmente edificato sul pilastro del rimprovero personale e colpevole.

2. Sull'imputazione diretta della responsabilità penale

Nel d.lgs. n. 231/2001, l'autonoma responsabilità da reato dell'"ente" è stata fondata su paradigmi antropomorfi, in quanto si tratta di una "persona giuridica" che per il diritto penale agisce tramite persone fisiche ed è destinataria di precetti e sanzioni [3].

Il primo quesito che si pone è se si possa identificare giuridicamente nei sistemi di IA una nuova categoria di "enti" cui sia possibile imputare la responsabilità per i fatti dannosi od illeciti da essi cagionati, ed eventualmente addirittura una responsabilità penale. Ed in caso affermativo, sulla base di quali criteri o tramite quali modelli di attribuzione.

La possibilità di elevare la stessa macchina a bersaglio del sistema punitivo [4] presupporrebbe, oltre che una soggettività giuridica del sistema intelligente, che ricorra tra il fatto e il suo asserito autore il tipico nesso "spirituale" richiesto dalle norme di diritto [5], reggendosi tale ricostruzione sulla sovrapposizione tra fenomeni sostanziali e fenomeni processuali.

Se l'imputazione quale giudizio attributivo postulasse l'accertamento della suità della lesione penale, dovrebbe concludersi col ritenere che difetti una "volontà" libera, effettiva e consapevole, rispetto al quale trovi spazio una sanzione individualizzata [6].

---

[3] G. DE SIMONE, *Persone giuridiche e responsabilità da reato. Profili storici, dogmatici e comparatistici*, Pisa, 2012, pp. 353 ss. In una prospettiva anche comparata e parzialmente critica, V. MONGILLO, *La responsabilità penale tra individuo ed ente collettivo*, Torino, 2018, pp. 175 ss.

[4] C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" a "autore" del reato?,* in *Riv. it. dir. proc. pen.*, 4/2020, p. 1763.

[5] G.D. PISAPIA, *Contributo alla determinazione del concetto di capacità nel diritto penale*, in *Studi di diritto penale*, Padova, 1956, p. 22; V. CAVALLARI, *La capacità dell'imputato*, Milano, 1968, p. 133; G. FOSCHINI, *Sistema del diritto processuale penale*, vol. II, Milano, 1968, p. 134.

[6] R. BORGOGNO, *La responsabilità penale nei processi ad elevata automazione*, in

© Wolters Kluwer Italia

Eppure, ripercorrendo le cadenze argomentative già proposte per affermare la responsabilità penale delle *societas*, si è ritenuto, superando le pregiudiziali ontologiche, che, perlomeno in riferimento ai sistemi di IA "forte" [7] capaci di partorire processi intellettivi identici a quelli umani, potrebbe ritenersi che pure un'entità astratta possa essere "*un conglomerato capace di intenzionalità in ragione della sua complessità interna*" [8] e, pertanto, assurgere a centro di imputazione giuridica. Se è vero che, secondo l'insegnamento tradizionale, il diritto penale ruota attorno all'autocoscienza della persona umana, è anche vero che a partire dall'affermazione *societas delinquere potest* si è fatta strada l'idea della personificazione di soggetti non umani, specie quando questi dispongano di una sfera operativa estremamente complessa [9].

Di tal guisa, non v'è chi, concependo la macchina come autonomo centro di interessi e di imputazione, non abbia ipotizzato una personalità giuridica alla quale venga affiancato un fondo patrimoniale alimentato *pro-quota* dai soggetti che hanno contribuito alla sua ideazione, gestione od utilizzo, di modo che il sistema risponda in proprio delle obbligazioni, così come delle eventuali sanzioni pecuniarie [10].

E ancora. In via ricostruttiva, si è ipotizzato altresì che nelle ipotesi in cui il sistema intelligente non programmato per commettere reati (ovvero non programmato per commettere quel reato), per errore di programmazione o di utilizzazione del sistema, realizzi la condotta criminosa ovvero abbia realizzato un diverso reato, in sostituzione o in aggiunta rispetto a quello programmato, insieme all'IA siano chiamati a rispondere il programmatore e/o l'utilizzatore secondo le clausole di incriminazione suppletiva del concorso di persone, del concorso c.d. anomalo, della cooperazione colposa nel reato [11].

R. Giordano - A. Panzarola - A. Police - S. Preziosi - M. Proto (a cura di), *Il diritto nell'era digitale*, Milano, 2022, p. 733.

[7] Per la definizione di IA "forte", J. Kaplan, *Intelligenza artificiale, guida al prossimo futuro*, Roma, 2016, pp. 62 ss., il quale mette in rilievo che "*l'IA forte postula che le macchine hanno una mente, o finiranno per averla, mentre l'IA debole asserisce che si tratta di una semplice simulazione, e non di una duplicazione, dell'intelligenza artificiale*".

[8] S. Preziosi, *La responsabilità penale per eventi generati da sistemi di IA*, in R. Giordano - A. Panzarola - A. Police - S. Preziosi - M. Proto (a cura di), *Il diritto nell'era digitale*, cit., pp. 725-726.

[9] D. Piva, *Machina discere, (deinde) delinquere et puniri potest*, in R. Giordano - A. Panzarola - A. Police - S. Preziosi - M. Proto (a cura di), *Il diritto nell'era digitale*, cit., pp. 688 ss.

[10] C. Piergallini, *Intelligenza artificiale*, cit., p. 1764; D. Piva, *Machina discere, (deinde) delinquere*, cit., p. 692.

[11] R. Borgogno, *La responsabilità penale*, cit., p. 732.

© Wolters Kluwer Italia

Tuttavia, pur a fronte delle anzidette audaci ricostruzioni, di recente è stata approvata una risoluzione durante il Colloquio internazionale svoltosi a Siracusa [12], nella quale si è affermato che i sistemi di intelligenza artificiale restano ontologicamente diversi dalle persone umane, in ragione del fatto che ad essi manca la libertà di autodeterminazione, essendo il loro agire essenzialmente dominato dall'algoritmo.

Invero, il sistema di IA non agisce ma è agito [13], dovendo ricercarsi il vero motore dell'azione nelle informazioni inserite a monte da colui che elabora l'algoritmo: i risultati che ne conseguono, benché caratterizzati da una imprevedibilità necessitata [14], non possono in ogni caso assurgere ad agire intelligentemente gestito.

Di talché, sul piano delle funzioni della pena, ne deriva che in alcun modo la sanzione penale potrebbe svolgere una funzione special-preventiva ovvero general-preventiva, né tantomeno una funzione retributiva, dal momento che, in ragione di quanto sin qui detto, non potrebbe essergli mosso alcun rimprovero soggettivo per le condotte poste in essere [15].

3. Sull'imputazione indiretta della responsabilità penale

Esclusa la ricostruzione che, in un'ottica funzionalista, propone di considerare le macchine come soggetti di diritto, meritevoli di tutela e destinatarie di funzione, il dato da cui muovere è il seguente: sul piano empirico, si osserva che se un sistema di IA viene progettato, prodotto, commercializzato ed utilizzato, ciò avviene nell'interesse o a vantaggio di una persona fisica o giuridica.

Una volta individuati tali soggetti, perché possa ritenersi che siano penalmente responsabili, occorre procedere con una rimodulazione dei tradizionali criteri di attribuzione della responsabilità penale; e ciò in ragione del fatto che la connaturale imprevedibilità della decisione del sistema di IA appare, a sua volta, esser *ab origine* genericamente prevedibile da parte del suo ideatore, il quale tuttavia non è in grado di governarne gli effetti.

---

[12] Ci si riferisce alle Raccomandazioni contenute nella *Resolution on Traditional Criminal Law Categories and AI*, in *Riv. it. dir. proc. pen.*, 2/2022, p. 57.

[13] C. PIERGALLINI, *Intelligenza artificiale*, cit., p. 1769.

[14] *Ibid.*

[15] F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. uomo*, 6/2019, p. 31. Sulle teorie della pena, v. per tutti D. PULITANÒ, *Diritto penale*, Torino, 2017, pp. 47 ss.

© Wolters Kluwer Italia

Ci si domanda se l'eventuale causazione dell'evento, debba esser imputata all'ideatore dell'algoritmo, al programmatore, a colui che ha attualizzato quel rischio, mettendo in commercio quel sistema, ovvero ancora a chi ha gestito il rischio nel caso concreto, servendosi della cosa o cooperando con essa [16].

Per individuare i criteri di attribuzione della responsabilità penale, di modo da soddisfare i requisiti di personalità o colpevolezza per il fatto offensivo, occorre muovere da una breve analisi delle categorie generali.

3.1. *La causalità materiale*

Sul piano della causalità, occorre verificare che il meccanismo eziologico appaia riconducibile alle azioni/decisioni *ab initio* programmate, avendo riguardo al fatto che i sistemi di *machine learning*, in ragione del margine di imprevedibilità insito nell'*output* dei meccanismi di autoapprendimento, potrebbero rendere ardua l'esatta allocazione delle responsabilità in relazione alle attività che, suddivise in fasi, comportano una ripartizione di competenze.

Si rende, pertanto, necessario modulare in maniera peculiare il criterio condizionalistico [17], giungendo a verificare, mediante un ragionamento ipotetico per il quale si elimina o si aggiunge mentalmente il contributo del sistema di IA, se l'evento o il fatto si sarebbero comunque verificati.

La nebulosità dell'accertamento causale si deve al fatto che l'interprete si trova dinanzi ad una congerie di fattori causali alternativi, operanti tra di loro in modo sinergico.

Le criticità si acuiscono in riferimento alle c.d. *black box*, quale fattispecie i cui possibili esiti non solo sono imprevedibili, ma in sede ricostruttiva, non appare nemmeno possibile delineare con esattezza i singoli anelli della catena che ha portato in concreto a quell'esito, con evidenti ripercussioni processuali.

In simili evenienze, lì dove il danno sia da ricondurre all'azione ovvero alla decisione del sistema di IA, estranea rispetto all'originario disegno operativo, potrebbe venire in rilievo la norma disciplinante

---

[16] V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *Discrimen*, 15 maggio 2020, p. 3.

[17] F. Antolisei, *Il rapporto di causalità nel diritto penale*, Padova, 1934, p. 216; F. Stella, *La nozione penalmente rilevante di causa: la condizione necessaria*, in *Riv. it. dir. proc. pen*., 1988, p. 1261.

© Wolters Kluwer Italia

l'interruzione del nesso causale dovuta ad un fattore sopravvenuto (art. 41, comma 2, c.p.), in ragione del fatto che il comportamento di un terzo si sarebbe interposto tra la condotta dell'ideatore/produttore/utilizzatore e l'evento penalmente rilevante, così innescando un nuovo rischio qualitativamente differente da quello inizialmente concepito.

Aderendo a tale impostazione, e tralasciando criteri meramente logici, troverebbero spazio la teoria della causalità adeguata e quella della causalità umana: si potrebbe sostenere che l'azione iniziale non fosse adeguata rispetto alla produzione dell'evento ovvero che l'eccezionalità dell'evento finale esulerebbe da qualsiasi capacità di dominio dell'uomo.

Inserendo dei criteri di selezione normativi, secondo taluno [18], da un lato si evita il pericolo di un regresso all'infinito (con conseguente ampliamento dell'area del penalmente rilevante); dall'altro, si esclude l'imputazione oggettiva di eventi del tutto anomali.

Peraltro, il ricorso a criteri normativi di delimitazione dell'area del rischio è stato, di recente, imposto dal regolamento dell'Unione europea sull'intelligenza artificiale, al fine di orientare la preventiva valutazione dei rischi (*risk assessment*) imposta ai titolari ed agli operatori dei sistemi classificati come "*ad alto rischio*" [19].

In dottrina, si è criticata la tenuta del sistema di fronte alla ricostruzione del nesso causale nei termini sin qui detti: parlare di interruzione di nesso causale e di fattore causale escludente significherebbe frustrare l'aspettativa di tutela delle vittime, giacché, se è vero che il sistema di *decision making* della macchina sia foriero di esiti imprevedibili, è pure vero che la non completa predicibilità sia scaturita, a monte, dall'azione umana.

Se appellarsi all'interruzione del nesso causale non sembra esser una soluzione giuridicamente corretta, ci si propone di delineare l'area del penalmente rilevante sul terreno della tipicità soggettiva.

3.2. *La colpevolezza*

Di recente, il citato regolamento europeo ha introdotto molteplici divieti con riferimento ai sistemi "*ad alto rischio*", regolando quali

---

[18] L. PICOTTI, *Categorie tradizionali del diritto*, cit., p. 9.

[19] Ci si riferisce al regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, il quale stabilisce regole armonizzate sull'intelligenza artificiale. V., in particolare, l'art. 9 rubricato "*Sistema di gestione dei rischi*".

© Wolters Kluwer Italia

debbano essere le "*pratiche di* governance *e gestione dei dati adeguate alla finalità prevista dal sistema*" e, al contempo, ha previsto specifici obblighi in capo ai singoli operatori.

Si tratta di un reticolo di regole cautelari idoneo a delimitare il perimetro del c.d. rischio consentito, la cui idoneità a fondare un rimprovero colposo [20] passa per l'accertamento del momento soggettivo di riprovazione personale, non risultando sufficiente la mera violazione della cautela per fondare la responsabilità penale per il fatto in concreto verificatosi.

Invero, a rigore, muovendo dal presupposto per il quale l'auto-apprendimento del sistema di IA determina esiti imprevedibili, il giudizio di imputazione per colpa dovrebbe ritenersi sempre paralizzato.

Affermare che, a fronte della violazione della regola cautelare, la prevedibilità fondativa dell'addebito colposo si risolva nella mera "possibilità di prevedere" che l'*output* prodotto dal sistema rientri nella correlata area di rischio, non essendo necessario che il soggetto abbia previsto in concreto l'evento o il fatto effettivamente realizzatosi, significa ri-descrivere l'evento da porre in correlazione alla regola cautelare disattesa e, in tal modo, bypassare il criterio di copertura del rischio tipico [21].

In breve: si tratterebbe di responsabilità oggettiva allo stato puro, legittimata da esigenze di semplificazione probatoria tali per cui a fronte di un evento cagionato dal sistema, di per sé imprevedibile, sarebbe possibile muovere un rimprovero in ragione del fatto che, *ab initio*, fosse genericamente prevedibile.

I pilastri fondativi del diritto penale vacillano di fronte a simili approdi, tali da revocare in dubbio i baluardi costituzionali.

3.3. *Le posizioni di garanzia*

Le richiamate disposizioni del regolamento europeo, nel delineare un "*sistema di gestione dei rischi*" (art. 9), hanno altresì individuato posizioni di garanzia penalmente rilevanti sulla scorta dell'archetipo di cui all'art. 40, comma 2, c.p., con corrispondenti doveri d'impedi-

---

[20] C. Piergallini, *Colpa* (voce), in *Enc. dir.*, *Annali*, vol. X, Roma, 2017, pp. 235 ss.

[21] Queste, le risultanze del par. 4 delle Raccomandazioni di cui alla *Resolution*, cit., pp. 57-58.

© Wolters Kluwer Italia

mento di eventi o fatti costitutivi di reati, anche laddove il decorso causale sia stato ultimato dai sistemi stessi.

Tra gli altri, si è previsto all'art. 14 uno specifico "*obbligo di sorveglianza umana*", il quale viene variamente modulato in ragione della fase di progettazione e sviluppo dei sistemi che viene in rilievo, sì da responsabilizzare penalmente soggetti chiamati ad impedire fatti o eventi e, al contempo, non render sterile il funzionamento del sistema, rischiando di contraddire l'utilità della loro autonomia.

Dinanzi alla previsione di nuovi obblighi di controllo, consistenti negli obblighi di identificazione e valutazione dei rischi derivanti dalle attività di sistemi di IA, cui consegue l'adozione delle corrispondenti misure di contenimento, ci si trova di fronte ad un evidente ampliamento dell'area del penalmente rilevante.

A fronte di ciò, è lecito domandarsi se sia effettivamente compito proprio del diritto penale il dover prevenire e/o punire simili fattispecie, in ragione del fatto che si impone ad un soggetto un obbligo di impedire un evento ontologicamente caratterizzato da una intrinseca incertezza, dando vita a forme mascherate di responsabilità oggettiva.

4. Considerazioni conclusive

Dalla lettura della recente normativa regolatoria sembrerebbe *prima facie* potersi escludere la prospettabilità di scenari in cui sistemi evoluti di intelligenza artificiale assumano preoccupanti attitudini criminali, generando rischi inaspettati; e ciò in ragione del fatto che il mantenimento del controllo umano sulla macchina si atteggia quale principio fondativo della normativa europea, così come della normativa nazionale *in fieri*[22]: l'opacità che caratterizza il *modus operandi* delle macchine intelligenti, secondo il legislatore, ben potrebbe essere neutralizzata mediante capillari sistemi di monitoraggio e di controllo sui sistemi di intelligenza artificiale, oltre che, in fase di progettazione, l'operare di una selezione preventiva dei sistemi da immettere sul mercato.

Invero, in disparte legittimi dubbi sull'idoneità di tali norme a fronteggiare i veloci sviluppi dell'IA in termini di autonomia e autoapprendimento, il quadro sin qui ricostruito sembra prefigurare un conflitto fondato su una coppia oppositiva: il sistema, da un lato, innesca volontariamente nuovi focolai di pericolo e, al contempo, non riesce a

[22] Ci si riferisce al contenuto del menzionato d.d.l. n. 1146 del 2024.

© Wolters Kluwer Italia

prevedere, prevenire e governare i rischi che esso stesso mette in moto [23].

Sanzionare le conseguenze indesiderate derivanti dall'operare del sistema di IA, in un'ottica reattiva, appare in definitiva inattuabile, a meno che non si vogliano violare i pilastri fondativi del diritto penale.

D'altra parte, privilegiare un approccio proattivo, atto ad intercettare i rischi attraverso l'introduzione di un serrato sistema di controlli preventivi e di continuo monitoraggio del rischio, non può dirsi idoneo a prevenire ogni rischio, proprio in ragione della imprevedibilità delle macchine pensanti.

Si è proposta, allora, una pluralità di regolamentazioni, nella quale coesistano norme etiche, giuridiche, tecniche e strumenti di autonormazione: in un governo condiviso della gestione del rischio, sarebbe auspicabile che il controllo penale, di per sé inadeguato in contesti di incertezza, ceda il passo a forme di *self-regulation*, limitandosi ad esercitare soltanto funzioni di indirizzo e coordinamento [24].

---

[23] C. Piergallini, *Intelligenza artificiale*, cit., p. 1771; Id., *Attività produttive, decisioni in stato di incertezza e diritto penale*, in M. Donini - M. Pavarini (a cura di), *Sicurezza e diritto penale*, Bologna, 2011, pp. 327 ss.

[24] C. Piergallini, *Intelligenza artificiale*, cit., pp. 1772-1773.

© Wolters Kluwer Italia

Sezione Sesta

NUOVE TECNOLOGIE E REALTÀ TRASFORMATE

IL PLURALISMO DELL'INFORMAZIONE AL VAGLIO DELLE PIATTAFORME DIGITALI *

Susanna De Stefani

Sommario: 1. Premesse all'origine. – 2. Informazione *online*: tra profilazione degli utenti e *fake news*. – 3. La strategia europea contro la disinformazione. – 3.1. Il Codice di buone pratiche sulla disinformazione. – 3.2. La legge europea sui servizi digitali. – 4. Alcune considerazioni conclusive.

Abstract: The traditional doctrine of informational pluralism, based on the paradigm of the "free market of ideas", has led to the belief that competition among numerous informational sources is sufficient to guarantee plural and different ideas. However, applying this approach to the digital ecosystem, characterised by the explosion of informational supply and free access to a multitude of sources, it becomes clear that traditional frameworks require new forms of regulation. The digital transformation presents the information world with new challenges, including the algorithmic profiling of information by digital platforms and content moderation policies to combat disinformation. On the one hand there is the issue of ensuring diversity and on the other the question of how to prevent this from turning into the spread of incorrect information. This contribution aims to examine the recent initiatives adopted by the European Union to increase the transparency and accountability of large online platforms through forms of co-regulation that focus on regulating the platforms themselves rather than restricting content, in order to find a balance between conflicting constitutional rights and freedoms.

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

1. Premesse all'origine

La relazione tra il pluralismo dell'informazione e il diritto della concorrenza ha posto negli anni numerose questioni che sono state affrontate dalla dottrina sotto diversi punti di vista [1].

Da alcuni è stato sostenuto come, a fronte della mancanza di competenze dell'Unione in materia di pluralismo, il diritto della concorrenza sia lo strumento più adatto per colmare tale vuoto normativo [2]. Questo perché, nella maggior parte dei casi, la tutela del pluralismo, più che l'obiettivo, rappresenta la conseguenza della concorrenza, dove l'obiettivo consiste nell'eliminazione di comportamenti abusivi e nella prevenzione di quelle concentrazioni che poterebbero falsare il funzionamento del mercato, costituendo così una minaccia per la varietà di fonti indipendenti [3]. In questo modo il diritto della concorrenza impedirebbe l'accumulo di potere nelle mani di pochi. Apparentemente, quindi, una pluralità di concorrenti (voci) consentirebbe una varietà di prodotti (opinioni).

Da tempo, tuttavia, una dottrina alternativa sostiene che, così come vi potrebbe essere un adeguato grado di concorrenza senza che sia garantito il pluralismo, viceversa, il pluralismo potrebbe essere garantito anche in assenza di un grado sufficiente di concorrenza [4]. Sul punto, secondo questa dottrina, l'assunto che la pluralità di fonti informative esigerebbe la pluralità di operatori sarebbe frutto di un equivoco, laddove invece i due fenomeni non sempre coinciderebbero [5].

---

[1] Sulla relazione tra pluralismo dei media e diritto della concorrenza, *ex multis*, K. BANIA, *The role of media pluralism in the enforcement of EU competition law*, Doctoral Thesis, Florence, 2015; più di recente, O. PALLOTTA, *Antitrust e pluralismo dell'informazione nel diritto UE: un'alternanza in favore della democrazia*, in *Dir. Un. eur.*, 1/2023, pp. 109-134.

[2] R. CRAUFURD-SMITH, *Rethinking European Union Competence in the Field of Media Ownership: The Internal Market, Fundamental Rights and European Citizenship*, in *European Law Review*, 2004, pp. 652-673; M. ARINO, *Regulation and Competition in European Digital Broadcasting-A study of pluralism through access*, Doctoral Thesis, Florence, 2005; P. KELLER, *European and international media law: liberal democracy, trade, and the new media*, New York, 2011.

[3] M. ARINO, *Competition Law and Pluralism in European Digital Broadcasting: Addressing the Gaps*, in *Communications and Strategies*, 54/2004, p. 117.

[4] F. BASSAN - S. VENTURINI, *Pluralismo e par condicio*, in F. BASSAN - E. TOSI (a cura di), *Diritto degli audiovisivi-Commento al nuovo Testo Unico dei Servizi di Media Audiovisivi e Radiofonici come modificato dal D. Lgs. 15 marzo 2010, n. 44*, Milano, 2012, p. 143.

[5] F. BASSAN, *Concorrenza e regolazione nel diritto comunitario delle comunicazioni elettroniche*, Torino, 2002; F. BASSAN - S. VENTURINI, *Op. cit.*, p. 142; B.P. PAAL,

© Wolters Kluwer Italia

È proprio tale equivoco che oggi, nell'ecosistema digitale, da più parti si propone di sfatare, dimostrando come il rapporto tra pluralismo e concorrenza nel mercato delle idee sia tutt'altro che lineare. In particolare, ad accendere il dibattito, è stata la dottrina statunitense del *free marketplace of ideas* [6] fondata su un orientamento di *digital trust*, ossia sulla fiducia nella capacità autocorrettiva del mercato digitale in cui la *free competition* di idee e opinioni aumenterebbe automaticamente il pluralismo e permetterebbe il conseguimento della verità [7]. Tale metafora è stata, in seguito, "traslata" nel contesto europeo per elaborare una strategia di contrasto ai problemi legati alla distorsione dell'informazione nel *web* di cui si dirà nel prosieguo [8].

Oggi si sostiene infatti come la concorrenza dei nuovi media soffra di una "*tirannia della maggioranza*" [9], nel senso che i numerosi concorrenti presenti nel mercato finiscono tutti per vendere lo stesso tipo di prodotto. Questo perché, nel mondo digitale, da un lato, il bene dell'informazione sta diventando sempre di più un prodotto di mercato a tutti gli effetti, in cui il consumatore sceglie quelle informazioni che più si avvicinano alle proprie convinzioni o al conformismo di gruppo; dall'altro, il fornitore di informazioni cercherà di offrire un prodotto quanto più soddisfacente possibile per il cliente. Il risultato di tutto ciò è che le opinioni prendono il posto dei fatti [10]. A tutto questo si de-

---

Current issues and recent developments on media concentration in the context of competition law and media law, in *Journal of Intellectual Property Law & Practice*, 7/2017, pp. 610-616; K. Cseres - M. Kozak, *Media pluralism and EU competition law. What role EU competition rules play in fostering media pluralism in the Member States?*, disponibile su: *www.acelg.uva.nl*, Amsterdam, 2021.

[6] Espressione coniata nella *dissenting opinion* del giudice Holmes nella sentenza della Corte Suprema federale degli Stati Uniti d'America, 10 novembre 1919, *Abrams v. United States*, poi ripresa dalla stessa Corte per riadattarla al contesto tecnologico nella successiva pronuncia del 26 giugno 1997, *Reno v. ACLU*, nella quale afferma "Internet is the new free marketplace of ideas".

[7] "*Come in un mercato concorrenziale dove i migliori prodotti o servizi prevalgono, lo stesso avviene per le informazioni vere e corrette destinate ad essere predilette dal mercato stesso*". Così G. De Gregorio, *The market place of ideas nell'era della post-verità: quali responsabilità per gli attori pubblici e privati online?*, in *MediaLaws-Rivista dir. media*, 1/2017, p. 95.

[8] O. Pollicino, *Migrazioni di idee costituzionali e implicazioni per le opzioni rilevanti di politica del diritto: il caso della strategia europea contro la disinformazione on line*, in R. Mastroianni - F. Ferraro (a cura di), *Libertà di informazione e diritto dell'Unione europea. Le nuove sfide a tutela della democrazia e del pluralismo*, I Quaderni del Corso di perfezionamento in Diritto dell'Unione europea dell'Università di Napoli Federico II, vol. VIII, Napoli, 2022, pp. 89-104.

[9] M. Arino, *Competition Law and Pluralism in European Digital Broadcasting*, cit., p. 102.

[10] Il mercato delle libere idee si trasforma nel mercato delle "verità desiderate", v.

© Wolters Kluwer Italia

ve aggiungere il fenomeno del decentramento della produzione dell'informazione [11]. È qui che il diritto della concorrenza incontra un limite nel garantire un ambiente pluralistico e la circolazione della verità. La concorrenza, contrariamente a quanto sostenuto, finisce per alimentare questa tendenza dal momento che l'offerta tende a specializzarsi per offrire solo il desiderato [12].

I paragrafi che seguono analizzeranno le caratteristiche dell'offerta informativa del *web* e le recenti iniziative europee pensate per preservare la qualità dell'informazione e disciplinare il ruolo dei nuovi attori del mercato digitale.

2. Informazione *online*: tra profilazione degli utenti e *fake news*

Una delle principali differenze che distingue l'informazione *online* da quella tradizionale è l'enorme volume dei dati degli utenti che circolano in rete. Tali dati vengono acquisiti dagli *Internet services providers,* ossia i fornitori di servizi *Internet* che gestiscono le piattaforme *online*, attraverso due metodi di apprendimento denominati *machine learning* (apprendimento automatico) e *deep learning* (apprendimento profondo) [13]. La combinazione di queste tecniche consente di acquisire i dati dal mondo esterno, rielaborarne il contenuto sulla base dei tratti comuni ed offrire un'informazione predittiva e completa. I *provider*, a loro volta, fungono da intermediari tra gli utenti e i motori di ricerca fornendo a questi ultimi le informazioni in precedenza raccolte.

L'informazione *online* viene quindi gestita dai c.d. *gatekeepers* (guardiani) della rete in quanto questi soggetti controllano e ordinano le notizie da distribuire ai consumatori, selezionando i contenuti multimediali attraverso l'uso di filtri algoritmici [14]. La particolarità sta nel

---

A. NICITA, *Il mercato delle verità. Come la disinformazione minaccia la democrazia*, Bologna, 2021.

[11] Sul tema v. il paragrafo successivo.

[12] M. GENTZKOW - J. M. SHAPIR, *Competition and Truth in the Market for News*, in *Journal of Economic Perspectives*, 2/2008, pp. 133-154.

[13] R. MONTALDO, *La tutela del pluralismo informativo nelle piattaforme online*, in *MediaLaws-Rivista dir. media*, 1/2020, pp. 224-229; M. FASAN, *Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico*, in *Rivista di BioDiritto*, 1/2019, pp. 101-113.

[14] Soggetti intermediari che esercitano un controllo diretto sull'informazione che passa attraverso una porta di accesso (o *gate*). Sull'argomento, *ex multis*, G. PITRUZZELLA, *La libertà di informazione nell'era di* Internet, in *MediaLaws-Rivista dir. media*, 1/2018, pp. 19-47; O. GRADINETTI, *Le piattaforme digitali come "poteri privati" e la censura online*, in *Riv. it. inf. dir.*, 1/2022, pp. 175-188.

© Wolters Kluwer Italia

fatto che tale selezione non avviene seguendo criteri oggettivi bensì le preferenze ricavate con i processi di apprendimento anzidetti. L'insieme di queste operazioni corrisponde alle tecniche di profilazione, ossia un trattamento automatizzato dei dati personali che permette di generare un'offerta informativa quanto più precisa e compatibile con il profilo dell'utente [15]. Questa personalizzazione dell'informazione basata sui comportamenti di ricerca del singolo crea le c.d. *filter bubbles* (bolle di filtraggio) [16], ossia delle "bolle informative" in cui l'utente non viene più esposto a prodotti alternativi ma finisce per ricevere "un eco" delle sue precedenti ricerche. Da qui il fenomeno delle *echo chambers* (camere di risonanza), comunità di utenti polarizzati intorno alle proprie convinzioni e attratti dal c.d. *confirmation bias* (pregiudizio di conferma), vale a dire quella tendenza che li induce a ricercare informazioni che confermano e rafforzano le proprie opinioni [17].

A ciò si deve aggiungere che chiunque oggi può contribuire a formare il discorso pubblico in rete. Si parla infatti di una produzione decentralizzata dell'informazione, considerando che è sufficiente avere accesso al *web* per condividere fatti, critiche e punti di vista. La creazione decentralizzata dei contenuti fa sì che tutti, indipendentemente dal grado di conoscenza di una determinata materia, hanno la possibilità di avere voce in capitolo. Questo, tuttavia, pone il problema della veridicità delle informazioni che circolano. Da qui la delicata questione della disinformazione, consistente in strategie di diffusione di informazioni false, deliberatamente create come tali, che, per l'impatto emotivo che suscitano nei confronti di chi le riceve, sono suscettibili di essere percepite come vere [18]. È chiaro che la rapidità che contraddistingue il *web* alimenta tale fenomeno.

Dunque, se, da un lato, la quantità delle informazioni offerte dalla

---

[15] R. Montaldo, *Op. cit.*, p. 225; M. Fasan, *Op. cit*., p. 105.

[16] L'espressione "*filter bubble*" è stata coniata da Eli Pariser in E. Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, London, 2012;

[17] Sull'argomento, W.H. Dutton - E. Dubois - G. Blank, *Social Shaping of the Politics of Internet Search and Networking: Moving Beyond Filter Bubbles, Echo Chambers, and Fake News*, in *Quello Center Working Paper*, n. 2944191, 2017, disponibile su: *https://ssrn.com*, p. 3; J.M. Reyes, *Social network, polarizzazione e democrazia: dall'entusiasmo al disincanto*, in E. Vitale - F. Cattaneo (a cura di), *Web e società democratica. Un matrimonio difficile*, Torino, 2018, pp. 18 ss.; A. Peruzzi - F. Zollo - A.L. Schmidt - W. Quattrociocchi, *From Confirmation Bias to Echo-Chambers: a data-driven approach*, in *Sociologia e Politiche Sociali*, 3/2018, p. 54.

[18] M. Buiten, *Combating Disinformation and Ensuring Diversity on Online Platforms: Goals and Limits of EU Platform*, 2022, disponibile su: *https://ssrn.com*; B. Martens - L. Aguiar - E. Gomez-Herrera - F. Mueller-Langer, *The Digital Transfor-*

© Wolters Kluwer Italia

rete espone il singolo ad una molteplicità di contenuti, dall'altro, il filtraggio algoritmico rende meno plurali le informazioni che l'utente riceve. Al contempo, la produzione decentralizzata solleva dubbi sull'affidabilità delle informazioni in circolazione. Queste osservazioni rivelano come un'informazione attendibile e plurale nell'odierna realtà digitale, non può essere garantita (solo) incentivando la pluralità e la diversità di opinioni, ma è necessario ricercare regole ulteriori che assicurino una corretta gestione dei contenuti multimediali da parte delle piattaforme digitali.

Data la varietà dei problemi che interessano lo spazio digitale, per ragioni di contenuto e di rilevanza del tema, il paragrafo successivo tratterà il fenomeno della disinformazione *online* con particolare riferimento alle iniziative sviluppate dalle istituzioni europee per contrastarne la rapida diffusione.

3. La strategia europea contro la disinformazione

L'Unione europea si è occupata per la prima volta di disinformazione nel 2015 quando il Consiglio europeo, seppur con riferimento ad un ambito specifico, esprimeva le sue preoccupazioni per la diffusione di *fake news* ed invitava l'Alto rappresentante per la politica estera e la sicurezza comune, insieme alle istituzioni europee e agli Stati membri, ad elaborare una strategia per contrastare le campagne di disinformazione [19].

Successivamente, da un lato, il Parlamento europeo presentava una risoluzione per incoraggiare la Commissione ad affrontare il problema della circolazione di notizie false *online* [20] e, dall'altro, il Consiglio europeo sollecitava, di nuovo, l'adozione di misure volte a combattere la disinformazione soprattutto in vista delle elezioni europee del 2019 [21].

In risposta, la Commissione istituiva un gruppo di esperti di alto

---

mation of News Media and the Rise of Disinformation and Fake News, JRC Digital Economy Working Paper, 2018, disponibile su: *https://ssrn.com*.

[19] Conclusioni del Consiglio europeo, 19 e 20 marzo 2015, p. 13, disponibili su: *https://www.consilium.europa.eu.* In particolare, i *leader* europei facevano riferimento alle campagne di disinformazione in corso da parte della Russia. Per un commento della questione v. S. LATTANZI, *La lotta alla disinformazione nei rapporti tra Unione e Stati terzi alla luce del conflitto russo-ucraino*, in *Media Laws*, 3/2022, pp. 158-178.

[20] Risoluzione del Parlamento europeo del 15 giugno 2017 sulle piattaforme *online* e il mercato unico digitale, 2016/2276(INI), p. 36.

[21] Conclusioni del Consiglio europeo, 18 ottobre 2018, disponibili su: *https://www.consilium.europa.eu*.

© Wolters Kluwer Italia

livello incaricato di individuare le strategie più efficienti per contrastare la diffusione della disinformazione *online* [22]. Sulla base del *report* elaborato del gruppo, la Commissione presentava una prima comunicazione al fine di delineare un approccio europeo al fenomeno e una seconda, nello stesso anno, contenente un Piano d'azione contro la disinformazione [23].

3.1. *Il Codice di buone pratiche sulla disinformazione*

Tra le azioni previste nella prima comunicazione della Commissione vi era quella di convocare un *forum* di *multistakeholder* incaricato di sviluppare un codice di condotta per contrastare la diffusione di informazioni false [24]. Si tratta del Codice di buone pratiche sulla disinformazione, pubblicato nel settembre del 2018 e "rafforzato" negli ultimi anni [25]. Attraverso il Codice, le piattaforme *online* e altri attori pertinenti [26] hanno concordato volontariamente degli *standard* di auto-

---

[22] High Level Group of Expert (HLEG), "*A multi-dimensional approach to disinformation. Report of the independent High level Group on fake news and online disinformation*", 2018, disponibile su: *https://digital-strategy.ec.europa.eu*.

[23] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "*Contrastare la disinformazione online: un approccio europeo*", Bruxelles, 26 aprile 2018, COM(2018)236 final; comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "*Piano d'azione contro la disinformazione*", Bruxelles, 5 dicembre 2018, JOIN(2018)36 final.

[24] Multistakeholder Forum on Disinformation, disponibile su: *https://digital-strategy.ec.europa.eu.*

[25] Codice di buone pratiche rafforzato sulla disinformazione, 2022, disponibile su: *https://digital-strategy.ec.europa.eu*. Per un commento v. M. Monti, *Lo strengthened Code of Practice on Disinformation: un'altra pietra della nuova fortezza digitale europea*, in *Media Laws*, 2/2022, pp. 317-32; P. Cavaliere, *The Truth in Fake News: How Disinformation Laws Are Reframing the Concepts of Truth and Accuracy on Digital Platforms*, in *European Convention on Human Rights Law Review*, 3/2022, pp. 481-523; G. Caggiano, *Il contrasto alla disinformazione tra nuovi obblighi delle piattaforme online e tutela dei diritti fondamentali nel quadro*, in *Papers di diritto europeo*, 1/2021, pp. 45-71; G. Pagano, *Il Code of Practice on Disinformation. Note sulla natura giuridica di un atto misto di autoregolazione*, in *Federalismi.it*, 1/2019, pp. 1-31.

[26] La prima versione del Codice veniva firmata soltanto dalle grandi piattaforme *online*. A queste si sono successivamente aggiunti nuovi firmatari, tra cui rappresentanti della società civile, imprese attive nel settore pubblicitario e *fact-checkers.* V. Signatories of the 2022 Strengthened Code of Practice on Disinformation, disponibile su: *https://digital-strategy.ec.europa.eu*.

© Wolters Kluwer Italia

regolamentazione per combattere la disinformazione in rete. Si tratta di un documento redatto dai firmatari che decidono in autonomia quali impegni assumere sotto la propria responsabilità in settori mirati [27].

Come anticipato, la decisione di percorrere la strada dell'autoregolamentazione affonda le sue radici nella metafora statunitense del *free market place of ideas* [28], per cui la rete deve essere considerata un mercato dotato di capacità autocorrettiva in grado di isolare fenomeni di disinformazione attraverso la libera competizione di idee e senza la necessità di alcun intervento da parte delle Autorità. Tuttavia, questo metodo è risultato ben presto deludente, soprattutto per la vaghezza degli impegni sottoscritti. Tra le criticità rilevate da una prima valutazione della Commissione sull'attuazione del Codice vi erano un'applicazione incoerente e incompleta degli impegni assunti dalle piattaforme e dagli Stati membri, la mancanza di definizioni uniformi e vari altri problemi legati alla natura di autoregolamentazione del Codice [29].

Per tale ragione, anche a seguito della diffusione di *fake news* nel corso della crisi pandemica, la Commissione pubblicava delle linee guida finalizzate al "rafforzamento" del Codice, raccomandandone anche l'estensione a nuovi firmatari [30]. Il nuovo Codice, fedele agli orientamenti dell'esecutivo europeo, rappresenta un importante cambio di paradigma per due ordini di ragioni: in primo luogo, un valore aggiunto è sicuramente la presenza più massiccia di indicatori di prestazione impiegati per attivare procedure di controllo sull'efficacia degli impegni assunti dalle piattaforme [31]. In secondo luogo, il Codice rafforzato

---

[27] Tra gli impegni originari: il controllo dei posizionamenti degli annunci pubblicitari; la trasparenza e la conoscibilità della pubblicità politica, soprattutto nei periodi elettorali; la responsabilizzazione dei consumatori di informazione e dei ricercatori, favorendo a questi ultimi l'accesso ai dati per studi approfonditi sulla disinformazione *online*. A questi si sono aggiunti il rafforzamento del ruolo dei *fact-checkers* e la previsione di indicatori strutturali che misurano l'impatto complessivo del codice sulla disinformazione.

[28] O. POLLICINO, *Op. cit.*

[29] Commission Staff Working Document "*Assessment of the Code of Practice on Disinformation-Achievements and Areas for Further Improvement*", Brussels, 10 September 2020, SWD/2020/180 final, pp. 7-19.

[30] V. la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "*Orientamenti della Commissione europea sul rafforzamento del codice di buone pratiche sulla disinformazione*", Bruxelles, 26 maggio 2021, COM(2021)262 final.

[31] La Commissione individua due classi di *Key Performance Indicators*: *i*) i *Service level indicators*, che misurano i risultati e l'impatto delle politiche attuate dai firmatari in ossequio agli impegni presi e *ii*) gli *Structural indicators*, che misurano l'impatto complessivo del Codice sulla disinformazione nell'UE. *Id.*, p. 21.

© Wolters Kluwer Italia

costituisce il primo esempio di co-regolamentazione nella lotta alla disinformazione. Esso si affianca infatti al nuovo regolamento sui servizi digitali (*Digital Services Act* o DSA) [32], di cui completa e persegue gli obiettivi [33]. In questo modo, diversamente dal precedente, è maggiormente in grado di produrre veri e propri effetti giuridici in capo ai suoi firmatari [34].

3.2. *La legge europea sui servizi digitali*

Insieme al Codice di buone pratiche, il nuovo regolamento sui servizi digitali (noto anche, seppure impropriamente, come legge europea sui servizi digitali) mira a garantire un ambiente *online* sicuro, prevedibile e affidabile [35]. Esso predispone le modalità di rimozione dei contenuti illegali in rete da parte dei "servizi intermediari" (*Internet services providers* o ISP) [36], modificando, in questo, la direttiva sul commercio elettronico [37]. La direttiva, infatti, già prevedeva un "onere" di disabilitazione di tali contenuti ma non definiva le procedure di rimozione, determinando una frammentazione di disciplina da Stato a Stato, né prevedeva obblighi di trasparenza in capo ai prestatori di servizi.

---

[32] Regolamento (UE) 2022/2065 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 (regolamento sui servizi digitali), in G.U.U.E. L277 del 27 ottobre 2022, pp. 1-102.

[33] Come chiarito nel Preambolo del Codice, lett. h) e i).

[34] Reg. (UE) 2022/2065, cit., art. 45.

[35] *Id*., art. 1, par. 1. Per un commento v. M.C. Buiten, *The Digital Services Act: From Intermediary Liability to Platform Regulation,* in *Journal of Intellectual Property, Information Technology and E-Commerce Law,* 12/2022, pp. 361-380; A. Palumbo, *Delega di funzioni regolamentari e lotta ai rischi sistemici causati della disinformazione nel Digital Services Act: quali rischi per la libertà di espressione?*, in *MediaLaws-Rivista dir. media*, 3/2023, pp. 114-143; G. Caggiano, *La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in G. Caggiano - G. Contaldi - P. Manzini (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021, pp. 3 ss.

[36] *Id*., art. 3, lett. g). I servizi intermediari si distinguono in: *i*) servizi di trasmissione di informazione c.d. *mere conduit*, *ii*) servizi di memorizzazione temporanea o *caching* e *iii*) servizi di memorizzazione di informazioni o di *hosting*. Le piattaforme *online* rappresentano una sottocategoria dei servizi di *hosting*.

[37] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (direttiva sul commercio elettronico), in G.U.C.E. L178 del 17 luglio 2000, pp. 1-16, Sez. 4.

© Wolters Kluwer Italia

Diversamente, il regolamento contempla un sistema di regole procedurali che disciplinano il modo in cui tali soggetti devono mitigare i contenuti illegali al fine di aumentare il livello di trasparenza. Tra queste vanno annoverate: la predisposizione di relazioni chiare e dettagliate sulle attività di moderazione dei contenuti avviate di propria iniziativa (art. 15); l'attivazione di sistemi interni di gestione dei reclami, in modo tale da consentire agli utenti di presentare in via elettronica la segnalazione della presenza di contenuti illegali (artt. 16 e 20); il rafforzamento dell'onere motivazionale a sostegno delle misure restrittive (art. 17). Si tratta di un sistema "a cerchi concentrici", in cui gli obblighi diventano più rigorosi all'aumentare della dimensione degli ISP [38].

Dal punto di vista sostanziale, il regolamento si applica a quei contenuti "illegali" definiti tali ai sensi del diritto dell'Unione o degli Stati membri [39]. Si omette pertanto di fornire una definizione comune di "illegalità" del contenuto, nonostante la centralità di una tale nozione. Probabilmente la scelta è dovuta alla difficoltà di trovare un equilibrio tra l'esigenza di elaborare una disciplina quanto più dettagliata possibile e il rischio di comprimere eccessivamente la libertà di espressione [40].

Al netto di quanto rappresentato, si nota come la disinformazione non sia espressamente contemplata nel testo di legge. Ciononostante, questa sembrerebbe rientrare in quei rischi sistemici che le piattaforme di grandi dimensioni sono tenute a valutare e mitigare per evitare la rapida diffusione "effetti negativi" in specifici settori [41]. Anche in questo caso manca una definizione di tali rischi, lasciando pertanto nelle mani delle piattaforme il potere di decidere quali contenuti possono circolare o meno.

4. Alcune considerazioni conclusive

Volendo svolgere alcune riflessioni conclusive, si rileva che, appurato che lasciare il mercato libero di far circolare una molteplicità di

[38] Reg. (UE) n. 2022/2065, cit., Sez. 5. Le piattaforme *online* di dimensioni molto grandi (*Very Large Online Platforms* o VLOP) e i motori di ricerca *online* di dimensioni molto grandi (*Very Large Online Search Engines* o VLOSE), che raggiungono in media più di 45 milioni di utenti, sono soggetti ad una regolamentazione più rigorosa.

[39] *Id*., art. 3, lett. h).

[40] Il regolamento si limita a fornire alcuni esempi dei contenuti che dovrebbero rispecchiare la nozione. *Id.*, 12° "considerando".

[41] *Id*., art. 34. In dottrina, M.C. BUITEN, *The Digital Services Act*, cit.

© Wolters Kluwer Italia

idee e opinioni non garantisce un'informazione plurale di qualità, le istituzioni europee, in luogo di un approccio repressivo orientato dall'alto verso il basso, hanno preferito intraprendere la strada del dialogo. Tuttavia, le osservazioni critiche rimarcano come il regolamento sui servizi digitali si mostri più attento all'apparato procedurale che alla dimensione sostanziale di definizione dei contenuti vietati. Ne deriva che il controllo contenutistico delegato alle piattaforme digitali fa sì che queste agiscano come legislatori privati tanto da provocare una "privatizzazione della censura" [42].

In realtà, il regolamento offre soluzioni che contemperano questo rischio, quali la previsione di "punti di contatto" con le autorità degli Stati membri e la Commissione (art. 11) o le istituzioni di autorità competenti incaricate della vigilanza dei fornitori di servizi intermediari (artt. 49 e 61). A parere di chi scrive considerare la scelta di favorire un rapporto di interdipendenza tra attori privati e attori pubblici come una rischiosa delega in bianco è una conclusione troppo severa, dal momento che permette ai poteri pubblici di ritagliarsi degli spazi di intervento in una realtà da sempre dominata dai privati.

[42] M. Monti, *La disinformazione online, la crisi del rapporto pubblico-esperti e il rischio della privatizzazione della censura nelle azioni dell'Unione Europea (Code of practice on disinformation)*, in *Federalismi.it*, 11/2020, pp. 281-305.

© Wolters Kluwer Italia

E-HEALTH E IA GENERATIVA. UN RICHIAMO ALLE PIÙ ALTE GARANZIE NELLA CURA DELLA PERSONA *

LUIGI PROSIA

SOMMARIO: 1. Definizioni e delimitazioni teoriche. – 1.1. Dall'IA classica a quella generativa. – 1.2. Il futuro della medicina. – 2. Tra percorsi storici, innegabili opportunità e rischi (sempre più) concreti. – 3. Segue: le cc.dd. vulnerabilità digitali. – 4. Alcuni buoni propositi.

Abstract: Technological innovation, which penetrates new sectors every day, is preparing to revolutionise the health sector as well, offering citizens unprecedented care paths. These paths are personalised and tailored, based on ease of access, and oriented towards the use of algorithms in support of medical diagnosis and scientific research. On the one hand, the remote delivery of medical services (so-called telemedicine) can limit the waste and inefficiencies of the public system, making it possible to benefit from the best specialised expertise regardless of the distance between professional and patient; on the other hand, generative AI promises to lighten the workload of operators, enhance analysis protocols and increase productivity. However, the objectives of efficiency, savings and territorial standardisation through digitisation and the development of AI solutions must be combined both with the principles of equality and universalism, which are being severely tested by cultural, generational, economic and technological gaps, and with a model for designing personal care according to accuracy, reliability, transparency and, above all, data security.

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

1. Definizioni e delimitazioni teoriche

Fornire una definizione univoca di *e-health* (o sanità digitale) costituisce un'impresa in bilico tra l'eccessiva semplificazione e l'incompletezza per via del tumultuoso incedere delle nuove tecnologie, che mettono di continuo in discussione categorie giuridiche e non da tempo stabili. È preferibile limitarsi a identificare l'*e-health* con il risultato dell'applicazione al settore sanitario dell'*Information and Communication Technologies* (ICT) al fine sia di erogare attività di prevenzione, diagnosi e cura da remoto delle malattie, sia di potenziare processi operativi e funzioni amministrative di supporto digitalizzando le informazioni relative ai pazienti [1]. I *social network*, ad esempio, configurano un terreno fertile per la diffusione di campagne di sensibilizzazione e raccolta fondi a favore della ricerca scientifica, operando talvolta come una precondizione della salute.

Laddove le stesse *ICT* servano al ramo sanitario per sviluppare macchine in grado di interagire e apprendere dall'ambiente esterno, arrivando ad assumere decisioni più o meno autonome con complessa imputazione della relativa responsabilità, si sconfina nel diverso campo dell'intelligenza artificiale (IA), rimandando attualmente tale locuzione a una famiglia di tecnologie progettate per funzionare con un certo grado di autonomia rispetto al coinvolgimento umano e con livelli variabili di adattabilità al contesto in cui operano. Il fine è di dedurre dalla mole sterminata di dati che ricevono come *input* la maniera più opportuna per generare *output* rilevanti quali previsioni, contenuti, raccomandazioni o decisioni in grado di influenzare ambienti fisici e/o virtuali (cfr. l'art. 3, par. 1, del regolamento UE 2024/1689) [2].

1.1. *Dall'IA classica a quella generativa*

La grande capacità inferenziale delle odierne tecnologie di IA è il risultato di un passaggio di paradigma nel programmare l'IA stessa:

---

[1] Per un'analisi critica delle tecnologie informazionali come fonti di ricchezza, salute e potere, v. G. SARACENI, ICT (voce), in A.C. AMATO MANGIAMELI - G. SARACENI (a cura di), *Cento e una voce di informatica giuridica,* Torino, 2023, pp. 258-261.

[2] Cfr. A.C. AMATO MANGIAMELI, *IA e diritto. In luogo di una introduzione, in Journal of Ethics and Legal Technologies*, 2/2023, pp. 81-93, in part. p. 86, la cui immagine della "stanza di Google" rappresenta bene la capacità dell'IA di estrapolare da grandi quantità di dati singole porzioni di informazione da collegare e incrociare per suggerire agli uomini modelli di interpretazione e azione.

© Wolters Kluwer Italia

non più un approccio logico-deduttivo, come per Deep Blue che gioca a scacchi, bensì statistico-esperienziale [3]. La macchina "impara" direttamente dai dati, con o senza supervisione, e l'esattezza delle risposte migliorerà al crescere sia della quantità che della qualità degli esempi di volta in volta acquisiti (c.d. *training set*). In tal modo, arriverà a fare scelte persino in condizioni di incertezza, sebbene non abbia preventivamente ricevuto le possibili chiavi di risoluzione del problema sotto forma di operazioni e regole prestabilite. Non vanno però tralasciate le criticità – a cui, qui, si accenna solamente – legate alla mancanza di una spiegazione del perché sia giunta a quella particolare predizione, e legate al fatto che l'intrinseca opacità non consente agli individui, più o meno esperti, di ripercorrere i passaggi svolti per ottenere un determinato *output* [4]. Di qui, il rischio di scambiare errori e distorsioni per soluzioni affidabili.

Ad ogni modo, provando a individuare il minimo comune denominatore di questa eterogeneità di applicazioni, che differiscono a seconda della tipologia di programmazione e funzionamento degli algoritmi alla base, esso risiede nella capacità di simulare i naturali processi cerebrali, *rectius* l'abilità dell'uomo a usare mente e corpo per pensare, sperimentare e agire, al punto da rendere impossibile la distinzione tra l'uomo medesimo e l'entità artificiale; proprio come avviene nel corso del test di Turing, padre della teoria computazionale (attraverso il codice binario), quando l'esaminatore fa fatica a riconoscere chi dei due interlocutori sia meccanico [5]. Non a caso, gli obiettivi a lungo termine dell'IA, fissati durante la conferenza di Dartmouth del 1956 (data alla quale si riconduce la sua nascita), ruotano tutti intorno alla realizzazione di macchine per svolgere funzioni che implichino aspetti profondamente umani: dalla classificazione alla pianificazione, dalla traduzione all'apprendimento, sino alla comprensione [6].

D'altra parte, si mostra più arduo fornire una definizione compiuta di IA, accettata e condivisa dall'intera comunità scientifica, a causa

---

[3] Cfr. A. Simoncini - S. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Riv. fil. dir.*, 1/2019, pp. 87-106.

[4] Da tale oscurità discende l'immagine della *black box* (scatola nera sigillata), rispetto alla quale il riferimento è specialmente a F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge, Massachusetts, 2016.

[5] A.M. Turing, *Computing Machinery and Intelligence*, in *Mind*, 236/1950, pp. 433-460.

[6] J. McCarthy - M.L. Minsky - N. Rochester - C.E. Shannon, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. August 31, 1955*, in *AI Magazine*, 4/2006, pp. 12-14.

© Wolters Kluwer Italia

dell'ambiguità del concetto stesso di intelligenza, ovvero di quel potenziale innato necessario agli uomini per formulare valutazioni giuste, profittare dell'esperienza e risolvere adeguatamente problemi [7]. Quest'ultima si connota di molteplici e variamente complessi elementi: alcuni, per così dire quantificabili e misurabili, sono più agevolmente di altri, attinenti al giudizio morale e/o allo spirito divergente, trasferibili nei sistemi artificiali. D'altronde, è difficile – almeno per ora – che una macchina possa acquisire una comprensione olistica del mondo, che le consenta di leggere tra le righe, di cogliere le sfumature o le implicazioni non dette, come pure di fare connessioni emotive. Inoltre, per quanto avanzata possa essere, la scintilla creativa è qualcosa che ancora non le appartiene.

L'IA, dunque, comprende due versanti strettamente correlati: da un lato, la c.d. scienza cognitiva, volta ad approfondire i principi che rendono possibile un comportamento intelligente per formalizzarli matematicamente in applicazioni informatiche; dall'altro, l'IA in senso stretto, che si occupa delle tecnologie per tali applicazioni, assumendo ora una connotazione "forte" (quando pretende di duplicare la mente nei dispositivi), ora "debole" (se svolge prestazioni normalmente attribuite all'uomo con più velocità ed efficienza non imitandone generalmente le funzioni cerebrali), ora ancora "generativa", facendosi da ultimo riferimento a una sottocategoria dell'IA classica che sembra conoscere le risposte a domande di qualsiasi tipo, coadiuvando l'utente nel risolvere alcuni quesiti pratici della quotidianità. Basti menzionare il *software* ChatGPT, ideato dalla società di ricerca statunitense OpenAI, al fine di riprodurre una conversazione con un essere umano e suggerire alle volte piani di azione [8].

1.2. *Il futuro della medicina*

Date le innegabili opportunità che tutte queste nuove tecnologie possono dispiegare in termini di riduzione dei tempi, accuratezza dei risultati e portabilità dei flussi informativi, se ne registra un notevole impiego anche nel campo medico, ove stanno accelerando il virtuoso cammino dell'assistenza sanitaria sempre più preventiva, predittiva,

---

[7] Cfr. M. IASELLI, *Le profonde implicazioni di carattere etico e giuridico dell'intelligenza artificiale*, in *Democrazia e diritti sociali*, 2/2020, pp. 79-102, in part. p. 80.

[8] Cfr. A.C. AMATO MANGIAMELI, *Intelligenza artificiale generativa: brevi note*, in *L'Ircocervo*, 1/2024, pp. 101-111.

© Wolters Kluwer Italia

partecipata e personalizzata. L'IA generativa, nello specifico, purché non aspiri a sostituirsi completamente alla conoscenza e all'esperienza del "vero" professionista della salute, costituisce un promettente strumento di supporto alla cognizione umana della diagnosi e del piano di cura, agevolando compiti gravosi inerenti, per esempio, le procedure di *imaging* medico (raggi X, risonanze magnetiche, ultrasuoni, scansioni TC), che risultano di sicuro accelerate, e riducendo al contempo l'incidenza di errori terapeutici: piccole alterazioni che possono sfuggire all'occhio umano vengono quasi certamente individuate dalla macchina [9].

L'IA generativa può rappresentare altresì una formidabile alleata nella fase di gestione della malattia conclamata, aumentando il coinvolgimento del paziente nel suo percorso di guarigione e alleggerendo di riflesso il carico di lavoro degli operatori sanitari. Si guardi, a tal proposito, anche all'impiego della robotica nell'assistenza domiciliare a pazienti (e anziani) non autosufficienti, oltre che nel loro percorso di rieducazione e riabilitazione. È il caso dei cc.dd. *social robot* capaci di ricordare a intervalli predefiniti l'assunzione di farmaci, di registrare e trasmettere a distanza dati sullo stato di salute, di analizzare i volti per comprendere lo stato emotivo delle persone osservate fino a manifestare una sorta di empatia artificiale [10]. D'altro canto, Da Vinci, Star, Excelsius GPS e altri sistemi robotici forniscono da tempo sostegno all'azione degli operatori umani nelle sale operatorie dei Paesi più tecnologicamente avanzati.

Se così stanno le cose, pare essere giunto il momento di una svolta della risposta terapeutica, che chiede di essere ridisegnata nei suoi caratteri fondamentali: aprirsi a percorsi di cura a distanza, o meglio di accompagnamento quotidiano nel decorso della malattia da remoto, in particolare di persone fragili o affette da patologie croniche, e non basarsi più solo su interventi chirurgici e/o farmacologici fruiti all'interno di apposite strutture ospedaliere da decongestionare. Siamo ormai dinanzi a una transizione epidemiologica [11] che rischia di compro-

---

[9] Sulle potenzialità tangibili che i sistemi intelligenti sono in grado di dispiegare nel campo medico, si rimanda a C. Nasi, *Generative IA: il futuro della medicina tra opportunità e sfide per i diritti fondamentali*, in *Riv. it. med. leg.*, 2/2023, pp. 319-338.

[10] Il passo ulteriore, non più tanto utopico, è quello dell'uomo-robot (o *cyborg*), simbolo della meccanizzazione del corpo, in quanto portatore di *pacemaker* o dotato di protesi tecnologiche, se non addirittura di *neurochip* BCI (*brain computer interface*). In merito, si rimanda a S. Bauzon, Cyborg (voce), in A.C. Amato Mangiameli - G. Saraceni (a cura di), *Cento e una voce di informatica giuridica,* cit., pp. 123-125.

[11] Cfr. A. Omran, *The Epidemiologic Transition: A Theory of the Epidemiology of Population Change*, in *The Milbanck Quarterly*, 4/2005, pp. 731-757.

© Wolters Kluwer Italia

mettere la stessa efficacia dei trattamenti erogati nelle modalità tradizionali, mentre sia le *ICT* che le tecnologie di IA promettono di rimediare ad alcuni dei mali che affliggono l'area medico-sanitaria degli odierni Stati industrializzati già da svariati periodi, primo fra tutti le ospedalizzazioni superflue.

2. Tra percorsi storici, innegabili opportunità e rischi (sempre più) concreti

Gli strumenti offerti dalla rivoluzione informatica, come pure le dirompenti tecnologie di IA, soccorrono oggi per conseguire l'obiettivo di una sanità più adeguata e sostenibile, capace cioè di reagire a fattori come l'invecchiamento della popolazione, la resistenza alle cure antibiotiche e il contestuale aumento delle patologie cronico-degenerative in luogo di quelle infettive. Nel concreto, l'idea alla base della virtualizzazione e/o artificializzazione degli approcci terapeutico-assistenziali risiede nell'intento di limitare gli sprechi e di ridurre le inefficienze che da anni investono la sanità pubblica, così come nello sviluppo di una gestione sempre più integrata delle condizioni cliniche, secondo il modello delle reti per patologia, al di là delle possibili differenze (e iniquità) territoriali. L'aspirazione condivisa è quella di dare impulso all'innovazione agevolando l'accesso a prestazioni mediche di alta qualità allo stesso modo in ogni regione.

Queste istanze di riconcettualizzazione del rapporto medico-paziente hanno assunto un ruolo determinante con l'emergere della telemedicina, a partire dalla metà del secolo scorso, quando sono stati concepiti alcuni progetti sperimentali per affrontare situazioni di emergenza, come quelle derivanti da disastri naturali, ovviando alla criticità di trovarsi fisicamente in luoghi diversi da quelli colpiti, per esempio, da un'inondazione o un terremoto. Non è un caso che le prime applicazioni di tali pratiche, sorte dal peculiare incontro di medicina e telematica, siano state finanziate negli anni '60 dalla NASA per fornire soccorso a distanza agli astronauti in missione orbitale.

Nei decenni successivi, in corrispondenza al progressivo aumento della capacità di trasmissione dei dati per via telematica e alla parallela riduzione dei costi dei dispositivi elettronici, compresi i sensori indossabili, impiantabili e persino ingeribili, ne è seguita una vera e propria proliferazione, spostando il fulcro di questa innovativa concezione di intervento sanitario dal livello specialistico-ospedalie-

© Wolters Kluwer Italia

ro a quello territoriale dell'assistenza primaria e, in determinati casi, direttamente al domicilio dell'ammalato [12].

Più di recente, la telemedicina, ovvero l'insieme di interazioni tra professionista della salute e paziente (o due professionisti) consentite e mediate dalle *ICT*, nonché dirette allo scambio di informazioni a carattere medico sotto forma di testi, suoni, immagini o altre forme utili a monitorare proattivamente la salute degli individui, ha disvelato tutto il suo grande potenziale nel corso della pandemia, quando la necessità di arginare il contagio tramite il distanziamento sociale ne ha determinato un uso massiccio. Le nuove tecnologie sono state impiegate innanzitutto per attività di prevenzione collettiva, si vedano le *app* per il *contact tracing* dei pazienti positivi al Covid-19; in secondo luogo, per garantire la continuità delle cure a tutti, restringendo i flussi da e verso gli ospedali e convertendo digitalmente molti servizi ordinari, come le visite (con annessa prenotazione telematica) o la valutazione dei referti diagnostici, che sono stati presto adattati alle misure di sicurezza necessarie a fronteggiare l'epidemia, con notevoli benefici anche rispetto alla raccolta e alla conservazione dei documenti. Di fronte all'assorbimento eccezionale di risorse umane, strumentali e organizzative, la sanità è stato il settore con il fabbisogno più alto di soluzioni alternative, arrivando a sperimentare inediti paradigma di relazione tra utenti, personale medico-infermieristico, imprese, pubblica amministrazione e chiunque altri fosse coinvolto nella presa in carico dei pazienti [13].

Proprio l'emergenza pandemica, che ha risvegliato molti dal sonno digitale, ha però evidenziato una generale impreparazione del sistema sanitario nazionale (SSN) rispetto ai servizi resi *online*, dovuta tanto alla mancanza di un quadro di riferimento normativo chiaro (al tempo esistevano solo le *Linee di indirizzo nazionali sulla telemedicina* risalenti al 2014), quanto all'assenza di una programmazione organica,

---

[12] C. Botrugno, *Telemedicina ed emergenza pandemica: un grande rimpianto per il nostro Paese*, in *BioLaw Journal-Rivista di BioDiritto*, special issue, 1/2020, pp. 691-696, in part. p. 692. I cc.dd. *wearable device* rientrano nella categoria dell'*m-health* (*mobile health*) potendo essere utilizzati tanto per l'erogazione da remoto delle prestazioni da parte degli operatori sanitari, o meglio in loro supporto, quanto per la misurazione da sé stessi di alcuni parametri di salute legati, per esempio, all'attività fisica o ai comportamenti alimentari.

[13] Oggi la pratica dei consulti a distanza, sebbene non opportuna per ogni patologia, resta parecchio proficua in determinati settori (per esempio, quello dermatologico o psicanalitico), talvolta in termini di primo approccio, talaltra di preludio a una visita tradizionale, talaltra ancora come ambito elettivo dell'intera terapia, cfr. G. Saraceni, ICT (voce), cit., p. 259.

© Wolters Kluwer Italia

venendo la disponibilità a curare da remoto rimessa spesso all'iniziativa di singole unità operative, con inevitabili disparità di accesso all'offerta assistenziale da parte delle persone. Più in generale, è emerso quanto l'utilizzo non governato delle tecnologie ne accentui l'ambivalenza: a fronte degli indiscutibili vantaggi in termini di ammodernamento, contenimento della spesa inappropriata e miglioramento delle prestazioni cliniche in qualità ed efficienza, molteplici sono anche i profili problematici:

a) dapprima, il rischio di compromissione della fiducia che connota il rapporto diretto tra medico e paziente nella misura in cui la perdita del contatto fisico – un po' come accaduto in passato con lo stetoscopio utilizzato per non accostare più l'orecchio al torace del malato – comporta la standardizzazione e conseguente depersonalizzazione delle cure, somministrate in "taglia unica" a tutti gli individui [14]. La tecnologia, invece, dovrebbe facilitare e arricchire questo legame fiduciario rendendo la comunicazione più accessibile, conveniente e aperta, al di là dell'ambito ristretto del consenso informato, che non di rado viene interpretato dal professionista della salute in una logica difensiva piuttosto che di dialogo e condivisione con l'utente. Proprio la comunicazione, pur posta l'irritualità del mezzo digitale, rappresenta il veicolo dell'informazione, che a sua volta è il presupposto del consenso all'atto medico inteso come processo relazionale di decisione tra sanitari, ammalato e suoi familiari [15];

b) poi, la sfida della sicurezza dei dati, per lo più di natura sensibile, in particolare quando le diverse applicazioni tecnologiche, pur non assumendo i connotati di prestazione mediche *stricto sensu*, siano strumentali alla corretta fruizione delle stesse. Basti pensare alla raccolta in forma integrale dei dati del paziente all'interno di un fascicolo sanitario elettronico; all'emissione delle prescrizioni mediche e dei certificati di malattia in formato digitale (c.d. *e-prescribing*); alla gestione informatizzata della cartella clinica. Trattasi di circostanze nelle quali, per salvaguardare la dignità del cittadino bisognoso di aiuto – già di suo fragile –, andrebbe adottato un metodo di progettazione dei servizi che consideri la tutela della sua *privacy* quale elemento essenziale

[14] Sui molteplici interrogativi di carattere (bio)etico posti in generale dall'incedere delle nuove tecnologie applicate alla vita degli esseri umani, v. P.B. HELZEL, *Quale bioetica nell'era dell'intelligenza artificiale?*, in *Politica.eu*, numero speciale, settembre 2023, pp. 28-52.

[15] Cfr. M. FOGLIA, *Consenso e cura. La solidarietà nel rapporto terapeutico*, Torino, 2018.

© Wolters Kluwer Italia

per impostazione predefinita, come vuole anche la normativa europea sulla protezione dati (cfr. l'art. 25 del regolamento UE 2016/679 sulla protezione dei dati, detto anche GDPR) [16];

c) da ultimo, qualora i pazienti versino in condizioni di vulnerabilità ulteriori rispetto alla malattia, quali risorse economiche insufficienti, età avanzata o scarsi livelli di conoscenze/competenze digitali [17], la possibilità di avvantaggiare quanti si trovino di per sé in una situazione per così dire di generale benessere, impedendo di fatto l'attuazione uniforme della garanzia costituzionale della salute come diritto fondamentale dell'individuo e interesse della collettività *ex* art. 32 Cost. sull'intero territorio nazionale.

3. Segue: le cc.dd. vulnerabilità digitali

L'applicazione dei nuovi strumenti tecnologici al settore sanitario, cui si accompagna necessariamente l'emersione di una nuova *forma mentis* del personale medico e paramedico, richiede una grande attenzione quando è potenzialmente in grado di compromettere diritti fondamentali della persona, come il diritto a non essere discriminati per ragioni razziali, di genere o socioeconomiche, oppure quello alla salute. Dal punto di vista etico-giuridico, infatti, il ricorso a *chatbot* e algoritmi avanzati suscita perplessità non di poco conto nei casi in cui possa dare luogo alle cc.dd. vulnerabilità digitali.

Si pensi a come un eccessivo affidamento della prestazione intellettuale al parere dato dalla macchina, con contestuale attenuazione del pensiero critico, possa essere foriero di pregiudizi derivanti da addestramenti della macchina stessa effettuati con dati non rappresentativi dell'intera popolazione a cui è destinata. Il rischio è che il sistema artificiale, allenato con un bacino ristretto e non diversificato di informazioni sanitarie, ad esempio solo quelle provenienti dai Paesi ad alto reddito, laddove utilizzato in maniera indiscriminata e incontrollata, possa minare l'integrità psico-fisica degli individui, determinando il

[16] Per un approfondimento sul tema, v. G. Fioriglio, *E-health: profili informatico-giuridici*, in Th. Casadei - S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, II ed., Milano, 2024, pp. 59-74.

[17] Sul significato plurale del divario digitale, che intercorre tra maschi e femmine, giovani e vecchi, nativi digitali e generazione *boomer*, lavoratori e disoccupati, e così via, cfr. G. Saraceni, *Digital Divide e povertà*, in *Dirittifondamentali.it*, 2/2019, pp. 1-19.

© Wolters Kluwer Italia

sorgere di importanti profili di responsabilità medica [18]. Ne consegue per il professionista con dotazioni tecnologiche una significativa estensione del suo *standard* di diligenza.

In senso più ampio, per evitare simili derive, e quindi ridurre al minimo il verificarsi di lesioni alle libertà e ai diritti fondamentali, è necessaria tanto una formazione specifica del personale sanitario, che in tempi presumibilmente brevi dovrà perfezionarsi nel settore delle tecnologie di IA, quanto una profonda consapevolezza delle ricadute che il loro uso può comportare sull'utente. Questi, magari per evitare i costi o i tempi di attesa associati alla visita presso un medico in carne e ossa, potrebbe fidarsi ciecamente del consiglio sanitario generato da ChatGPT in base ai propri sintomi, non preoccupandosi affatto delle rappresentazioni inique della realtà che potrebbero manifestarsi. Di qui, un insolito capovolgimento nell'agire del medico, che potrebbe vedersi costretto a correggere informazioni, più o meno attendibili, già acquisite dal paziente. D'altro canto, la cura della persona esige un grado elevato di accuratezza, affidabilità, trasparenza e soprattutto sicurezza [19], cioè di quell'insieme di garanzie che il nuovo regolamento UE sull'IA mira a consolidare attraverso regole proporzionate e flessibili, ossia calibrate sul rischio specifico posto da una nuova e versatile generazione di prodotti e servizi ad alto tasso tecnologico, che non vanno certamente osteggiati, bensì accolti e quanto più possibile governati.

4. Alcuni buoni propositi

Da quanto sopra esposto, è di solare evidenza come l'innovazione tecnologica si appresti a rivoluzionare l'ambito sanitario, offrendo al cittadino inediti percorsi di cura: personalizzati e di precisione, basati sulla facilità di accesso, nonché orientati all'utilizzo di algoritmi in supporto alla diagnosi medica, che risulta potenziata, e alla ricerca scientifica, accresciuta nella sua produttività.

Gli obiettivi di efficientamento, risparmio e uniformazione territo-

---

[18] Cfr. G. COLLECCHIA, *L'intelligenza artificiale in medicina: limiti di big data e algoritmi*, in *quotidianosanità.it*, 20 aprile 2019, che si sofferma sulla necessità che i dati utilizzati per il processo di apprendimento della macchina vengano opportunamente selezionati, strutturati e interpretati affinché possano risultare utili.

[19] Sugli attacchi informatici alle strutture sanitarie e sulla necessità di azioni preventive e di reazione, si rimanda a G. ZICCARDI, *Dati avvelenati. Truffe, virus informatici e falso online*, Milano, 2024, in part. pp. 107-118.

© Wolters Kluwer Italia

riale attraverso la digitalizzazione e lo sviluppo di soluzioni di IA devono però coniugarsi – come sopra illustrato – sia con i principi di uguaglianza e universalismo messi a dura prova dagli attuali divari culturali, generazionali, economici e tecnologici, sia con un modello di progettazione e implementazione dei servizi che ponga la sicurezza dei dati, in unione con la loro esattezza, a presidio sostanziale della dignità umana.

Ciò equivale a riconoscere che quanto svolto attraverso gli strumenti di sanità digitale, IA compresa, configura comunque un atto medico, del quale occorre rispettare sempre finalità, caratteristiche e obbligazioni. In realtà, se pensata come mera componente aggiuntiva, la virtualizzazione e/o automazione degli approcci terapeutici potrebbe migliorare di molto l'adeguatezza e l'interoperabilità della stessa pratica clinica tradizionale, senza per questo arrivare a sostituirla.

Ciò equivale altresì a dire che, una volta riconosciuta la sua funzione ausiliaria, in mancanza di un adeguato nucleo regolatorio del connubio tra sanità e innovazione tecnologica, ben inserito nel contesto delle fonti e non affidato a mere linee guida o di indirizzo come quelle vigenti [20], risulta difficile assicurare all'*e-health* una diffusione coerente con i principi cardine del diritto e dell'etica medica [21]. Poi, se in parallelo non viene attivato un piano appropriato di politiche e interventi in settori funzionalmente contigui, è dubbio che questa inedita concezione terapeutica possa integrarsi pienamente nell'intero comparto sanitario; anzi, già la sola emarginazione digitale, causata da fattori di diversa matrice, dunque non semplicemente infrastrutturali, potrebbe divenire il nuovo volto della negazione delle cure.

Se questo è il quadro, non si tratta più di mettere in discussione i nuovi orizzonti di sviluppo che *ICT* e tecnologie di IA (generativa e

---

[20] Il riferimento è alle *Indicazioni nazionali per l'erogazione di prestazioni di telemedicina* del 2020, che rappresentano un'evoluzione di quelle del 2014, e a cui si aggiungono le *Indicazioni per l'erogazione di prestazioni e servizi di teleriabilitazione da parte delle professioni sanitarie* del 2021. Di recente, in attuazione della missione 6 del PNRR, è stato emanato il decreto ministeriale del 21 settembre 2022 recante *Approvazione delle linee guida per i servizi di telemedicina-requisiti funzionali e livelli di servizio*, che di fatto riprende e rielabora molti dei contenuti delle precedenti linee guida.

[21] Sul filo sottile che unisce il diritto alla medicina, quali attività-per l'uomo e al suo servizio, dal momento che entrambe le discipline tendono a conservare l'ordine riconosciuto o a ripristinarlo, l'uno in relazione alla vita sociale, l'altra rispetto alla vita umana, oltre che sulla compenetrazione di conoscenze mediche e filosofiche, si rimanda alle riflessioni di A.C. Amato Mangiameli, *Natur@. Dimensione della Biogiuridica*, Torino, 2021, in part. pp. 1-19.

© Wolters Kluwer Italia

non) aprono al genere umano, o in generale di soffocare l'innovazione, bensì di vagliare sotto la lente giuridica i diversi profili di utilizzo, così da prevenire abusi o limitazioni dei diritti e delle libertà inviolabili. D'altronde, sin da quando ha avuto mezzi tecnici sufficienti, l'uomo si è sempre dedicato alla costruzione di macchine e meccanismi capaci di emulare alcune caratteristiche del suo intelletto (comprensione del linguaggio, apprendimento, *problem solving*, ecc.), e oggi (con lo sviluppo delle auto a guida autonoma, l'impiego di sistemi automatizzati nel settore economico e finanziario, il ricorso a *software* di riconoscimento facciale nella lotta al terrorismo, l'utilizzo della robotica nelle operazioni chirurgiche, nella rieducazione e riabilitazione dei pazienti), questa sua aspirazione sembra avere definitivamente abbandonato la dimensione fantascientifica per entrare a far parte a pieno titolo del mondo reale.

La prospettiva futura è allora quella di una continua collaborazione tra individuo e macchina, quasi una simbiosi, in cui ognuno svolgerà il proprio ruolo fondato sui propri punti di forza, contribuendo al conseguimento di una vasta gamma di benefici a livello economico, ambientale e sociale, entro l'ampio spettro delle attività umane (cfr. il 4° "considerando" del regolamento UE 2024/1689); una prospettiva, questa, ancora più preziosa per il settore sanitario che, per sua natura, vive del progresso scientifico e di investimenti in ricerca e sviluppo allo scopo di elevare il livello generale di vita degli individui.

© Wolters Kluwer Italia

UNIONE EUROPEA, "*CYBER THREATS*" E SANZIONI: UN APPROCCIO MULTIFASE *

LORENZO CORDA

SOMMARIO: 1. Un "cyber" panorama in cambiamento: la *EU cybersecurity law* nella sua svolta esterna. – 2. Cenni generali sulle misure restrittive dell'Unione e specifici sul regime di sanzioni cyber. – 2.1. I cyberattacchi quali "*minacce esterne*" ai sensi della decisione (PESC) 2019/797. – 2.2. Attacchi "significativi". – 3. Considerazioni conclusive.

Abstract: The cyber domain hosts both public and private actors in a continuous exchange of information. As such, it has a role to play in areas ranging from banking operations to the proper functioning of essential infrastructures and services, as well as in the transparent and impartial access to digital media. The potential for cyberattacks to breach this network and to cause widespread damage asks for a proactive management of cyber risks. Against this background, the European Union is a key actor in defining measures to mitigate risks common to its Member States. One way to achieve this, downstream, involves imposing cyber-specific sanctions on perpetrators and facilitator of cyberattacks. The Russian aggression against Ukraine has further transformed the landscape of malicious cyber activities, increasing both their scale – marked by the rise of (para)state actors – and their complexity, with the rapid advancement of tools. Notably, this evolution has introduced sophisticated malicious techniques that, among other challenges, complicate the attribution of attacks. This paper provides, on the one hand, a critical review of EU cyber-related sanctions in light of their recent activation, and on the other hand, an analysis of the legal notions involved, with a particular focus on the definition of a significant cyberattack.

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

1. Un "cyber" panorama in cambiamento: la *EU cybersecurity law* nella sua svolta esterna

La quasi totalità dei cittadini degli Stati membri dell'Unione europea fa ampio affidamento su dispositivi tecnologici digitali basati sul dominio informatico (cyber dominio, cyberspazio). Ciò risulta particolarmente vero alla luce di un processo di forte digitalizzazione *quantitativa* e *qualitativa* che ha alterato il rapporto che ogni persona nell'Unione intrattiene con lo Stato mediante i servizi da esso erogati. Di conseguenza, le branche del diritto pubblico, in particolare penale, internazionale ed europeo, sono chiamate a una rincorsa costante per arginare i rischi a cui la dimensione informatica espone: le cc.dd. *cyber threats*, di cui gli attacchi informatici (o cyberattacchi) rappresentano il picco della gravità.

Di pari passo con i fenomeni di cui sopra, ha preso da tempo piede la tendenza a sfruttare le brecce nella rete per finalità criminali. Ripercorrendo le maglie del sistema, malintenzionati compromettono il funzionamento dei servizi pubblici e attività economiche, causando perdite finanziarie e danneggiando l'interconnessa struttura informatica dell'Unione. Nei casi peggiori sono contemplate conseguenze gravi, se non addirittura letali, per la salute dei cittadini.

Il legislatore dell'Unione ha dunque approvato atti derivati per fare fronte a minacce cibernetiche, in un *corpus* di legislazione frammentata nelle basi legali che la dottrina definisce "*EU cybersecurity law*" [1]. Nel tempo, la mancanza di una competenza nella cybersicurezza *per sé* nei Trattati ha indotto le istituzioni europee a sviluppare un nesso logico-funzionale tra questa e diverse basi legali adottate [2]. In un costante intento della disciplina di connettere il mantenimento del corretto funzionamento del mercato interno alla cybersicurezza [3], l'art. 114 TFUE emerge quale base principale, vista anche la posizione benevola della Corte in tal senso [4]. Un secondo insieme di atti armonizza sanzioni

---

[1] R.A. WESSEL, *European law and cyberspace*, in N. TSAGOURIAS - R. BUCHAN (eds.), *Research Handbook in International Law and cyberspace*, Cheltenham, 2021, p. 507.

[2] V. la risoluzione del Parlamento europeo del 23 novembre 2016 sull'attuazione della politica di sicurezza e di difesa comune (sulla base della relazione annuale del Consiglio al Parlamento europeo sulla politica estera e di sicurezza comune), 2016/2067(INI). In particolar modo "*(...) la sicurezza e la difesa informatiche devono pertanto essere [...] integrate pienamente in tutte le politiche interne ed esterne dell'Unione*".

[3] R.A. WESSEL, *European law and cyberspace*, cit., pp. 501 ss.

[4] C. giust. UE, 2 maggio 2006, C-217/04, *Regno Unito* c. *Parlamento europeo e Consiglio*.

© Wolters Kluwer Italia

per i reati transfrontalieri nel cyber dominio ai sensi degli artt. 82, par. 2, e 83, par. 1, TFUE.

L'imposizione di obblighi adeguati ai corretti attori in gioco con gli strumenti legali adatti rappresenta per l'Unione una delle sfide maggiori nella regolamentazione del cyber dominio [5]. La disciplina ha perseguito questo fine, *extrema ratio*, mediante inasprimenti giuridici attuati nell'ambito della Politica Estera e di Sicurezza Comune (PESC), nella quale l'UE si ritaglia competenza in "*tutte le questioni relative alla sicurezza dell'Unione*", cybersicurezza compresa.

Prendendo spunto da recenti avvenimenti, sarà cura di questo contributo inquadrare le misure restrittive adottate dall'Unione come parte di una rinnovata "esternalizzazione" della *EU cybersecurity law*. Si rifletterà in particolare sulla nozione di cyberattacchi significativi quali minaccia esterna, sulla sua specificità e sui suoi limiti. Tale concezione è un importante riferimento legale per la disciplina, per la sua estensiva (seppur vaga) formulazione così come per la sua unicità per l'azione esterna dell'Unione. A titolo di esempio, una sua maggiore comprensione potrebbe fornire "guidance on the legal notion of cyber-attacks and their relevance to the EU" in generale [6].

2. Cenni generali sulle misure restrittive dell'Unione e specifici sul regime di sanzioni cyber

Per quanto riguarda il fronte "punitivo" del diritto, all'Unione è permesso adottare misure restrittive, ovvero sanzioni, mirate contro entità e persone o settori economici di Stati terzi.

Il 24 giugno 2024 sono stati approvati due atti, la decisione (PESC) 2024/1779 e il regolamento di esecuzione (UE) 2024/1778 [7], il cui scopo è multifase: prevenire, scoraggiare e contrastare attività in-

---

[5] G. Fuster - L. Jasmontaite, *Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights*, in M. Christen - B. Gordijn - M. Loi (eds.), *The Ethics of Cybersecurity*, Cham, 2020, p. 109.

[6] E. Suwara, *Cyber operations and Article 42.7 of the Treaty on European Union*, in *Krakow International Studies*, 1/2022, p. 88.

[7] Decisione (PESC) 2024/1779 del Consiglio, del 24 giugno 2024, che modifica la decisione (PESC) 2019/797, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, in G.U.U.E. L/2024/1779 del 24 giugno 2024, pp. 1 ss.; regolamento di esecuzione (UE) 2024/1778 del Consiglio, del 24 giugno 2024, che attua il regolamento (UE) 2019/796, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, in G.U.U.E. L/2024/1778 del 24 giugno 2024, pp. 1 ss.

© Wolters Kluwer Italia

formatiche malevoli, dolose e significative dirette a Stati membri, all'Unione e organizzazioni internazionali e Stati terzi. Gli atti del 2024 emendano la legislazione quadro della decisione (PESC) 2019/797 e del regolamento (UE) 2019/796 [8], ampliando la lista nera di cui all'Allegato I [9]. Le misure sono individuali e afferiscono alla macroarea legale dell'azione esterna, disciplinata nei Trattati dal Titolo V TUE e dalla Parte V TFUE.

Infatti, da una parte le sanzioni considerate sono inevitabilmente legate alla PESC [10], in quanto è competenza degli Stati membri impedire "*l'ingresso e il transito*" a persone o entità colpite [11]. Esse sono introdotte *ex* art. 29 TUE mediante atti legali [12], decisioni PESC, e come tali perseguono obiettivi e sottostanno ai principi generali di cui all'art. 21, par. 2, TUE [13].

D'altra parte, la prassi vuole che all'atto PESC segua un regolamento *ex* art. 215 TFUE vincolante per gli Stati membri [14] ad implementarne il contenuto [15] per attuare sanzioni nella forma di congelamento di beni e proibizione di messa a disposizione di fondi nell'ambito della Politica Commerciale Comune. I due atti citati, identici per bersagli e misure, mostrano lievi differenze [16]: per semplicità, ci si ri-

---

[8] Decisione (PESC) 2019/797 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri e regolamento (UE) 2019/796 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, entrambi in G.U.U.E. L129 del 17 maggio 2019, pp. 13 ss. e pp. 1 ss.

[9] L'Allegato I, lett. A), contiene la lista delle persone sanzionate, mentre l'Allegato I, lett. B), l'elenco delle entità.

[10] Disciplinata dagli artt. 23-46 TUE.

[11] Art. 4, par. 1, decisione (PESC) 2019/797.

[12] Le decisioni PESC recanti sanzioni non sono atti legislativi: le procedure legislative non vengono contemplate. Si tratta di una delle "procedure specifiche" PESC di cui all'art 24, par. 1, TUE.

[13] L. LONARDO, *Common Foreign and Security Policy and the EU's external action objectives: an analysis of Article 21 of the Treaty on the European Union*, in *European Constitutional Law Review*, 3/2023, pp. 588-589. Le lett. a), b) e c) dell'art. 21, par. 2, TUE, sono tra quelle che rispecchiano meglio gli obiettivi di atti PESC.

[14] Art. 19, regolamento (UE) 2019/796.

[15] L. LONARDO, *EU Common Foreign and Security Policy After Lisbon*, Cham, 2023, p. 75. Stando all'art. 215 TFUE, la decisione PESC effettivamente deve anticipare il regolamento con base nel TFUE. Invece, secondo C. giust. UE, 30 settembre 2017, C-72/15, *PJSC Rosneft Oil Company* c. *Her Majesty's Treasury e altri*, par. 55, la decisione PESC antecedente è un vero e proprio prerequisito per "*la validità di un regolamento adottato in base all'articolo 215 TFUE*".

[16] Gli atti giuridici recanti sanzioni possono differire nel contenuto o non prevedere il regolamento *ex* art 215, in quanto misure restrittive di embargo o di divieto di

© Wolters Kluwer Italia

ferirà alla decisione (PESC) 2019/797 come emendata dalla decisione (PESC) 2024/1779.

Una particolarità del regime di sanzioni a tema cyber è il suo essere tematico in natura [17], per cui il quadro giuridico che ne risulta evita il bersagliamento diretto di Stati coinvolti in (tentati) cyber attacchi, la cui attribuzione di responsabilità rimane, come ribadito dalle linee guida in materia, "a sovereign political decision of Member States" [18]. Tuttavia, le sanzioni del 2024 bersagliano 4 individui russi e 2 ucraini vicini al Cremlino. Il nesso causa-effetto tra questo inasprimento giuridico e il panorama di cyber insicurezza dovuto alla guerra nel 4° "considerando" rende le recenti misure mirate implicitamente, ma chiaramente, alla Russia [19].

2.1. *I cyberattacchi quali "*minacce esterne*" ai sensi della decisione (PESC) 2019/797*

Andando con ordine, l'art. 1 della decisione (PESC) 2019/797 formula la nozione di cyberattacchi quali "*minaccia esterna*". Sin da subito, traspare l'intenzione del Consiglio di aver voluto elaborare criteri duttili e vaghi alla base di quest'ultima per garantire flessibilità all'impianto sanzionatorio [20].

Di per sé, la decisione (PESC) 2019/797 non sembra rifarsi ad altri atti di *EU cybersecurity law* e alle relative nozioni di minacce o attacchi informatici. Al contrario, ne elabora una versione a sé stante, a riprova della particolarità degli atti PESC recanti limitazioni invasive a persone e entità. È bene dire che ai fini della decisione (PESC) 2019/797, un cyberattacco comporta l'accesso o l'interferenza in sistemi di informazione; l'interferenza in dati o intercettazione di dati: per quanto rilevante in altre trattazioni, tale definizione tecnica ricoprirà un ruolo secondario.

Da una parte, una breve ma necessaria scorsa ad una diversa sezione della disciplina aiuta a contestualizzare la specificità e la rilevanza

---

transito e accesso nell'Unione possono costituire in sé sanzioni e dunque richiedere che venga approvata esclusivamente solo una decisione PESC.

[17] Un regime di sanzioni tematico o orizzontale non si applica direttamente a Stati terzi o a regioni. Al contrario, bersaglia violazioni prescindendo dai colpevoli o facilitatori delle stesse, siano essi attori (para-) statali o meno.

[18] General Secretariat of the Council, *Revised Implementing Guidelines of the Cyber Diplomacy Toolbox*, 8 June 2023, disponibile su: *www.consilium.europa.eu*.

[19] Così il 4° "considerando" della decisione (PESC) 2024/1779.

[20] R.A. Wessel - Y. Miadzvetskaya, *The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox*, in *European Papers.eu*, 1/2022, p. 430.

© Wolters Kluwer Italia

della nozione che verrà illustrata a breve. Per il rappresentativo regolamento (UE) 2019/881 ("atto sulla cybersicurezza") "*minaccia informatica*" è, sinteticamente, ciò che "*potrebbe danneggiare, perturbare o avere un impatto negativo [...] sulla rete e sui sistemi informativi, sugli utenti [...] e altre persone*" [21]. Si evince da ciò come tale atto appartenente ad una differente anima della *EU cybersecurity law ex* art. 114 TFUE (di cui all'introduzione), si concentri solo sul lato ricevente delle azioni malevoli informatiche, scorporando la nozione di "cyberattacco" dal protagonismo dei responsabili.

Dall'altra, la decisione (PESC) 2019/797 e il regime di sanzioni cyber, invece, sono nel contesto legale naturale per approfondire la nozione per il diritto europeo, quantomeno da un punto di vista geografico esterno, dovendo specificamente individuare i responsabili e bilanciare deterrenza a punizione.

Per il regime in oggetto, è da sottolineare infatti come l'origine esterna all'Unione degli attacchi sia *conditio sine qua non* affinché essi rappresentino "*minacce esterne*" e dunque rientrino nell'ambito di applicazione *ratione materiae* dei due atti che introducono sanzioni [22]. Gli aggressori – le strutture utilizzate con loro – devono situarsi in Stati terzi al momento del (tentato) attacco. Questo elemento, sovrapposto alle ragioni sottostanti alle sanzioni introdotte dalla decisione (PESC) 2024/1779 [23], conferma la correttezza dell'atto PESC. Al contempo, chiarisce come l'art. 75 TFUE, altra potenziale base legale per sanzioni dell'Unione relative al controterrorismo interno – area sovrapponibile se si prescindesse dall'origine – non sia stato adottato [24].

Una volta appurato ciò, l'attenzione passa alla soglia da superare degli effetti dei cyberattacchi, soglia che tradisce un bilanciamento con la scelta dei loro obiettivi.

Da una parte, gli attacchi rientrano nell'ambito di applicazione se

---

[21] E. FAHEI, *The EU as a Global Digital Actor*, Oxford, 2022, p. 95: "[A] new Cybersecurity Act in 2019 has shifted EU cybersecurity substantially towards the internal market", così come "[t]he key legal instrument of the EU's cyber law-making reforms in recent times is the Cybersecurity Act (...)". Art. 2, par. 8, regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (regolamento sulla cibersicurezza), in G.U.U.E. L151 del 7 giugno 2019, pp. 15 ss.

[22] Art. 1, par. 2, lett. a), b) e c), decisione (PESC) 2019/797.

[23] Da cui emergono forti legami con la Russia non solo dei sanzionati, ma dell'intero sistema con cui hanno sferrato gli attacchi.

[24] Segretariato generale del Consiglio, *Op. cit.*

© Wolters Kluwer Italia

arrecano "*effetti significativi*", ma basta siano "*tentati*" e con potenziale impatto analogo se diretti a Stati membri o all'Unione: infrastrutture critiche, servizi necessari alla società e l'economia nonché funzioni statali chiave per i primi; istituzioni, organi(smi), delegazioni e addirittura missioni di Politica di Sicurezza e Difesa Comune (PSDC) per la seconda (aprendo alla deterrenza cybernetica del fianco militare dell'Unione).

D'altra parte, il regime trova applicazione anche nel caso i bersagli siano Stati terzi e organizzazioni internazionali se necessario al perseguimento degli obiettivi propri PESC [25]. È qua argomentato che, in questo secondo scenario, un'interpretazione rigorosa del testo risulti in una seconda soglia per cui solo cyberattacchi effettivamente avvenuti rientrerebbero nell'ambito di applicazione. Ciò è supportato dal fatto che in questo caso, apparentemente, tali cyberattacchi non sarebbero "*minacce esterne*" per l'Unione o i suoi Stati membri, perlomeno non ai sensi della decisione (PESC) 2019/797.

Detto questo, il tentato attacco all'Organizzazione per la proibizione delle armi chimiche e relative sanzioni del 2020 è indicativo: sembra confutare ciò *in primis* [26], ma suggerisce come l'organizzazione internazionale vittima debba risiedere fisicamente nel territorio dell'Unione – in questo caso, i Paesi Bassi – *in secundis*. D'altronde, il fatto che in questo caso i sanzionati abbiano anche attentato sistemi informatici di uno Stato terzo (l'Ucraina) fa sospettare che quest'azione da sola superi una soglia i cui labili contorni sono definiti dalla prassi e dalla politica.

2.2. *Attacchi "significativi"*

Ogni cyberattacco in questione, per caratterizzarsi come minaccia esterna a norma dell'art. 3 della decisione (PESC) 2019/796, deve dimostrarsi "*significativo*" [27]. All'apparenza una semplice precisazione, l'attributo è fondamentale per meglio delimitare l'entità del cyberattacco a cui si può rispondere con il regime sanzionatorio.

Tornando brevemente alla *EU cybersecurity law*, da una parte la direttiva (UE) 2022/2555 richiama la terminologia nel caso di minacce "*significative*", che in questo caso arrecano "*grave impatto sui sistemi*

[25] Art. 1, par. 6, decisione (PESC) 2019/797.
[26] Allegato A, lett. I), decisione (PESC) 2019/797.
[27] Art. 3, par. 1, decisione (PESC) 2019/797.

© Wolters Kluwer Italia

informatici e di rete [...] causando perdite materiali o immateriali considerevoli" [28]. Logicamente, le gravi conseguenze sono il primo passo per delimitare – dal basso – tale concezione legale di cyberattacco significativo.

Dall'altra, la decisione (PESC) 2019/797 espande (ma si limita a) la lista dei fattori che concorrono gerarchicamente alla rilevanza dell'attacco, lasciando al Consiglio notevole discrezionalità su come interpretarli caso per caso. È comunque degno di nota che all'impatto "umano" sia data precedenza su quello "economico" e "del sistema". Tolte le turbative causate, infatti, il numero di persone interessate dall'attacco figura in cima davanti alla perdita economica originata, così come al numero di Stati membri coinvolti e i dati informatici sottratti o compromessi. Per la prassi, altre caratteristiche minime distintive e ricorrenti dei cyberattacchi significativi sono la ricaduta su più Stati membri o terzi; l'appartenenza a ampie campagne malevoli; la persistenza nel tempo. Talvolta, figura anche lo sfruttamento eventuale di *malware* o *software* autonomi una volta "impiantati" [29].

Più complessa è la delimitazione – dall'alto – di cosa rientri tra gli attacchi significativi per il regime sanzionatorio. Si proverà a costruirne (e ponderarne) una per esclusione accostando la *soft law* PESC alla clausola di mutua difesa dell'Unione, di cui all'art. 42, par. 7, TUE, per cui scattata questa si potrebbero escludere sanzioni ai sensi della decisione (PESC) 2019/797 in forza di un loro ambito *ratione materiae* vicino e confinante.

Come premessa, tale lettura si regge sull'assunto dottrinale e giurisprudenziale in base al quale attacchi cibernetici *per sé* possano costituire illecito internazionale, segnatamente "*attacco armato*" ai sensi dell'art 51 della Carta ONU [30]: a tal fine, dovrebbero dimostrare una

---

[28] Art. 6, par. 11, direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), in G.U.U.E. L333 del 27 dicembre 2022, pp. 80 ss.

[29] Allegato I, lett. A) e B), decisione (PESC) 2019/797.

[30] Art. 51 Carta ONU, in particolare "*[n]essuna disposizione [...] pregiudica il diritto naturale di autotutela individuale o collettiva, nel caso abbia luogo un attacco armato*". Cfr. M. SCHMITT, *Tallin manual on the international law applicable to cyber warfare*, Cambridge, 2013, pp. 54 ss.: "The right to employ force in self defence extends beyond kinetic armed attacks to those that are perpetrated entirely through cyber operations. [...] [S]ome cyber operations may be sufficiently grave to warrant classifying them as an «armed attack» within the meaning of the [UN] Charter"; v. anche C. int. giust., 8 luglio 1996, *Legality of the threat or the use of nuclear weapons*, parere

© Wolters Kluwer Italia

significatività elevata con ricadute enormi. Appurato ciò, spetterebbe agli Stati membri quali Stati sotto il diritto internazionale esercitare in primo luogo il diritto all'autotutela individuale o collettiva *ex* art. 51.

Di nostro interesse, inoltre, se lo Stato (membro) colpito optasse per una risposta europea condivisa, sarebbe il ricorso alle opzioni che il diritto Unione presenta: in campo PESC, infatti, l'attivazione dell'art. 42, par. 7, TUE parrebbe preferibile alle sanzioni, in quanto impone obblighi di "*aiuto e assistenza con tutti i mezzi*" in capo agli altri Stati membri [31].

Stando alle linee guida sulle sanzioni, invece, queste "could be used as a response to malicious cyber activities that do not rise to the level of internationally wrongful acts" circoscrivendole ad attacchi significativi che si "limitino" a "unfriendly acts" [32]. Incidentalmente, tale posizione "supera" la verifica della prassi sanzionatoria.

In conclusione, dunque, una tale interpretazione "per esclusione" limiterebbe dall'alto la nozione di attacchi cybernetici significativi di cui al regime sanzionatorio a quelli che arrivano al più a configurarsi come atti ostili, lasciando ad altre disposizioni la risposta agli attacchi qualificanti come illeciti internazionali, di scala maggiore.

Detto questo, criticità emergono in una divisione netta di "competenza" tra sanzioni e clausola: nulla esclude *a priori* che il ricorso al regime sanzionatorio possa seguire una risposta dell'Unione *ex* art. 42, par. 7, TUE. Per di più, la complessa attribuzione di cyberattacchi ad attori parastatali e, dunque, a Stati complica l'attivazione della clausola, solo uno dei dispositivi rilevanti per il diritto dell'Unione (si veda l'art. 222 TFUE) [33] o internazionale (l'art. 5 del Trattato NATO). Inoltre, l'attivazione dell'art. 42, par. 7, TUE è subordinata alla volontà politica dello Stato vittima e non è automatica, aspetto che si aggiunge ai fattori che rendono incerto il suo ricorso in caso di cyberattacco estremamente significativo.

L'elemento apprezzabile che emerge per questa trattazione è il seguente: atti recanti sanzioni e clausola di mutua difesa godono di una sovrapposizione giuridica da investigare a fondo nel caso fosse affidata al diritto europeo la risposta a cyberattacchi di forte significatività.

---

consultivo, par. 39; C. int. giust., 27 giugno 1986, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, par. 195.

[31] Art. 42, par. 7, TUE.

[32] Segretariato generale del Consiglio, *Op. cit.*

[33] La clausola di solidarietà di cui all'art. 222 TFUE è sovente accostata all'art. 42, par. 7, TUE per ambito e natura. Più estesa della sua controparte, coinvolge di più le istituzioni dell'Unione, sovrapponendosi per numerosi casi ad una applicazione della clausola di mutua difesa.

© Wolters Kluwer Italia

3. Considerazioni conclusive

Complessivamente, l'Unione europea è particolarmente attiva nella regolamentazione del cyberspazio. Sebbene non aderisca al principale trattato internazionale sulla cybersicurezza, la Convenzione sulla criminalità informatica conclusa il 23 novembre 2001 a Budapest, essa ha partecipato ai negoziati del relativo Protocollo addizionale sulla cooperazione rafforzata e la divulgazione di prove elettroniche del 14 febbraio 2023 [34].

Con la guerra in Ucraina si è rinvigorita la tendenza ad "esternalizzare" la *EU cybersecurity law* visto l'impatto, la frequenza e la sofisticazione di attacchi informatici di nuova generazione provenienti da Stati terzi [35], ponendo le basi per una svolta che impone al legislatore il superamento dei paradigmi di difesa convenzionale dei *network* e di *resilience-building*. [36] La minaccia che i cyberattacchi pongono agli Stati membri va oltre l'aggressione ed è destinata a persistere, data la molteplicità di soggetti allineati ai governi da una parte, criminali e "hacktivisti" autonomi dall'altra.

Le sanzioni orizzontali a tema cyber si calano dunque in tale volatile scenario e rappresentano lo strumento unionale più aggressivo e flessibile per rispondere alle maggiori minacce informatiche: i cyberattacchi significativi. Il presente contributo si è concentrato sulla nozione giuridica di questi quali "*minaccia esterna*" per il regime sanzionatorio cibernetico, privilegiando dunque l'ambito di applicazione *ratione materiae*. Ciò ha permesso di scorgerne particolarità e unicità per l'azione esterna dell'Unione: è ragionevole pensare che un'analisi ancor più ap-

---

[34] Convenzione sulla criminalità informatica (STE no. 185), Budapest, 23 novembre 2001. Si fa riferimento al Secondo Protocollo addizionale ivi contenuto, implementato dalla decisione (UE) 2023/436 del Consiglio, del 14 febbraio 2023, che autorizza gli Stati membri a ratificare, nell'interesse dell'Unione europea, il Secondo Protocollo addizionale alla Convenzione sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche, in G.U.U.E. L63 del 28 febbraio 2023, pp. 48 ss.

[35] Agenzia dell'Unione europea per la cibersicurezza, *ENISA Threat Landscape (2023)*, disponibile su: *www.enisa.europa.eu*: "The Russia-Ukraine crisis has defined a new era for cyberwarfare and hacktivism (...)".

[36] Si pensi alla grande quantità di strumenti normativi (e non) dell'Unione che rafforzano – passivamente – resilienza alle *cyber threats* rafforzando capacità industriali e tecnologiche fin dagli stadi di progettazione di dispositivi, in un approccio che punta a mitigare i rischi *a fortiori*. V. la comunicazione congiunta della Commissione e dell'Alto Rappresentante per gli Affari Esteri e la Politica di Sicurezza al Parlamento europeo e al Consiglio, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, Bruxelles, 16 dicembre 2020, JOIN(2020)18 final.

© Wolters Kluwer Italia

profondita beneficerebbe la *EU cybersecurity law* nella sua complessità, area legale trasversale destinata inevitabilmente a crescere e a "esternalizzarsi" ulteriormente.

Una menzione la merita l'ambito *ratione personae* della decisione (PESC) 2019/797 che, qui sacrificato per motivi di spazio e di *focus* del contributo, include sia i responsabili dei cyberattacchi che chi ne facilita la (tentata) attuazione così come chi la agevola "*per azione o omissione*" [37]. In aggiunta, dispositivi quali la c.d. *clausola antielusione* rafforzano le sanzioni in incisività ed efficacia, il cui principio è da bilanciare con quello di proporzionalità [38].

In conclusione, il recente ricorso alle sanzioni si cala nella rinnovata volontà del Consiglio di superare gli ostacoli che impediscono un "*cyberspazio globale e aperto*" [39]. Purtroppo, o per fortuna, tale strumento è subordinato più di altri al volere politico, che contribuisce con la prassi al segnare i confini delle nozioni qui contenute.

[37] Artt. 4, par. 1, lett. b), e 5, par. 1, lett. c), decisione (PESC) 2019/797.

[38] Art. 9 regolamento (UE) 2019/796. Per una trattazione su tale disposizione comune ad altri regimi di sanzioni: F. Finelli, *Principio di effettività e misure restrittive UE: la lotta all'elusione nel contesto della guerra in Ucraina*, in *Quad. AISDUE*, 4/2023, pp. 726 ss.

[39] Comunicazione congiunta della Commissione e dell'Alto Rappresentante per gli Affari Esteri e la Politica di Sicurezza al Parlamento europeo e al Consiglio, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, cit., pp. 5 ss.

© Wolters Kluwer Italia

ARTE E TECNOLOGIA: TRACCIABILITÀ E INTELLIGENZA ARTIFICIALE *

VALERIO MAGGIO

SOMMARIO: 1. Varie possibili applicazioni dell'intelligenza artificiale al mercato dell'arte. – 2. Intelligenza artificiale e tracciabilità ai fini del diritto dei beni culturali. – 3. Intelligenza artificiale e tracciabilità fiscale delle operazioni su opere d'arte. – 4. La *blockchain* come strumento di tracciabilità. – 5. Conclusioni sulla gestione combinata degli strumenti di tracciabilità fiscale.

Abstract: The traceability of artworks is crucial to ensure compliance with tax obligations, which were clarified by the Italian Supreme Court, in March 2023 with a ruling that classified three parties involved in the sale of artworks, distinguishing between art dealers, occasional speculators, and collectors, with their specific tax implications. This traceability is facilitated in the case of artworks of cultural interest, through the Ministry of Culture, which monitors the transfer of ownership. Despite the absence of direct communication to the tax authority following the declaration of cultural interest, the public records make available for consultation, including in the case of tax inspections, the decrees on artworks circulation restrictions. Artificial intelligence is emerging as a powerful tool to enhance tax assessments, enhancing the use of digital technologies and big data to identify tax risks. However, the effectiveness of artificial intelligence depends on the completeness and timeliness of the data. Private registries which use blockchain technology to ensure the traceability of artworks could complement administrative artificial intelligence and improve transparency and tax compliance.

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

1. Varie possibili applicazioni dell'intelligenza artificiale al mercato dell'arte

La tracciabilità è intesa tradizionalmente come il principio che consente di monitorare beni o attività ai fini di diverse forme di controllo sociale, sia delle controparti sia di autorità amministrative.

Nel contesto della compravendita di opere d'arte c'è prima di tutto una tracciabilità destinata a garantire le controparti sull'autenticità dell'opera, come presidio contro ipotetiche contraffazioni.

C'è poi la tracciabilità amministrativa, tendente a salvaguardare eventuali vincoli culturali dovuti all'interesse storico artistico di determinate opere.

In ambito artistico, le opere dichiarate d'interesse culturale ai sensi del d. lgs. 22 gennaio 2004, n. 42 (ovverosia, il Codice dei beni culturali e del paesaggio, *breviter* "Codice") godono sicuramente di notevole visibilità, venendo di fatto censite, dal Ministero della Cultura (*breviter*, "MiC") tramite i suoi organi competenti; tuttavia, sembra che tale censimento delle opere ad oggi rimanga un meccanismo solo ed unicamente utilizzato ai fini amministrativi di tutela.

Visto che anche la vendita delle opere d'arte determina per le parti coinvolte presupposti economici d'imposta (ricavi, costi, consumi, ecc.), ad essa si collega anche una tracciabilità fiscale, diretta a prevenire l'evasione, nonché il riciclaggio di denaro [1] o l'autoriciclaggio; questi ultimi fenomeni possono avvenire con una certa frequenza in questo settore, viste la soggettività delle relative valutazioni e la loro oscillazione nel tempo.

Per tutte queste forme di tracciabilità possono essere utili strumenti tecnologici come l'intelligenza artificiale (*breviter*, "IA").

2. Intelligenza artificiale e tracciabilità ai fini del diritto dei beni culturali

La dichiarazione d'interesse culturale viene apposta su tutti quei beni, mobili o immobili, che abbiano un valore artistico, storico, archeologico o etnoantropologico eccezionale per l'integrità e la completezza del patrimonio culturale italiano [2], o che siano particolarmente

[1] Art. 648-*bis* e *ter* c.p.

[2] Art. 10, lett. d-*bis*), d. lgs. 22 gennaio 2004, n. 42.

© Wolters Kluwer Italia

importanti a causa del loro riferimento con la cultura in tutte le sue declinazioni [3].

Laddove questo interesse venga rinvenuto dal MiC, o uno dei suoi organi, la Soprintendenza competente per territorio avvia il procedimento di dichiarazione d'interesse culturale [4] (più comunemente chiamato "vincolo" o "notifica"), andando a "censire" queste opere da quel momento catalogate nei registri del MiC, tenendo traccia dei successivi passaggi di proprietà.

Il proprietario del bene vincolato è obbligato, tra i vari obblighi, alla tutela di detto bene, ed il MiC, tramite i suoi organi, è chiamato ad esercitare una forma di monitoraggio che include quello sulla titolarità dei beni.

Nello specifico, il proprietario è obbligato a denunciare al MiC tutti quegli atti che trasferiscono, anche in parte, la proprietà o detenzione dei beni, qualunque sia la ragione [5].

S'intende, dunque, che il MiC sia sempre informato, salvo casi di violazione della norma, sulla titolarità dei beni vincolati durante i suoi trasferimenti.

Ovviamente l'applicabilità del regime descritto rimane limitata, escludendo casistiche che comprendono compravendite di, a titolo esemplificativo, opere d'arte contemporanea e *non-fungible tokens* (*breviter*, "NFT"), vale a dire immagini registrate e vendute sulla *blockchain* aventi (a detta di alcuni) valore artistico.

Dunque, eccezion fatta per arte contemporanea ed NFT, come può la tecnologia intervenire per migliorare la tracciabilità amministrativa?

L'impiego di un'IA associata ad un registro di opere su *blockchain* potrebbe essere uno strumento di ausilio che a processa automaticamente le disposizioni dei beni e garantisce, oltre che la genuinità dell'opera nel rapporto di compravendita, anche la tracciabilità delle opere e dei flussi finanziari nel commercio d'arte tramite i dati digitali cui ha accesso, quando le funzionalità del *software* sono interconnesse a registri digitali come potenzialmente quelli del MiC, ricomprendendo opere sia censite in via amministrativa (attingendo ai registri della pubblica amministrazione) che in via privatistica (come nel caso di registri di privati a cui l'IA ha accesso dove le opere vengono registrate dagli autori o dai mercanti), incluso su *blockchain*.

Questo possibile scenario sarebbe anche supportato dal fatto che, a

[3] Art. 10, lett. d), d. lgs. n. 42/2004.
[4] Art. 14 d. lgs. n. 42/2004.
[5] Art. 59, comma 1, d. lgs. n. 42/2004.

© Wolters Kluwer Italia

dispetto di quanto accade in molti altri uffici della macchina pubblica, la Soprintendenza sembra agire con disturbante prontezza quando i beni culturali sono coinvolti, avendo dunque nella propria disponibilità registri presumibilmente adeguati.

Per comprendere il livello di operatività degli uffici competenti, solo la Soprintendenza del MiC per il Lazio, tra il 2018 ed il 2019, ha emanato 37 decreti di interesse culturale, di cui 11 relativi ad opere d'arte mobili [6].

È inoltre importante evidenziare come ogni decreto può contenere più beni, come ad esempio il decreto della Soprintendenza n. 50 del 22 marzo 2019, che contiene 58 opere appartenenti alla "Collezione Esso".

Mettendo da parte la tracciabilità amministrativa per considerare quella fiscale in questo settore, ai fini tributari è bene chiarire che vincoli o alienazioni di beni vincolati sembrano non innescare un'immediata comunicazione all'Agenzia delle Entrate, tuttavia, il Codice ci dice che a seguito di denuncia di un atto dispositivo del bene, il Soprintendente ne dà comunicazione "*agli altri enti pubblici territoriali*", mentre la Regione ne dà notizia sul proprio bollettino ufficiale indicando il prezzo di vendita [7].

Nell'improbabilità che per "*altri enti pubblici territoriali nel cui ambito si trova il bene*" s'intenda anche l'Agenzia delle Entrate, i decreti di vincolo e le alienazioni dei beni in esame sono in ogni caso pubblici e accessibili dai cittadini, e quindi, ovviamente, anche dai diversi organi statali (qualora ci fosse la volontà).

Un eventuale sospetto potrebbe quindi portare l'ufficio tributario ad effettuare un accertamento con relativa indagine dei registri del MiC dove sono riportati i beni censiti, o del bollettino ufficiale ove è riportata l'ipotetica cessione.

Se si prende il caso del mercante d'arte proprietario di beni vincolati che vende opere, con annessa denuncia al MiC, per poi non rendicontare l'incasso ai fini fiscali, il reddito generato dall'attività potrebbe essere desunto anche dalle due fonti suddette.

Visto il valore medio di tali opere (anche di diversi milioni di euro) ed i potenziali introiti, anche un'analisi basata su criteri induttivi relativi alle eventuali variazioni di spesa del contribuente (successive alla compravendita) ed una determinazione presuntiva dell'insieme del reddito, sebbene disattendendo le scritture contabi-

[6] Disponibile su: *https://lazio.cultura.gov.it*.
[7] Art. 62 d. lgs. n. 42/2004.

© Wolters Kluwer Italia

li [8], potrebbe concludersi con l'identificazione di transazioni i cui profitti sono ricollegabili ai redditi apparentemente non dichiarati.

Il meccanismo del vincolo e l'utilizzo dei registri del MiC, tuttavia, rimane legato a dinamiche sintetiche (*id est*, spesa) susseguenti alla vendita di opere e ad arte vincolata; quindi, quando si parla di arte contemporanea dal basso valore (spesso sotto il limite di €5.000 per pagamenti in contanti) che non gode della tutela prevista dal Codice, eventuali compravendite non verrebbero denunciate né registrate, parallelamente ad insignificanti variazioni di spesa.

Fa sempre eccezione, tuttavia, il caso dell'acquirente che per garantirsi una rivendita vantaggiosa chiede fattura a suo nome, fermo restando che nulla impedisce alle parti di concordare che una parte del prezzo d'acquisto venga riportata in fattura e bonificata e l'altra invece pagata in contanti, dinamiche che non troverebbe terreno fertile nel caso di impiego di tecnologie come l'IA nelle forme sotto riportate.

3. Intelligenza artificiale e tracciabilità fiscale delle operazioni su opere d'arte

Sulla qualificazione dei presupposti economici d'imposta connessi alla cessione di opere d'arte si sta profilando, anche nella giurisprudenza della Corte di Cassazione [9], un'articolata serie di sfumature tra mercanti d'arte, speculatori che effettuano atti d'impresa occasionali, rilevanti come redditi diversi, e collezionisti, i cui atti non rilevano affatto né ai fini dell'IVA né delle imposte sui redditi.

Lo scopo culturale e collezionistico di quest'ultima figura, scevro da qualunque interesse per il valore economico della *res* né tantomeno dalla volontà di rivenderla per generare una plusvalenza, può essere però lo sfondo in cui si collocano isolati atti d'impresa occasionali imponibili come redditi diversi, come quelli menzionati nella sopracitata ordinanza.

Il mercante d'arte è invece un ordinario imprenditore [10] anche soggetto IVA [11].

Il *curiosum* di quest'assetto è il possibile innestarsi di "redditi di-

---

[8] R. Lupi, *L'imposizione tributaria come diritto amministrativo speciale*, Milano, 2023, pp. 295 ss.

[9] Cass. civ., sez. V, 8 marzo 2023, n. 6874.

[10] Art. 55 ss. d.P.R. 22 dicembre 1986, n. 917.

[11] Art. 4 d.P.R. 26 ottobre 1972, n. 633.

© Wolters Kluwer Italia

versi", per alcune opere, sullo sfondo di un collezionista che normalmente non li realizza.

L'impresa occasionale finisce così per supplire alla soppressione del c.d. intento speculativo, normativamente venuto meno dal Testo unico del 1986.

Si ripercorrono insomma, per le opere d'arte, le stesse argomentazioni effettuate decenni or sono per le plusvalenze di borsa; mentre quest'ultima supplenza era molto debole [12], trova un argomento in più nell'attività di valorizzazione effettuata dal collezionista sulla specifica opera.

Ad arricchire ulteriormente questa complessa panoramica di fattispecie, la possibilità di riportare l'alienazione di un'opera anche ai redditi di lavoro autonomo, ove venga effettuata direttamente dall'artista.

Su questo sfondo di diritto sostanziale tributario ci si interroga quindi fino a che punto le suddette modalità di tracciabilità amministrativa possono essere impiegate con successo anche ai fini fiscali per mezzo della tecnologia.

Un aiuto proviene dalla legislazione in ambito di tracciabilità finanziaria (antiriciclaggio) che ha finora imposto che determinati pagamenti o transazioni venissero effettuati attraverso bonifici bancari, carte di credito o debito, assegni, o altri mezzi tracciabili [13]; questo non garantisce certo che il soggetto d'imposta, alienante del bene artistico, assolva ai suoi obblighi dichiarativi, ma lo rende visibile a posteriori in caso di controlli.

Col passaggio ad opere d'arte di minore rilevanza, e la possibilità di pagamenti per contanti o la minore visibilità degli strumenti tracciabili, abbiamo un piccolo cabotaggio di piccoli commercianti e speculatori persone fisiche [14] cui è più difficile star dietro.

In questa misura è proporzionalmente più facile utilizzare il tenore di vita, facendo leva sui consumi e investimenti privati, nel senso di personali, facendo valere la discrepanza rispetto ai redditi dichiarati.

Diverse disposizioni invocano l'interoperabilità tra le banche dati, disponibilità delle informazioni rilevanti [15], il monitoraggio del com-

---

[12] Come sottolinea giustamente R. BAGGIO, *Ancora in tema di attività commerciali occasionali e di intento speculativo*, in *Riv. dir. trib.*, 1/1992, pp. 233-246.

[13] Art. 1, comma 679, l. 27 dicembre 2019, n. 160.

[14] R. LUPI, *Diritto amministrativo dei tributi*, II ed., Roma, 2017, p. 230.

[15] La legge delega al Governo per la riforma fiscale del 9 agosto 2023, n. 111, all'art 17 prevede: "*(...) per la revisione dell'attività di accertamento, anche con riferimento ai tributi degli enti territoriali: [...] potenziare l'utilizzo di tecnologie digitali, anche con l'impiego di sistemi di intelligenza artificiale, al fine di ottenere, attraverso*

© Wolters Kluwer Italia

portamento dei contribuenti e la loro propensione all'adempimento [16], controlli preventivi, *machine learning* [17] e analisi probabilistiche tramite IA [18].

Da un punto di vista pratico, le modalità di accertamento potrebbero fondarsi sull'impiego di algoritmi che, dato un certo comportamento del contribuente e analizzando i dati cui l'IA ha accesso, elaborano il rischio fiscale.

Questo viene indagato in base alla platea ed il fenomeno fiscale in esame, che può portare la ricerca verso banche dati esterne cui l'Agenzia delle Entrate ha accesso [19].

Risulta evidente come una delle problematiche principali rimane l'affidabilità e la completezza delle informazioni a disposizione, ed un'IA che agisce intrecciando le varie banche dati non avrebbe la possibilità di fornire un risultato affidabile sul rischio fiscale di un contribuente qualora le sue elaborazioni fossero basate su dati obsoleti e/o parziali.

Come sempre, solo il pronto ricevimento e utilizzo di dati precisi, esaustivi e accurati (da qui la necessità dell'interoperabilità automatizzata dell'IA) consentirebbe all'amministrazione intervenire in maniera tempestiva in casi di condotte evasive [20].

Quindi, nel caso dell'arte, immaginando l'introduzione dell'IA nelle procedure di controllo e accertamento, e prendendo in esame i so-

---

la piena interoperabilità tra le banche di dati, la disponibilità delle informazioni rilevanti (...)".

[16] La Convenzione Triennale per gli Esercizi 2023-2024 (d. lgs. 30 luglio 1999, n. 300, art. 59, commi 2, 3 e 4) prevede all'art. 5 che "*l'Agenzia monitorerà, inoltre, il comportamento dei contribuenti che hanno subito un controllo fiscale per verificare nel tempo il loro grado di propensione all'adempimento e, più in generale, per valutare il livello di fedeltà fiscale; sarà incrementata la capacità operativa nell'ottica di favorire il miglioramento della qualità dei controlli, attraverso nuovi strumenti e progetti di analisi avanzata dei dati, l'applicazione di tecniche come l'intelligenza artificiale, il machine learning e il text mining*".

[17] Direttiva della Direzione dell'Agenzia delle Entrate (prot. n. 2023/74424), "*Modifiche all'organizzazione e alle attribuzioni della Divisione Contribuenti e della Direzione Centrale Piccole e Medie Imprese*".

[18] Secondo il d. lgs. 12 febbraio 2024, n. 13, art. 2, lett. f), per "analisi probabilistica" s'intende un "*insieme dei modelli e delle tecniche di analisi che, sfruttando soluzioni di intelligenza artificiale ovvero di statistica inferenziale, consentono di isolare rischi fiscali, anche non noti a priori, che, una volta individuati, possono essere utilizzati per l'elaborazione di autonomi criteri selettivi, ovvero permettono di attribuire una determinata probabilità di accadimento a un rischio fiscale noto*".

[19] Agenzia delle Entrate, "*Informativa sulla logica sottostante i modelli di analisi del rischio basati sui dati dell'archivio dei rapporti finanziari*".

[20] A. Mastromatteo - B. Santacroce, *Guida ai controlli fiscali. Contrasto all'evasione fiscale, valorizzate nuove fonti di dati*, Roma, 2019, pp. 20-22.

© Wolters Kluwer Italia

pracitati decreti di vincolo del biennio 2018-2019 (para. 2) (gli unici disponibili sul sito del Segretariato del MiC per la Regione Lazio), un eventuale mercante che trae profitto dalla vendita di una collezione vincolata con decreto *post*-2019, seppure con l'impiego dell'IA con accesso alle banche dati del MiC, avrebbe meno possibilità di vedere il suo comportamento evasivo rilevato se i decreti *post*-2019 non sono stati archiviati correttamente e digitalmente in banche accessibili e leggibili dal sistema di IA implementato.

Un'ulteriore "doccia fredda" arriva a seguito del regolamento (UE) 2024/1689 sull'intelligenza artificiale, denominato "*AI Act*", pubblicizzato con orgoglio come il primo del suo genere, che prevede la classificazione dell'attività dell'IA in esame in quattro possibili fasce di rischio dove, in quella indicata come "rischio alto", viene menzionata la profilazione di persone fisiche [21] nell'amministrazione della giustizia e nei processi democratici (ad esempio, l'applicazione della legge a una serie concreta di fatti) [22], nel quale rientrerebbe per analogia la tracciabilità fiscale.

Questi sistemi di IA ad alto rischio sono soggetti ad obblighi rigorosi mediante adeguati sistemi di valutazione e attenuazione dei rischi, elevata qualità dei dati di sistema, documentazione dettagliata che fornisca tutte le informazioni necessarie, appropriate misure di sorveglianza umana, ecc.

In un contesto come quello italiano, caratterizzato dall'inefficienza di molti pubblici uffici, quanto descritto sopra lascia aperti due possibili scenari dove nel primo l'IA non viene mai adoperata per adempiere a funzioni amministrative, mentre nel secondo lo Stato italiano viene sanzionato dall'Unione europea per le violazioni della normativa eurounitaria.

Cionondimeno, mettendo da parte il rischio di *non-compliance* da parte dello Stato, è innegabile che, qualora l'interoperatività dell'IA arrivasse alla consultazione automatica di registri digitali sia pubblici che privati (in formato leggibile), la tracciabilità potrebbe beneficiarne.

Come già accennato, però, ai fini di un'efficiente tracciabilità è necessario che i dati sulla base dei quali l'IA opera siano precisi, esaustivi ed accurati.

A tal proposito, nel settore dell'arte, specialmente durante la pandemia, hanno proliferato proposte tecnologiche volte a catalogare beni

[21] Art. 6 reg. (UE) 2024/1689.
[22] All. III reg. (UE) 2024/1689.

© Wolters Kluwer Italia

artistici, specialmente quelli non vincolati, su piattaforme private accessibili al pubblico via *Internet*, sfruttando la tecnologia *blockchain*.

Questa si è rivelata essere uno strumento utile che, data la sua natura, rende immutabili le informazioni ivi contenute, garantendo affidabilità a chi consulta il registro.

4. La *blockchain* come strumento di tracciabilità

La tecnologia *blockchain* può essere intesa come un *network* di *computers* che seguono regole matematiche per creare un "libro mastro" (*ledger*) digitale, decentralizzato e distribuito su questo stesso *network* ove vengono registrati dati che sono irremovibili ed immodificabili grazie a crittografie e protocolli di consenso [23].

Un esempio dell'applicabilità di questa tecnologia alle transazioni con opere d'arte è Artory [24], un registro digitale utilizzato per registrare opere e transazioni che diventano susseguentemente immodificabili.

Artory si appoggia a periti indipendenti per la verifica dei dati e la provenienza dell'opera d'arte.

La registrazione in piattaforma permette la visibilità ad altri *partners* della società titolare che verificano l'affidabilità dei dati inseriti.

La *blockchain* ha la possibilità di operare sulla ricezione di *inputs* provenienti da sistemi informatici esterni chiamati "oracoli" e che comunicano alla *blockchain* le informazioni in base alle quali questa farà o non farà una data azione programmata.

Gli oracoli possono a loro volta funzionare per mezzo di *softwares* di IA rendendo le due soluzioni tecnologiche complementari per una loro ipotetica applicazione nella tracciabilità di opere d'arte, dove la titolarità di un'opera viene registrata sulla *blockchain* insieme ai passaggi di proprietà successivi [25] andando a creare un registro dove l'IA amministrativa può accedere automaticamente ai fini del rilevamento di flussi finanziari e titolarità di opere garantendo una più adeguata e puntuale determinazione della ricchezza dei contribuenti ai fini

---

[23] G. Chiap - J. Ranalli - R. Bianchi, *Blockchain: Tecnologia e applicazioni per il business*, Milano, 2021, pp. 15-16.

[24] Disponibile su: *https://www.artory.com.*

[25] La registrazione e aggiornamento della titolarità fa sì che ci sia certezza circa l'autenticità delle opere ed il loro valore, oltre ad essere utile in caso di furti. L'affidabilità, come accennato, dipende dal lavoro degli operatori della piattaforma ed il protocollo di consenso programmato nella *blockchain* (es., *proof of work*, *proof of stake*, ecc.).

© Wolters Kluwer Italia

dell'applicazione delle relative imposte, attività che da sempre viene svolta dall'autorità amministrativa [26], sebbene con le dovute difficoltà date da dinamiche che l'amministrazione al momento non ha la possibilità di contrastare [27].

5. Conclusioni sulla gestione combinata degli strumenti di tracciabilità fiscale

Dai paragrafi che precedono si può ricavare qualche indicazione conclusiva sulla pluralità di strumenti di tracciabilità amministrativa e finanziaria utilizzabili per contrastare la mancata dichiarazione di proventi connessi alla compravendita di opere d'arte.

Da una parte c'è l'eventuale organizzazione aziendale del mercante d'arte, con la sua documentazione contabile su base ragionieristica [28].

Tuttavia, anche qui, nel caso di clienti persone fisiche, può crearsi una convergenza d'interessi col mercante d'arte per un occultamento totale o parziale del corrispettivo.

L'unica controindicazione è l'eventuale desiderio dell'acquirente a possedere una documentazione di supporto del prezzo pagato, per valorizzare il bene, anche in sede di successive eventuali rivendite.

Uno strumento parallelo di visibilità fiscale diventano quindi le valutazioni sul tenore di vita del cedente, come indizio dell'attività che svolge, combinando strumenti di accertamento "valutativo-presuntivi" (basati su compensi e costi) e "sintetico-presuntivi" (basati sul tenore di vita e investimenti privati) [29] estranei all'esercizio dell'attività [30].

Gli strumenti presuntivi, sia relativi all'attività che al tenore di vita, si addicono di più ai casi in cui si effettuano molte vendite di importo relativamente piccolo, difficili da gestire non solo quando regolate in contanti, ma anche quando regolate con strumenti di pagamento tracciabili.

L'individuazione analitica delle singole operazioni è infatti diffici-

---

[26] R. LUPI, *Compendio di scienza delle finanze*, Roma, 2017, pp. 162 ss.

[27] Si pensi al sopracitato caso di pagamenti parte contante e parte bonifico, se non addirittura totalmente in contanti, nei casi di acquirenti meno esperti.

[28] R. LUPI, *Compendio di scienza delle finanze*, cit., pp. 162 ss.

[29] Si parla qui di accertamento "sintetico-reddittometrico" basato sul rapporto reddito-tenore di vita (R. LUPI, *Diritto amministrativo dei tributi*, cit., p. 252).

[30] *Id.,* pp. 244 ss.

© Wolters Kluwer Italia

le, soprattutto in un contesto in cui l'intervento degli uffici tributari è finalizzato più a indurre all'adempimento i contribuenti che ad acquisire direttamente gettito [31].

Su queste premesse solo cessioni di opere di grande valore, che spesso fanno notizia in sé, innescano indagini puntuali, con determinazioni ragionieristiche, anche per i vincoli amministrativi sulla circolazione di opere d'arte.

Su questo sfondo l'utilizzo di entità e strumenti tecnologici, incluso quelli privati in *outsourcing*, potrebbe facilitare il monitoraggio del settore artistico ai fini tributari; si contribuirebbe così a far percepire ai relativi operatori un certo controllo tributario del territorio, spingendoli quindi all'adempimento.

[31] R. Lupi, *Manuale di evasione fiscale*, I ed., Roma, 2020, *passim*.

© Wolters Kluwer Italia

L'ECONOMIA DIGITALE E LE NUOVE REGOLE SULLA TASSAZIONE MINIMA *

MARINA RIGHI

SOMMARIO: 1. Premessa: il rapporto tra tassazione ed economia. – 2. L'implementazione delle imposte minime globali nell'UE. – 3. L'introduzione dell'imposta minima in Italia. – 4. Conclusioni.

Abstract: The significant technological advancements of recent decades have brought about new economic realities that present a substantial challenge to current tax systems, which have been shaped by traditional economies predicated on the physical location of taxpayers and the origin of income. This is particularly pertinent as large multinational corporations engaged in such types of economic activity, which are not reliant on physical presence, have begun to adopt international structures designed to exploit existing gaps and tax mismatches among many jurisdictions to minimise their overall tax burden. This behaviour has given rise to the phenomenon of base erosion and profit shifting, which the Organisation for Economic Cooperation and Development ("OECD") seeks to combat through the Base Erosion and Profit Shifting ("BEPS") Project. As will be discussed throughout this work, it is within this context that the new European Union ("EU") rules on effective minimum taxation, which come into effect on 1 January 2024, formalise the EU's implementation of the so-called second pillar rules of the BEPS Project. In this sense, the present contribution aims to analyse the impact of these rules on the taxation of new digital economy models that, until that point, were facts that did not have their consequences regulated in the field of European tax law. Finally, within this context, the current Italian legislation on the subject will also be analysed.

* Contributo sottoposto a doppio referaggio in forma anonima.

© Wolters Kluwer Italia

1. Premessa: il rapporto tra tassazione ed economia

Significativi progressi tecnologici hanno generato nuove realtà economiche, precedentemente estranee alla considerazione giuridica. Questo fenomeno ha portato a una società e un'economia sempre più globalizzate, con nuovi modelli di *business*. Tra le peculiarità di questi modelli, si evidenzia la crescente irrilevanza della presenza fisica nel luogo in cui si svolge l'attività economica, con un processo produttivo che è diventato sempre più integrato e intangibile [1].

Naturalmente, l'ascesa di questa nuova tipologia di economia, comunemente definita *economia digitale*, ha presentato una sfida significativa per gli attuali sistemi fiscali, che sono stati concepiti in base ai principi dell'economia tradizionale, focalizzandosi sul luogo fisico dei contribuenti e sull'origine del reddito. Infatti, la sovranità di ciascuno Stato è storicamente stata riconosciuta con un'ottica territoriale, consentendo a ciascuno di regolare le attività svolte all'interno del proprio territorio senza subire condizionamenti da parte di altri Stati [2].

A questo punto, in un primo momento, nel periodo tra le due grandi guerre, la principale preoccupazione degli Stati era quella di evitare che la tassazione fungesse da ostacolo agli investimenti internazionali. Ciò ha dato origine a una serie di convenzioni internazionali finalizzate a stabilire regole atte a distribuire il carico fiscale tra gli Stati coinvolti in operazioni transnazionali, prevenendo situazioni di doppia imposizione. A tal proposito, il modello di convenzione di maggior rilevanza è stato definito dall'Organizzazione per la Cooperazione e lo Sviluppo Economici ("OCSE") nel 1963.

Il punto è che negli ultimi anni, con l'avanzare sempre più rapido della tecnologia, si è manifestato un nuovo fenomeno, diametralmente opposto, che ha sollevato gravi preoccupazioni tra gli Stati: l'erosione delle basi imponibili e il trasferimento dei profitti. Le grandi multinazionali, infatti, sono attualmente tenute a versare l'imposta sul reddito delle società esclusivamente negli Stati di origine in cui possiedono una presenza fisica.

In questo senso, i giganti tecnologici come Google, Facebook e Amazon, che sono in grado di generare entrate da Stati di mercato interamente *online*, senza stabilire una presenza fisica (c.d. economia di-

---

[1] A. MARINELLO, *La rarefazione della sovranità tributaria dello Stato nell'era dell'economia digitale e il progetto della "Global Minimum Tax"*, in *Rivista di studi giuridici*, 27/2023, p. 132.

[2] C. GARBARINO, *Diritto Convenzionale Tributario*, Milano, 2019, p. 1.

© Wolters Kluwer Italia

gitale), hanno strutturato le proprie operazioni internazionali per sfruttare le lacune e i disallineamenti fiscali esistenti tra i diversi ordinamenti giuridici, al fine di ridurre o addirittura annullare il proprio onere fiscale complessivo. È proprio la natura intangibile di beni moderni, quali marchi, *software* e altre forme di proprietà intellettuale, a permettere a queste multinazionali di trasferire i profitti da Stati con tassazione elevata, dove hanno la loro sede centrale [3].

Proprio per contenere questo fenomeno, l'OCSE ha creato il Progetto BEPS nel 2013. Comunque, pochi anni dopo l'emanazione dei Rapporti finali BEPS, l'accelerazione digitale ha portato con sé la necessità, sempre più allarmante, di mettere nuovamente in discussione alcuni dei fondamenti della tassazione internazionale delle imprese, il che è stato chiamato di BEPS 2.0. A questo punto, in risposta a queste nuove prospettive, l'OCSE ha proposto agli Stati membri di implementare due pilastri (denominati "1" e "2").

Il Primo Pilastro prevede una modifica delle attuali regole di allocazione dei profitti e di *nexus*, assegnando una parte dei profitti residui di una multinazionale alle giurisdizioni di mercato, a prescindere dalla sua presenza fisica in tali Stati. Il Secondo Pilastro, invece, ha come obiettivo la riduzione del trasferimento dei profitti e dell'erosione della base imponibile, introducendo una tassazione minima globale del 15%.

Se può dire che il Secondo Pilatro rappresenta il primo tentativo multilaterale di coordinare le aliquote dell'imposta sul reddito delle società, realizzato attraverso regole di *switch-over* [4]. In questo senso, se una giurisdizione che ha aderito all'accordo non applica l'aliquota minima di imposta effettiva, un'altra giurisdizione interverrà e riscuoterà le entrate.

È proprio in questo contesto che la nuova direttiva UE, oggetto di analisi nel prossimo paragrafo e in vigore dal gennaio 2024, si inserisce.

2. L'implementazione delle imposte minime globali nell'UE

In attuazione del c.d. Secondo Pilastro raggiunto in sede OCSE, nel dicembre 2022, il Consiglio dell'Unione europea, attraverso la di-

[3] R. Avi-Yonah - Y.R. Kim - K. Sam, *A New Framework for Digital Taxation*, in *Harvard International Law Journal*, 2/2022, pp. 279-341.

[4] A.P. Dourado, *Pillar Two from the Perspective of the European Union*, in *British Tax Review*, 5/2022, pp. 573-600.

© Wolters Kluwer Italia

rettiva (UE) 2022/2523 del 14 dicembre 2022, ha implementato delle imposte minime globali e gli Stati membri sono stati obbligati a adottare le norme entro il 31 dicembre 2023.

In breve, la direttiva si basa sull'idea che, in un'Unione europea le cui economie sono strettamente integrate, sarebbe essenziale che la riforma fiscale minima globale fosse attuata in modo sufficientemente coerente e coordinato per evitare la frammentazione del mercato interno e una struttura compatibile con le libertà fondamentali che assicuri ai contribuenti la certezza del diritto nell'attuazione di tali norme. In altre parole, poiché l'obiettivo della direttiva è proprio quello di creare un quadro comune per un livello minimo generale di tassazione nell'Unione sulla base di un approccio comune contenuto nella normativa modello dell'OCSE, la questione non può essere raggiunta dall'azione isolata degli Stati membri, in quanto un'azione indipendente degli Stati membri comporterebbe un ulteriore rischio di frammentazione del mercato interno.

In questo contesto, la direttiva stabilisce alcune disposizioni generali, stabilendo nel suo primo articolo una serie di misure comuni per la distribuzione minima effettiva dei gruppi multinazionali e dei grandi gruppi nazionali, sia sotto forma di (i) una regola di inclusione del reddito (*income inclusion rule* - IIR), con la quale un'entità controllante di un gruppo multinazionale di imprese o di un gruppo nazionale su larga scala calcola e versa la propria quota imputabile di imposta integrativa per le entità costitutive a bassa imposizione del gruppo; e (ii) una regola sui profitti a bassa imposizione (*undertaxed profit rule* - UTPR), con la quale un'entità costitutiva di un gruppo multinazionale di imprese ha un onere fiscale supplementare pari alla sua quota di imposta integrativa che non è stata applicata nell'ambito dell'IIR per le entità costitutive a bassa imposizione del gruppo.

Inoltre, la direttiva prevede anche la possibilità degli Stati membri scegliere di applicare un'imposta integrativa domestica (*Qualified Domestic Minimum Top-up Tax* - QDMTT) calcolata e versata sugli utili in eccesso di tutte le entità costitutive a bassa imposizione localizzate nella loro giurisdizione. In altre parole, le entrate raccolte secondo le Regole GloBE deriveranno dalla differenza tra il 15% dell'aliquota di imposta effettiva (*Effective Tax Rate* - ETR) e l'ETR applicata nella giurisdizione a bassa tassazione.

Si può dire che questa imposta svolge fondamentalmente due funzioni: (i) allocativa [5], cioè, di conferire alla giurisdizione "ospitante" il

[5] Sul punto, Galendi sostiene che, poiché la QDMTT corrisponde all'aliquota dell'imposta complementare moltiplicata per i profitti in eccesso, questa regola è in

© Wolters Kluwer Italia

diritto di tassare primariamente l'importo sotto tassato; (ii) semplificatrice [6], cioè, di creare una norma rispetto alla necessità di riformare l'intero sistema tributario di ciascuno Stato al fine di tassare determinate entità. Si tratta, però, di un tributo molto complesso e ancora poco chiaro nei suoi effetti.

È importante rilevare che queste regole si applicano soltanto ai gruppi di grandi società multinazionali e nazionali – la cui società madre o filiale è situata in uno Stato membro dell'UE – con entrate finanziarie totali superiori a 750 milioni di euro all'anno. Questo perché, secondo la direttiva stessa, sebbene sia necessario garantire che siano scoraggiate le pratiche di elusione fiscale, si dovrebbero evitare le ripercussioni negative sui gruppi multinazionali di imprese di dimensioni più modeste sul mercato interno.

Infine, la direttiva prevede anche alcune entità che dovrebbero essere

---

grado di annullare qualsiasi diritto di altre giurisdizioni di applicare un'imposta complementare ai sensi di un IIR o di un UTPR, a condizione che vi sia un'attuazione e un'applicazione uniforme delle *GloBE Model Rules*. Secondo l'Autore, tale meccanismo consentirebbe a una giurisdizione di riscuotere il gettito che altrimenti sarebbe stato riscosso da una giurisdizione estera sul reddito derivante da una entità costitutiva (*constituent entity* o CE) all'interno del territorio di competenza della CE stessa. In base a questo meccanismo, ipotizzando l'esistenza di IIR e UTPR in vigore a livello globale, gli Stati sarebbero fortemente incentivati a introdurre una QDMTT, consapevoli che tale introduzione non comprometterebbe la propria posizione competitiva. A questo punto, in uno scenario di implementazione e applicazione uniforme delle *GloBE Model Rules*, l'adozione di una QDMTT non comporterebbe un aumento dell'imposta totale dovuta da un'impresa multinazionale, ma comporterebbe semplicemente un cambio di giurisdizione per il pagamento dell'imposta. Se l'imposta complementare fosse riscossa in entrambi i casi in base a un IIR o a un UTPR, l'introduzione di una QDMTT consentirebbe allo Stato della CE di riscuotere l'imposta, evitando così di rinunciare al gettito a favore di un'altra giurisdizione. Da questa prospettiva, secondo l'Autore, si potrebbe argomentare che le *GloBE Model Rules* stabiliscono una soglia minima per la concorrenza fiscale, incentivando gli Stati ad adottare una QDMTT. V. R.A Galendi Junior, *The Justification and Structure of the GloBE Model Rules,* Doctoral Thesis, Universität zu Köln, 2023, pp. 231-232.

[6] Per quanto riguarda la semplificazione, Galendi sostiene che, anche in assenza di una QDMTT, il diritto iniziale di imporre un'imposta spetterebbe alla giurisdizione in cui si trova la CE, poiché, aumentando le imposte, potrebbe eliminare completamente qualsiasi addebito ai sensi di un IIR o di un UTPR. La QDMTT, quindi, consente agli Stati di definire in modo specifico l'aumento dell'imposta al minimo necessario per conformarsi alle *GloBE Model Rules*. In altre parole, se uno Stato presenta un'aliquota inferiore al 15% e si limita ad aumentare l'aliquota, le *Top-up Tax* potrebbero comunque risultare dovute, tenendo conto delle differenze nella base imponibile. Secondo l'Autore, le naturali difficoltà di una riforma generale di un sistema nazionale, che deve affrontare gli incentivi fiscali esistenti e il contesto politico che li circonda, rendono l'adozione di una QDMTT molto più praticabile, giustificandola come "un meccanismo pratico". V. R.A Galendi Junior, *Op. cit.*, pp. 232-233.

© Wolters Kluwer Italia

escluse dal suo ambito di applicazione, ad esempio, entità che non svolgono generalmente un'attività commerciale o imprenditoriale ed esercitano attività di interesse generale, quali la prestazione di assistenza sanitaria pubblica e l'istruzione o la costruzione di infrastrutture pubbliche. Prevede anche l'esclusione di fondi d'investimento e i veicoli di investimento immobiliare che si trovano al vertice della catena di proprietà, poiché il reddito conseguito da tali entità è tassato al livello della loro proprietà.

In termini generali, queste sono state delle linee guida stabilite dall'Unione europea affinché gli Stati membri mettessero in attuazione le indicazioni stabilite dall'OCSE nel suo secondo pilastro.

3. L'introduzione dell'imposta minima in Italia

Con il d. lgs. 27 dicembre 2023, n. 209 e l'art. 3 della l. 9 agosto 2023, n. 111 [7], l'Italia ha recepito la direttiva (UE) 2022/2523, introducendo, tra l'altro, (i) un'imposta minima nazionale applicabile a tutte le imprese localizzate sul territorio italiano, appartenenti a gruppi multinazionali o nazionali e soggette a un'imposizione ridotta; e (ii) un regime sanzionatorio, in linea con quello vigente per quanto concerne le imposte sui redditi, per violazioni relative agli obblighi previsti per l'imposizione minima delle imprese appartenenti a gruppi multinazionali e nazionali, nonché un regime sanzionatorio effettivo e dissuasivo per la violazione dei relativi adempimenti informativi.

L'art. 18, comma 9, del suddetto d. lgs. n. 209/2023 ha rinviato a un decreto del Ministro dell'Economia e delle Finanze l'individuazione delle disposizioni di attuazione della disciplina sull'imposta minima nazionale [8], possibilità questa prevista dall'art. 11 della direttiva (UE)

---

[7] Art. 3: "*Principi generali relativi al diritto tributario dell'Unione europea e internazionale. 1. Nell'esercizio della delega di cui all'articolo 1 il Governo osserva, oltre ai principi e criteri direttivi generali di cui all'articolo 2, anche i seguenti ulteriori principi e criteri direttivi generali: [...] e) recepire la direttiva (UE) 2022/2523 del Consiglio, del 14 dicembre 2022, seguendo altresì l'approccio comune condiviso a livello internazionale in base alla guida tecnica dell'OCSE sull'imposizione minima globale, con l'introduzione, tra l'altro, di: 1) un'imposta minima nazionale dovuta in relazione a tutte le imprese, localizzate in Italia, appartenenti a un gruppo multinazionale o nazionale e soggette a una bassa imposizione; 2) un regime sanzionatorio, conforme a quello vigente in materia di imposte sui redditi, per la violazione degli adempimenti riguardanti l'imposizione minima dei gruppi multinazionali e nazionali di imprese e un regime sanzionatorio effettivo e dissuasivo per la violazione dei relativi adempimenti informativi;(...)*".

[8] Art. 18: "*(...) 9. Le disposizioni attuative del presente articolo sono adottate*

© Wolters Kluwer Italia

2022/2523. Si tratta di quella già menzionata imposta facoltativa applicata nelle rispettive giurisdizioni che decidono di attuarla, in via prioritaria rispetto all'IIR e all'UTPR. Cioè, un'imposta di natura compensativa che, ponendosi come un'alternativa all'applicazione dell'IIR e dell'UTPR, autorizza la giurisdizione in cui sono realizzati i profitti in eccesso soggetti a un livello di imposizione inferiore al 15% a provvedere direttamente alla loro tassazione.

Essendo disegnata come "qualificata", ossia per essere detratta dall'imposizione integrativa complessivamente dovuta nello Stato, e costituire quindi un "porto sicuro", quest'imposta consente ai gruppi che intendono avvalersi della semplificazione prevista dall'OCSE, di assumere l'importo pagato a titolo di imposta minima nazionale pari all'imposizione integrativa complessivamente dovuta in Italia.

Secondo Marinello [9], la motivazione alla base di questa regola sarebbe principalmente la necessità di (i) proteggere l'efficacia delle strategie nazionali volte ad attrarre investimenti esteri in modo leale, indirizzando agevolazioni o livelli fiscali ridotti verso profitti "routinari", esclusi dall'applicazione della *minimum tax* e (ii) impedire che altri stati (e non le imprese) usufruiscano dei benefici in questione, tramite le norme IIR/UTPR dello Stato che ha rinunciato sugli *excess profits*, garantendo così anche la sovranità fiscale di ciascun sistema [10].

Inoltre, importa segnalare che quest'imposta, ai sensi dell'art. 2 del decreto, si rivolge alle imprese e alle entità a controllo congiunto localizzate in Italia, nonché alle entità apolidi costituite in base alle leggi dello Stato italiano che fanno parte di un gruppo multinazionale o nazionale che soddisfano determinati requisiti stabiliti dall'art. 10 dello stesso decreto. In brevissima sintesi, i soggetti indicati devono appartenere a gruppi multinazionali o nazionali con ricavi annui consolidati pari o superiori a 750 milioni di euro, in almeno due dei quattro esercizi immediatamente precedenti l'anno di riferimento.

---

con decreto del Ministro dell'economia e delle finanze, entro novanta giorni dalla data di entrata in vigore del presente decreto".

[9] A. Marinello, *Sovranità dello Stato e global minimum tax*, Pisa, 2023, p. 132.

[10] A proposito di quest'ultimo punto, si segnalano le interessanti osservazioni di Corasaniti, per cui sarebbe chiaro che le agevolazioni fiscali per le imprese potrebbero interferire con il funzionamento della regola, dal momento in cui il vantaggio derivante dal beneficio fiscale potrebbe portare a un'aliquota effettiva inferiore al 15% ed essere annullato l'applicazione della *minimum tax*, che riallineerebbe l'imposizione al livello minimo previsto. A questo punto, se la giurisdizione di residenza non adotta una regola del genere, lo Stato della *ultimate parent company* potrebbe beneficiare delle tasse a cui l'altra giurisdizione ha rinunciato. V. G. Corasaniti, *La minimum tax delle multinazionali: collegamenti con la riforma fiscale e con il country by country reporting, criticità e azioni,* disponibile su: *www.commercialisti.brescia.it.*

© Wolters Kluwer Italia

Infine, è opportuno evidenziare che l'art. 35 del d. lgs. n. 209/2023 prevede una riduzione dell'imposizione integrativa connessa allo svolgimento di un'attività economica sostanziale. Questo aspetto è stato recentemente affrontato nel decreto dell'11 ottobre 2024, emanato dal Vice Ministro dell'Economia e delle Finanze.

Secondo la relazione illustrativa, il nuovo decreto considera i chiarimenti contenuti nella Guida Amministrativa "*Tax Challenges Arising from the Digitalisation of the Economy – Administrative Guidance on the Global Anti-Base Erosion Model Rules (Pillar Two)*", approvata dal Quadro Inclusivo sul BEPS il 13 luglio 2023. Tali chiarimenti riguardano l'importo del reddito pertinente che può essere escluso dall'imposizione integrativa, in quanto riferibile allo svolgimento, in un determinato Stato, di un'attività economica sostanziale.

Insomma, tale riduzione, nota anche come *Substance-based Income Exclusion* (SBIE), nel senso dell'art. 2 del decreto, si calcola considerando il Valore Contabile Netto delle Immobilizzazioni Materiali Ammissibili non destinate alla vendita, all'investimento o alla locazione e i salari dei dipendenti. Il ricorso a questi indicatori di attività sostanziali deriva dal fatto che tali fattori, oltre a essere indicativi dell'effettivo esercizio di un'attività economica, presentano una mobilità ridotta e, pertanto, sono meno suscettibili al rischio di manovre elusive.

Per concludere, considerando l'obiettivo di questo lavoro, si può affermare che, in modo molto generale e sintetico, questo rappresenta l'attuale panorama legislativo riguardante la tassazione minima in Italia.

4. Conclusioni

Come è stato dimostrato nel corso di questo lavoro, i significativi progressi tecnologici degli ultimi decenni hanno avuto un impatto diretto su diversi settori del diritto, compreso quello tributario. In questo contesto, il presente studio ha cercato di dimostrare in modo descrittivo alcune delle conseguenze/problematiche fiscali associate al nuovo modello dell'economia digitale nonché le più recenti azioni intraprese dagli Stati per affrontare tali questioni.

In un primo momento, è stato analizzato il contenuto della direttiva dell'UE in materia, seguito da un'analisi più specifica dei recenti cambiamenti legislativi avvenuti in Italia negli ultimi mesi. Tuttavia, il nuovo contesto è estremamente recente e pertanto risulta lontano dall'essere pienamente risolto. Pur avendo condotto un'analisi puramente descrittiva dello scenario attuale, a causa dei limiti insiti a questo stu-

© Wolters Kluwer Italia

dio, non se nega l'esistenza di numerose debolezze e anche punti di forza di questa legislazione. Il reale impatto, però, sul sistema fiscale italiano e anche su quello europeo sarà indubbiamente oggetto di ulteriori studi e ricerche approfondite.

In ogni caso, è evidente che, per affrontare questa nuova realtà, gli Stati dovranno abbandonare una visione esclusivamente nazionale della sovranità statale e collaborare nella costruzione di soluzioni innovative per una problematica in continua evoluzione. Solo attraverso un approccio coordinato e standardizzato sarà possibile giungere a risposte e soluzione più efficaci alle sfide poste dal nuovo modello di economia digitale.

© Wolters Kluwer Italia

APPENDICE

ATTIVITÀ DIDATTICHE DEL DOTTORATO DI RICERCA IN DIRITTO PUBBLICO A.A. 2023/2024

Prof. Luigi Daniele, *I valori dell'Unione al centro del progetto di integrazione europea*.

Prof.ssa Samantha Velluti, *Climate change and forced migration after Teitiota*.

Prof. Pierluigi Simone, *La cooperazione di polizia nell'Unione europea: recenti novità nell'ottica del "codice operativo" proposto dalla Commissione*.

Dott.ssa Luisa Lodevole, *Il caso* Indi Gregory *e la dignità della vita umana: concezioni del diritto all'autodeterminazione e del diritto alla salute a confronto*.

Prof. Raffaello Lupi, Prof.ssa Alessia Vignoli, *La funzione come elemento unificante tra diritto pubblico e privato*.

Prof. Roberto Rampioni, *Il delitto di usura nella interpretazione giurisprudenziale*.

Prof.ssa Agata C. Amato Mangiameli, *Il ruolo del giurista e la funzione pedagogica del diritto*.

Prof. Luigi Daniele, *La crisi di Gaza: il ruolo della diplomazia e quello del diritto internazionale*, *discussant*: Patrizio Fondi, già Ambasciatore, Prof.ssa Federica Mucci, Dott.ssa Chiara Venturini, Dott. Riccardo Di Marco.

© Wolters Kluwer Italia

Prof. Stelio Mangiameli, *Diritto, emergenza e pubblica amministrazione*.

Prof.ssa Samantha Velluti, *Labour standards in the global garment supply chain and the proposed EU-wide mandatory due diligence regime*.

Prof. Barry Furrow, *Abortion Rights in the U.S.: What does the Dobbs case say about U.S. constitutional law?*

Dott.ssa Maria Novella Campagnoli, Gamification*: verso un nuovo paradigma*.

Prof. Roberto Cisotta*, Le recenti sentenze della Corte di giustizia sul mandato d'arresto europeo su rinvii pregiudiziali della Corte costituzionale*.

Prof.ssa Alessandra Gianelli, *La neutralità in diritto internazionale*.

Prof. Fabio Spitaleri, *La tutela giurisdizionale effettiva dei singoli nei settori dell'immigrazione e dell'asilo*.

Prof. Pierluigi Simone, *Le c.d. competenze deboli dell'Unione europea*.

Prof. Alessandro Dani, *Il "peso dei numeri": come le dinamiche demografiche hanno più volte inciso nella storia degli ordinamenti giuridici*.

Prof. Alberto Zito, *La discrezionalità amministrativa tra ragionevolezza e razionalità*.

Prof. Alberto Zito, Nudge Theory *e agire amministrativo*.

Prof. Luigi Daniele, Prof.ssa Federica Mucci, Dott.ssa Chiara Venturini, *L'obbligo degli Stati di prevenire il genocidio nella recente prassi internazionale*.

Prof. Carlo Longari, Avv. Federico Bonaiuto, General Counsel di Leonardo, *Rapporto tra l'Organismo di Vigilanza della società controllante e gli Organismi di Vigilanza delle controllate*.

© Wolters Kluwer Italia

Prof. Luigi Daniele, *L'Unione europea e le crisi del mondo contemporaneo*.

Prof. Alberto Zito, *Intelligenza artificiale e pubblica amministrazione: problemi e prospettive*.

Dott.ssa Federica Palomba, Dott. Gabriele Dammicco, *Contratti pubblici: aggiudicazione e rinegoziazione fra il principio del risultato e la tutela della concorrenza*.

Prof. Nino Paolantonio, Prof. Alberto Zito, *La concretizzazione dell'interesse pubblico nell'azione amministrativa*.

Prof. Luigi Daniele, *Le prossime elezioni del Parlamento europeo nella prospettiva della riforma dei Trattati*.

Prof. Michał Gierycz, *discussant*: Dott.ssa Luisa Lodevole, *Person and Nation: perspective of John Paul II*.

Prof.ssa Maria Rosa Di Simone, *Il delitto di stregoneria. Fonti normative e scienza giuridica tra medioevo ed età moderna*.

Prof. Nino Paolantonio, Prof. Alberto Zito, *Il sindacato giurisdizionale sull'azione amministrativa*.

Prof. Stelio Mangiameli, *Riforma del premierato e legge elettorale*.

Prof. Carlo Longari, Dott. Andrea Abodi, Ministro dello Sport, *Violenze negli stadi e relative sanzioni*.

Prof. Massimo Gandolfini, *Nuove tecnologie e dipendenze*.

Prof.ssa Arianna Andreangeli, *L'intelligenza artificiale e il diritto della concorrenza: riflessioni sull'*Artificial Intelligence Act.

Prof.ssa Agata C. Amato Mangiameli, Dott.ssa Paola Bianchi, *Il rifiuto da parte del figlio a incontrare un genitore o gli ascendenti: art. 473-bis. 6 c.p.c.*

Dott. Luca Panico, *Temi e riflessioni su "Carl Schmitt. Il problema della mediazione giuridica nel «politico»"*.

© Wolters Kluwer Italia

Prof. Victor Grandaubert, *discussant*: Dott. Riccardo Di Marco, Dott.ssa Chiara Venturini, *Green transition and critical raw materials: legal issues and prospects?*

Dott. Luigi Prosia, *Pungoli digitali e Super Data. Propositi e sviluppi in chiave di sostenibilità e sicurezza*.

Dott.ssa Chiara Venturini, Dott. Riccardo Di Marco, *Future Generazioni*.

Dott.ssa Cristina Colombo, *Terrorismo come macroarea criminologica. "Il caso di «Sendero Luminoso»"*.

Prof. Giorgio Ricci, Prof. Furio Pesci, *IA, post-umano, trans-umano*.

Convegno in omaggio a Claudio Franchini, *Sul potere amministrativo e sulla sua legittimazione*.

Prof. Stelio Mangiameli, *Il suicidio assistito tra Regioni e Servizio Sanitario*.

Prof. Guido Saraceni, *Giustizia e disagio mentale*.

Prof. Carlo Pisani, *Certezza del diritto, volontà del legislatore, ruolo della Corte costituzionale nell'evoluzione della disciplina rimediale per il licenziamento ingiustificato*.

Prof. Stephane Bauzon, *The concept of fairness in Aristotle's philosophy.*

Prof.ssa Elda Turco Bulgherini*, La legge sullo spazio ed il ruolo dell'Agenzia Spaziale Italiana – ASI*.

Prof. Alessandro Dani, *Il giudice e le fonti del diritto nell'Antico regime*.

Prof.ssa Federica Mucci, *Diversità biologica nel mare internazionale e "*Stewardship*" degli Stati. Uno* standard *a vocazione universale per una VIA il più partecipata possibile*.

© Wolters Kluwer Italia

UNIVERSITÀ DEGLI STUDI DI ROMA "TOR VERGATA"
PUBBLICAZIONI DELLA FACOLTÀ DI GIURISPRUDENZA

SEZIONE DI DIRITTO PUBBLICO

1. Scritti in memoria di Pietro Gismondi - Vol. I (1987) - Vol. II (1991) - Vol. III (1988).
2. Leanza U. (a cura di), *Il regime giuridico internazionale del mare Mediterraneo* (1987).
3. Leanza U. (a cura di), *Costituzione dello Stato e norme internazionali* (1988).
4. Pezzini B., *Il Bundesrat della Germania Federale* (1990).
5. Lillo P., *Concordato, «accordi» e «intese» tra lo Stato e la Chiesa cattolica* (1990).
6. Lillo P., *L'adattamento dell'ordinamento interno al "diritto pattizio"* (1992).
7. Mangiameli S., *Le materie di competenza regionale* (1992).

SEZIONE DI DIRITTO E PROCEDURA CIVILE

1. Carratta A., *Il principio della non contestazione nel processo civile* (1995).
2. Lener R., *Forma contrattuale e tutela del contraente "non qualificato" nel mercato finanziario* (1996).
3. Massa Felsani F., *Contributo all'analisi del know-how* (1997).
4. Figà-Talamanca G., *Bilanci e organizzazione dei poteri dispositivi sul patrimonio sociale* (1997).
5. Morace Pinelli A., *La crisi coniugale tra separazione e divorzio* (2001).

SEZIONE DI STORIA E TEORIA DEL DIRITTO

1. Cardilli R., *L'obbligazione di «praestare» e la responsabilità contrattuale in diritto romano (Il sec. a.C. -Il sec. d.C.)* (1995).
2. Petrucci A., *Il trionfo nella storia costituzionale romana dagli inizi della repubblica ad Augusto* (1996).
3. Bauzon S., *Il mestiere del giurista.* Il diritto politico nella prospettiva di Michel Villey (2001).
4. Saccoccio A., *Si certum petetur.* Dalla *condictio* dei *veteres* alle *condictiones* giustinianee (2002).
5. Vinci M., *Fines regere.* Il regolamento dei confini dall'età arcaica a Giustiniano (2004).
6. Bianchi P., *Iura-leges. Un'apparente questione terminologica della tarda antichità. Storiografia e storia* (2007).
7. Zhang L., *Contratti innominati nel diritto romano.* Impostazioni di Labeone e di Aristone (2007).

8. Calore E., *Actio quod metus causa.* Tutela della vittima e azione *in rem scripta* (2011).

NUOVA SERIE

1. *I mercati monetari finanziari in Italia fra internazionalizzazione e controllo*, a cura di Enzo Rossi (1998).
2. Rota R., *Gli interessi diffusi nell'azione della pubblica amministrazione* (1998).
3. *Scritti in onore di Serio Galeotti* - Tomo I-II (1998).
4. Morozzo Della Rocca P., *Gratuità, liberalità e solidarietà.* Contributo allo studio della prestazione non onerosa (1998).
5. Xerri Salamone A., *L'ordinamento giuridico dei porti italiani* (1998).
6. *La legge sul procedimento amministrativo*. Legge 7 agosto 1990 n. 241 - Prospettive di alcuni istituti, a cura di Francesco Paolo Pugliese (1999).
7. Masini S., *Ambiente, agricoltura e governo del territorio*. Contributo ad uno studio sulla riforma delle autonomie locali (2000).
8. Giacobbe E., *Brokeraggio e tipo contrattuale* (2001).
9. *Il corpo de-formato*. Nuovi percorsi dell'identità personale, a cura di Francesco D'Agostino (2002).
10. Rossi R., *Insolvenza, crisi di impresa e risanamento*. Caratteri sistematici e funzionali del presupposto oggettivo dell'amministrazione straordinaria (2003).
11. Semeraro M., *Il tribunale del Santo Officio di Oria*. Inediti processi per la storia dell'Inquisizione in età moderna (2003).
12. Tucci A., *Gestione dell'impresa sociale e "supervisione" degli azionisti*. L'esperienza italiana a confronto con la disciplina delle *public companies* nordamericane (2003).
13. Morace Pinelli A., *Interesse della famiglia e tutela dei creditori* (2003).
14. Arru D., *Il concordato italiano del 1803* (2003).
15. Tarullo S., *Il giusto processo amministrativo*. Studio sull'effettività della tutela giurisdizionale neila prospettiva europea (2004).
16. *Corpo esibito, corpo violato, corpo venduto, corpo donato*. Nuove forme di rilevanza giuridica del corpo umano, a cura di Francesco D'Agostino (2003).
17. Iurilli C., *Autonomia contrattuale e garanzie nella vendita di beni di consumo* (2004).
18. Scognamiglio A., *Il diritto di difesa nel procedimenio amministrativo* (2004).
19. Masini S., *La piccola impresa agricola* (2004).
20. Saraceni E. G., *L'autorità ragionevole*. Premesse per uno studio del diritto canonico amministrativo secondo il principio di ragionevolezza (2004).
21. Tzitzis S., *La vittima e il carnefice*. Lezioni romane di filosofia del dirit-

to, a cura di Francesco D'Agostino e Fabio Macioce. Traduzione di Fabio Macioce (2004).

22. Scacchi A., *La proprietà temporanea* (2005).
23 Lanni S., *America latina e tutela del consumatore*. Le prospettive del mercosur tra problemi e tecniche di unificazione del diritto (2005).
24. Dipace R., *Partenariato pubblico privato e contratti atipici* (2006).
25. Nardi S., *Frode alla legge e collegamento negoziate* (2006).
26. Gambino G., *Le unioni omosessuali*. Un problema di filosofia del diritto (2007).
27. Morace Pinelli A., *Atti di destinazione,* trust *e responsabilità del debitore* (2007).
28. *I beni pubblici: tutela, valorizzazione e gestione*. Atti del Convegno di Studi - Ville Tuscolane, 16-18 novembre 2006, a cura di Aristide Police (2008).
29. Caprioli S., *Codice civile*. Struttura e vicende (2008).
30. Bellante M., *La caparra* (2008).
31. Scoca S. S., *Evidenza pubblica e contratto: profili sostanziali e processuali* (2008).
32. *Darwinismo e problemi di giustizia*, a cura di Francesco D'Agostino (2008).
33. Cataudella M. C., *Contratto di lavoro e nullità parziale* (2008).
34. Votrico A., *Uccidersi per uccidere. Il suicidio per vendetta* (2009).
35. Fioravanti M., *Le potestà normative del Governo*. Dalla Francia *d'ancien régime* all'Italia liberale (2009).
36. Franza G., *Il lavoro a termine nell'evoluzione dell'ordinamento* (2010).
37. Sangermano F., *Presupposizione e causa nel negozio testamentario* (2011).
38. *Studi in onore di Pierfrancesco Grossi*, a cura di Antonio D'Atena (2012).
39. Arru D., *La legislazione della Repubblica romana del 1849 in materia ecclesiastica*. Prefazione di Mauro Ferri - Presidente Emerito della Corte Costituzionale (2012).
40. Roiati A., *Medicina difensiva e colpa professionale medica in diritto penale*. Tra teoria e prassi giurisprudenziale (2012).
41. Chizzola F., *La relazione umana alla luce della differenza sessuale* (2012).
42. Sirgiovanni B., *Prefazione legale e acquisto della proprietà* (2012).
43. Gabrielli E., *"Operazione economica" e teoria del contratto. Studi* (2013).
44. Iurilli C., *Interessi superindividuali e danno collettivo* (2016).
45. Grisafi R., *Sopravvenienze, squilibri contrattuali e ruolo della presupposizione* (2016).

46. Massella Ducci Teri N., *Contributo ad una teoria generale del negozio di recesso* (2016).

TERZA SERIE (Wolters Kluwer)

1. Mancinetti G., *L'emersione dei doveri «accessori» nella* 'locatio conductio' (2017).
2. Marini R., *Contrarius consensus* (2017).
3. Sirgiovanni B., *Autonomia privata e risoluzione del contratto per inadempimento* (2019).
4. *I diversi settori del Fintech. Problemi e prospettive*, a cura di Corapi E. - Lener R. (2019).
5. Leonardi F., *Comportamento omissivo dell'impresa e pratiche commerciali scorrette* (2019).
6. Gabrielli E., *L'autonomia privata vol. 1. Dal contratto alla crisi d'impresa* (2019).
7. Iurilli C., *I contratti di gioco e scommessa all'epoca del disturbo da gioco* (2020).
8. Madia N., *Ne bis in idem europeo e giustizia penale. Analisi sui riflessi sostanziali in materia di convergenze normative e cumuli puntivi nel contesto di uno sguardo d'insieme* (2020).
9. Vignoli A., *La giurisdizione nella funzione tributaria* (2020).
10. Longari C., *Soglie di punibilità e diritto penale tributario* (2020).
11. Rossi M., *Pagamenti intermediati e disciplina concorsuale* (2020).
12. Gabrielli E., *L'autonomia privata vol. 2. Teoria del contratto e diritto comparato* (2021).
13. Ricciuto V. e Solinas C., *Forniture di servizi digitali e «pagamento» con la prestazione dei dati personali. Un discusso profilo dell'economia digitale* (2022).
14. Iurilli C., *Mutui e nullità di scopo* (2022).
15. Longari C., *«Esiguità dell'offesa» vs. «colpa di organizzazione» nella responsabilità da reato degli enti*. Tra interpretazione analogica e sistematica (2022).
16. Lattanzi S., *I 'travaux préparatoires' del diritto dell'Unione europea: tassonomia, ruolo e funzioni* (2022).
17. Colombo C., *Il bullismo, un terreno di verifica per la devianza minorile* (2023).
18. Corapi E. (a cura di), *Sostenibilità e mercato finanziario. Questioni aperte e profili comparati* (2023).
19. Santoni G., *La piattaforma* online *e l'illecito civile dell'utente: dalla gatekeeper liability alla regolazione degli algoritmi* (2024).
20. Gabrielli E., *L'autonomia privata vol. 3. Il diritto della giurisprudenza e della dottrina* (2024).
21. Daniele L. - Simone P. - Venturini C. - Di Marco R. (a cura di), *L'Unio-*

ne europea e le crisi del mondo contemporaneo. Tra "valorizzazione" delle competenze e prospettive di riforma (2025).

QUADERNI DEL DOTTORATO DI RICERCA IN DIRITTO PUBLICO

1. *Principi generali del diritto, diritti fondamentali e tutela giurisdizionale: nuove questioni*, a cura di Luigi Daniele e Andrea Buratti (2019).
2. *Le sanzioni: poteri, procedimenti e garanzie nel diritto pubblico*, a cura di Aristide Police e Cristiano Cupelli (2020).
3. *L'emergenza pandemica e l'impatto sul diritto pubblico: innovazione e prospettive future*, a cura di Donatella Morana e Stefania Mabellini (2022).
4. *Il ritorno dello Stato. Spunti giuridici per un rapporto equilibrato tra mercato e intervento pubblico*, a cura di Raffaello Lupi e Marco Fioravanti (2023).
5. *Giustizia e Potere(i). Riflessioni sull'indipendenza del giudice*, a cura di Luigi Daniele, Alessia Vignoli e Maria Novella Campagnoli (2024).
6. *Nuove tecnologie e diritto. Opportunità e rischi per la società del XXI secolo*, a cura di Agata C. Amato Mangiameli, Pierluigi Simone, Chiara Venturini (2025).