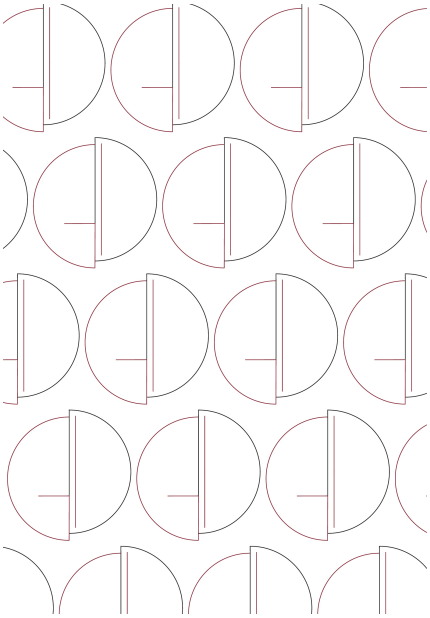
Materiali e documenti

Annuario 2022 Osservatorio Giuridico sulla Innovazione Digitale

Yearbook 2022 Juridical Observatory on Digital Innovation

a cura di
Salvatore Orlando e Giuseppina Capaldo



University Press

Sapienza Università Editrice

Collana Materiali e documenti 90

Annuario 2022
Osservatorio Giuridico sulla Innovazione Digitale

Yearbook 2022
Juridical Observatory on Digital Innovation

a cura di
Salvatore Orlando e Giuseppina Capaldo

SAPIENZA
UNIVERSITÀ EDITRICE
2022

Sapienza Università Editrice
Piazzale Aldo Moro 5 – 00185 Roma

www.editricesapienza.it
editrice.sapienza@uniroma1.it

Iscrizione Registro Operatori Comunicazione n. 11420
Registry of Communication Workers registration n. 11420

ISBN 978-88-9377-256-3

DOI 10.13133/9788893772563

Pubblicato nel mese di dicembre 2022 | *Published in December 2022*

Impaginazione a cura di | *Layout by*: Lucio Casalini e Enzo Maria Incutti

In copertina | *Cover image*: Michela Tenace, *Elaborazione grafica del logo OGID/JODI*, 2022, Archivio personale dell'a.

Indice

12. L'intelligenza artificiale nel prisma dell'impresa: evoluzione normativa e prospettive di studio

Francesco Pacileo (Università di Roma La Sapienza)

12.1. Alcuni fra i principali rischi connaturati all'intelligenza artificiale

Le istituzioni europee e la letteratura scientifica hanno evidenziato alcuni rischi connaturati all'impiego dei sistemi di intelligenza artificiale (IA) [1] ed al connesso utilizzo dei *big data* [2].

---

[1] Ad oggi non esiste ancora una definizione univocamente accettata e compiuta di "intelligenza artificiale. Per una definizione, anche con riferimento al *machine learning* ed al *deep learning* cfr., comunque, COMMISSIONE EUROPEA, *L'intelligenza artificiale per l'Europa*, COM(2018) 237 final, Bruxelles, 25 aprile 2018, pt. 1, secondo cui «"Intelligenza artificiale" (IA) indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi». In dottrina, cfr. M. GUIHOT, A.F. MATTHEW, N.P. SUZOR, *Nudging Robots: Innovative Solutions to Regulate Artificial Intelligence*, in 20 *Vand. J. Ent. & Tech. L.* (2017), da p. 385, pp. 393 ss.; M.U. SCHERER, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, in 29 *Harv. J.L. & Tech.* (2016), da p. 354, pp. 359 ss.; A. BERTOLINI, *Artificial Intelligence and Civil Liability*, Study requested by JURI committee, July 2020, p. 9, pp. 15 ss. Per ulteriori definizioni di "electronic agent", S. WETTIG, E. ZEHENDNER, *A legal analysis of human and electronic agents*, in 12 *AI & L.* (2004), da p. 111, pp. 129 ss. Cfr., inoltre, M. HILDEBRANDT, *Law* as *Information in the Era of Data-Driven Agency*, in 79 *Modern L. Rev.* (2016), da p. 1, p. 4.

[2] Per una definizione anche del c.d. *big data analytics* cfr. BANCA D'ITALIA, *Fintech in Italia. Indagine conoscitiva sull'adozione delle innovazioni tecnologiche applicate ai servizi finanziari*, dicembre 2017, in www.bancaditalia.it, 31, secondo cui essi costituiscono un «insieme di dati di enorme dimensione, memorizzati anche in archivi eterogenei, ossia non correlati tra loro, per la cui analisi vengono utilizzati strumenti di statistica inferenziale e concetti di identificazione di sistemi non lineari per dedurre regressioni, effetti causali e relazioni. A differenza dei sistemi gestionali tradizionali, che trattano

Al riguardo si segnalano innanzi tutto il rischio di "contagio", inconsapevole o meno, dai programmatori ed utilizzatori all'algoritmo, di pregiudizi ed elementi ingiustificatamente discriminatori [3]; il rischio di sviluppi dannosi imprevisti ed imprevedibili degli algoritmi soprattutto di *machine learning* [4]; i rischi, strettamente collegati all'ultimo menzionato, conseguenti alla difficoltà se non addirittura all'impossibilità di ricostruire tutti i processi logici che hanno portato ad un determinato *output* (c.d. *black box algorithm*) [5].

Tuttavia, alla maggiore complessità dell'algoritmo e alla mole di dati trattati corrisponde in maniera direttamente proporzionale una maggiore *accuracy* delle previsioni e degli *output* [6].

---

dati strutturati o strutturabili in tabelle tra loro relazionabili, i big data comprendono anche dati semistrutturati o non strutturati (ad es. dati che provengono dal web come i commenti sui social media, documenti di testo, audio, video disponibili in diversi formati, etc.)»; FSB, *Artificial intelligence and machine learning in financial services. Market developments and financial stability implications*, 1 November 2017, in www.fsb.org, 4 ss.

[3] Cfr. S. BAROCAS, A.D. SELBST, *Big Data' s Disparate Impact*, in 104 *Cal. L. Rev.* (2016), da p. 671, p. 677 ss.; M. GUIHOT, A.F. MATTHEW, N.P. SUZOR, *Nudging Robots*, cit., pp. 404 s.; J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YUT, *Accountable Algorithms*, in 165 *U. Pa. L. Rev.* (2017), da p. 633, pp. 678 ss.; M. HILDEBRANDT, *Law* as *Information*, cit., pp. 24 s.; L. ENRIQUES, D. ZETZSCHE, *Corporate Technologies and the Tech Nirvana Fallacy*, in 72 *Hastings L. J.* (2020), da p. 55, 66 ss. e *passim* Nella letteratura italiana, cfr. N. ABRIANI, G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corptech*, Bologna, 2021, 38 ss.; A. NUZZO, *Algoritmi e regole*, in *AGE*, 1/2019, da p. 39, p. 43.

[4] Cfr. H. EIDENMÜLLER, *The Rise of Robots and the Law of Humans*, Oxford Legal Studies Research Paper No. 27/2017, p. 5, secondo cui detti sistemi «are unpredictable by design»; H. ZECH, *Zivilrechtliche Haftung für den Einsatz von Robotern – Zuweisung von Automatisierungs- und Autonomierisiken*, in *Intelligente Agenten und das Recht*, Hrsg. S. Gless, K. Seelmann, Baden Baden, 2016, da p. 163, pp. 172 ss.; U. PAGALLO, *Killers, fridges, and slaves: a legal journey in robotics*, in *AI & Society*, January 2011, p. 6.

[5] Sul *black box algorithm* cfr. F. PASQUALE, *The Black Box Society. The secret Algorithms That Control Money and Information*, Cambridge-London, 2015; J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YUT, *Accountable Algorithms*, cit., *passim*; M. HILDEBRANDT, *Law* as *Information*, cit., p. 26; Y. BATHAEE, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, in 31 *Harvard Journal of Law & Technology* (2018), da p. 889; E. PELLECCHIA, *Profilazione e decisioni automatizzate al tempo della* black box society*: qualità dei dati e leggibilità dell'algoritmo nella cornice della* responsible research and innovation, in *NLCC*, 2018, da p. 1209, 1209 ss. spec. 1212; A. NUZZO, *Algoritmi e regole*, cit., p. 44; M.L. MONTAGNANI, *Flussi informativi e doveri degli amministratori di società per azioni ai tempi dell'intelligenza artificiale*, in *Persona e Mercato*, 2020/2, da p. 65, pp. 78 ss. Cfr., altresì, COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*, Bruxelles, 19 febbraio 2020, COM(2020) 65 final, p. 13.

[6] Cfr. A. MATTHIAS, *Automaten als Träger von Rechten. Plädoyer für eine Gesetzänderung*,

Una trattazione a parte, che non può essere effettuata in questa sede, meriterebbero poi i rischi connessi a chi dispone dei *big data* nonché i rischi connessi a dolose manomissioni e ad attacchi informatici, sintetizzabili nell'espressione *cybersecurity* ovvero connessi alla protezione della riservatezza e dei dati personali.

Nondimeno alcune fra le questioni (anche) giuridiche maggiormente controverse sorgono in relazione alla capacità o meno dei sistemi di IA di assumere "decisioni" (si preferisce il temine *output*) e di assumerle in maniera sostanzialmente autonoma [7] rispetto ai programmatori, fornitori, utilizzatori e tutti i componenti della catena di valore dei sistemi di IA.

In particolare, un'attenta dottrina ha segnalato un potenziale vuoto di responsabilità (*Verantwortungslücke*) che consiste nella difficoltà per gli uomini ad avere un sufficiente controllo sulle macchine autonome, tale da giustificare una responsabilità correlata all'abilità del controllore: in particolare, detta difficoltà discende non solo dalla menzionata imprevedibilità (*Unberechenbarkeit*) di tali macchine ma altresì dalla circostanza che esse si trovano al di là dell'"orizzonte visuale" del produttore, il quale allora si troverebbe nell'impossibilità di evitare il pregiudizio [8].

Berlin, 2008, p. 22, p. 37; P.B. DE LAAT, *Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?*, in 31 *Philos. Techn.* (2018), da p. 525.

[7] Sull'autonomia dell'IA cfr. COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale*, cit., p. 18; COMMISSIONE EUROPEA, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*, COM(2020) 64 final, Bruxelle, 19 febbraio 2020, pp. 7 s. In dottrina, cfr. A. WIEBE, *Die elektronische Willenserklärung*, Tübingen, 2002, pp. 27 ss. Nella letteratura italiana, cfr. A. BERTOLINI, *Robots as Products: The Case for Realistic Analysis of Robotic Applications and Liability Rules*, in *Law, Innovarion, Technology*, 2013, da p. 213, pp. 220 ss. Sui concetti di indipendenza e controllo cfr., altresì, R. ABBOTT, *The Reasonable Computer: Disrupting the Paradigm of Tort Liability*, in 86 *Wash. L. Rev.* (2018), da p. 1, p. 23. Cfr. U. PAGALLO, *Killers, fridges, and slaves*, cit., p. 6; ID., *The Law of Robots: Crimes, Contracts and Torts*, Heidelberg-New York-London, 2013, p. 2, secondo cui sussiste autonomia quanto i robot «sense-think-act» senza l'intervento o il coinvolgimento degli uomini. Nella letteratura giuridica, propendono per la capacità di assumere decisioni R. ABBOTT, *The Reasonable Computer*, cit., p. 23; T. ALLEN, R. WIDDISON, *Can Computers Make Contracts?*, in 9 *Harv. J. L. & Tech.* (1996), da p. 25, p. 27; R. ROMANO, *Intelligenza artificiale, decisioni e responsabilità in ambito finanziario*, cit., p. 325. Di opposto avviso, H. EIDENMÜLLER, *The Rise of Robots and the Law of Humans*, cit., pp. 12 ss.; H.P. BULL, *Sinn und Unsinn des Datenschutzes*, Tübingen, 2015, pp. 118 ss.

[8] Cfr. A. MATTHIAS, *op. loc. cit.*; B.-J. KOOPS, M. HILDEBRANDT, D.-O. JAQUET-CHIFFELLE, *Bridging the Accountability Gap: Rights for New Entities in the Information Society?*, in 11

L'importanza e la serietà del problema è certificata da una risoluzione del Parlamento europeo del 2017 (di seguito anche "Risoluzione del 2017"), che individua, tra un ventaglio di ipotesi di regolamentazione di diritto civile della robotica, anche quella di istituire normativamente una «personalità elettronica» («electronic person») da attribuire all'IA, che in tal modo verrebbe ad avere una propria soggettività giuridica, un proprio patrimonio ed una propria responsabilità [9].

Il rischio più grave, allora, può apparire quello di parificare in qualche modo esseri umani e sistemi di IA e, di conseguenza, di comprimere, e di comprimere eccessivamente, gli affari e le attività umane se non addirittura l'essenza degli esseri umani [10].

12.2. Il difficile inquadramento della natura giuridica dell'IA. Opportunità di un'interpretazione funzionale ed evolutiva

Prendendo parte all'esercizio intellettuale denominato "Gaio digitale" in voga tra i relatori dell'Osservatorio Giuridico sull'Innovazione Digitale, i problemi finora posti in evidenza potrebbero spingere persino a domandarsi ove si collochi l'IA nell'ambito della nota tripartizione gaiana [11]. Nondimeno si crede opportuno seguire un approccio

Minn. J. L. Sci. & Tech. (2010), da p. 497, p. 546, p. 553. Cfr., altresì, G. TEUBNER, *Digitale Rechtssubjekte? Zum privatrechtlichen Status automater Softwareagenten*, in 218 *AcP* (2018), da p. 155, (anche nella versione in italiano *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, a cura di P. Femia, Napoli, 2019), p. 157 ss.

[9] Cfr. PARLAMENTO EUROPEO, *Norme di diritto civile sulla robotica. Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, (2015/2103(INL), 17 febbraio 2017, P8_TA(2017)0051, ptt. 49 ss. spec. pt. 59, lett. (*f*). In dottrina, cfr. H. EIDENMÜLLER, *The Rise of Robots and the Law of Humans*, cit., critico; B.-J. KOOPS, M. HILDEBRANDT, D.-O. JAQUET-CHIFFELLE, *Bridging the Accountability Gap*, cit., p. 510; G. SCARCHILLO, Corporate Governance *e Intelligenza Artificiale*, in *NGCC*, 2019, da p. 881, p. 884; R. ROMANO, *Intelligenza*, cit., pp. 326 ss.

[10] Cfr., tra i molti che paventano un rischio di sopravvivenza dell'umanità di essere sopraffatta da macchine con intelligenza superiore, B.-J. KOOPS, M. HILDEBRANDT, D.-O. JAQUET-CHIFFELLE, *Bridging the Accountability Gap*, cit., *passim*, spec. pp. 557 ss.; I. OLEKSIEWICZ, M.E. CIVELEK, *From Artificial Intelligence to Artificial Consciousness: Possible Legal Bases for the Human-Robot Relationships in the Future*, in 7 *Int. J. Adv. Res.* (2019), da p. 254. Cfr., altresì, U. RUFFOLO, A. AMIDEI, *Intelligenza Artificiale e diritti della persona: le frontiere del ''transumanesimo''*, in *Giur. it.*, 2019, da p. 1658.

[11] Il riferimento va alla nota massima «Omne autem ius quo utimur, vel ad personas pertinet vel ad res vel ad actiones» (Gai. 1.8). Per l'esercizio intellettuale relativo a

funzionale e allora in questi termini l'impressione è che assuma uno specifico interesse scientifico la prospettiva dell'*impresa* e, specificamente, dell'impresa organizzata in forma societaria, ed in particolare di una società che può permettersi di disporre di simili tecnologie, quindi oggi una società di capitali [12].

La prospettiva dell'impresa, si crede, pur non dovendosi considerare in termini assoluti, è senz'altro centrale nell'analisi giuridica dell'IA, posto che buona parte di produttori, programmatori e degli utilizzatori di questi sistemi sono imprese, e imprese organizzate in forma di società di capitali, o comunque persone fisiche che operano nell'ambito di un'organizzazione imprenditoriale.

Trascurare questo dato di fatto potrebbe implicare criticità non dissimili da quelle riscontrate nel diritto concorsuale, ove la legge fallimentare è impostata sulla crisi e l'insolvenza del debitore imprenditore individuale ma poi la maggior parte dei debitori sottoposti a procedure concorsuali sono società, e società di capitali.

L'indagine circa l'opportunità di un'impostazione incentrata sull'impresa può procedere sulla base di almeno due percorsi, non necessariamente alternativi: l'analisi del dibattito dottrinale in merito alla natura giuridica dell'IA [13] e lo studio dell'evoluzione normativa tuttora in atto, quanto meno nell'UE. Per esigenze di sintesi, le successive pagine si concentreranno su tale ultimo aspetto.

"Gaio digitale" sono debitore di D. IMBRUGLIA, che ringrazio, e che pure ha scritto *L'intelligenza artificiale (IA) e le regole. Appunti*, in *Media Laws*, 2020, da p. 18.

[12] Sul tema dell'IA e della *corporate governance* cfr. M. FENWICK, J.A. MCCAHERY, E. P.M. VERMEULEN, *The End of Corporate Governance*, working paper, in *ECGI*, December 2018; M. FENWICK, E. P.M. VERMEULEN, *Technology and Corporate Governance: Blockchain, Crypto and Artificial Intelligence*, working paper, in *ECGI*, November 2018; F. MÖSLEIN, *Robots in the Boardroom: Artificial Intelligence and Corporate Law*, in W. Barfield, U. Pagallo (Eds.), *Research Handbook on the Law of Artificial Intelligence*, Northampton MA, 2018, da p. 649; L. ENRIQUES, D. ZETZSCHE, *Corporate Technologies*, cit.; J. ARMOUR, H. EIDENMÜLLER, *Self-Driving Corporations?*, in 10 *Harvard Business Law Review* (2020), da p. 87; L. LOPUCKY, *Algorithmic Entities*, in 95 *Wash. U. L. Rev.* (2018), da p. 887. Nella letteratura italiana cfr. G.D. MOSCO, *Roboboard. L'intelligenza artificiale nei consigli di amministrazione*, in *AGE*, 1/2019, da p. 247; N. ABRIANI, G. SCHNEIDER, *Il diritto societario incontra il diritto dell'informazione.* IT, Corporate governance *e* Corporate Social Responsibility, in *Riv. soc.*, 2020, da p. 1326; N. ABRIANI, *La* corporate governance *nell'era dell'algoritmo. Prolegomeni a uno studio sull'impatto dell'intelligenza artificiale sulla* corporate governance, in *NDS*, 2020, da p. 261; G. SCARCHILLO, Corporate Governance *e Intelligenza Artificiale*, in *NGCC*, 2019, da p. 881, M.L. MONTAGNANI, *Flussi informativi*, cit.

[13] Cfr., per tutti, B.-J. KOOPS, M. HILDEBRANDT, D.-O. JAQUET-CHIFFELLE *Bridging the Accountability Gap*, cit., *passim*; G. TEUBNER, *Digitale Rechtssubjekte?*, cit., *passim*.

12.3. Mancanza di una regolamentazione compiuta in tema di IA

Le istituzioni europee hanno promosso e portato avanti numerose ricerche sul tema: in particolare si è preso atto che ad oggi non esiste una normativa che disciplini in maniera soddisfacente l'impiego dell'IA e dei *big data*.

Qualche spunto potrebbe ricavarsi dalla direttiva sui prodotti difettosi (85/374/CEE del Consiglio) [14], ma con risultati parziali, come osservato dalla stessa Commissione europea [15].

Al riguardo, tale ultima direttiva è applicabile limitatamente ai danni materiali patiti dai consumatori, mentre andrebbe chiarito il concetto di "difettosità" dei sistemi di IA e se tali sistemi rientrino nella nozione di "prodotti" o in quella di "servizi" [16]. Significativamente gravoso, inoltre, può risultare l'onere probatorio a carico del danneggiato, che attualmente deve dimostrare il danno patito ed il nesso di

---

[14] Anche nell'ordinamento degli Stati Uniti la disciplina dei prodotti difettosi è stata attentamente presa in considerazione dalla dottrina, ai fini dell'applicabilità alle nuove tecnologie quale regola di responsabilità da *tort*. Cfr. R. ABBOTT, *The Reasonable Computer*, cit., pp. 13 ss., 22 ss.; D.C. VLADECK, *Machines without Principals: Liability Rules and Artificial Intelligence*, in 89 *Wash. L. Rev.* (2014), da p. 117, pp. 127 ss., seppure in chiave critica. Nella letteratura italiana, cfr. A. BERTOLINI, *Robots as Products*, cit., pp. 235 ss.; L. LIGUORI, in M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di Intelligenza Artificiale, responsabilità e* accountability*. Verso nuovi paradigmi?*, in *Intelligenza Artificiale, protezione dei dati personali e regolazione*, a cura di F. Pizzetti, Torino, 2018, da p. 333, pp. 348 ss., ove numerosi riferimenti giurisprudenziali.

[15] Cfr., sul tema della responsabilità *de qua*, PARLAMENTO EUROPEO, *Norme di diritto civile sulla robotica*, cit.; COMMISSIONE EUROPEA, Relazione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo «sull'applicazione della direttiva del Consiglio relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi (direttiva 85/374/CEE)», COM(2018) 246 final, Bruxelles, 7 maggio 2018; COMMISSIONE EUROPEA, *L'intelligenza artificiale per l'Europa*, COM(2018) 237 final, Bruxelles, 25 aprile 2018; COMMISSIONE EUROPEA, *Liability for emerging digital technologies*, SWD(2018) 137 final; COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale*, cit., pp. 14 ss.; FSB, *op. cit.*, p. 26, 38. In dottrina, cfr. A. AMIDEI, *Intelligenza Artificiale e* product liability*: sviluppi del diritto dell'Unione Europea*, in *Giur. it.*, 2019, da p. 1715.

[16] Cfr. COMMISSIONE EUROPEA, COM(2018) 246 final, *cit.*, pt. 5.4.; COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale*, cit., pp. 14 ss.; A. BERTOLINI, *Artificial Intelligence and Civil Liability*, cit., pp. 50 ss.; H. ZECH, *Zivilrechtliche Haftung*, cit., p. 176, pp. 184 s.; A. AMIDEI, *Intelligenza Artificiale*, cit., pp. 1720 ss.

causalità tra danno e difetto. Occorrerebbe poi aggiornare la nozione di "produttore" [17].

In buona sostanza, rileva il Parlamento europeo che, nonostante l'ambito di applicazione della direttiva sui prodotti difettosi, «l'attuale quadro giuridico non sarebbe sufficiente a coprire i danni causati dalla nuova generazione di robot, in quanto questi possono essere dotati di capacità di adattamento e di apprendimento che implicano un certo grado di imprevedibilità nel loro comportamento, dato che imparerebbero in modo autonomo, in base alle esperienze diversificate di ciascuno, e interagirebbero con l'ambiente in modo unico e imprevedibile» [18].

Altre normative – alcune di carattere generale, altre più specifiche – che in qualche modo possono contribuire a regolamentare l'impiego di sistemi di IA sono la direttiva sulla sicurezza generale dei prodotti (2001/95/CE), la direttiva macchine (2006/42/CE), la direttiva apparecchiature radio (2014/53/UE), la direttiva sui dispositivi medici (93/42/CEE), la direttiva sulla sicurezza dei giocattoli (2009/48/CE), la direttiva sugli strumenti di misura (2014/32/UE) e la normativa sull'omologazione dei veicoli [19].

Va da subito sottolineato che la normativa europea in materia di sicurezza dei prodotti e di responsabilità per i prodotti difettosi è retta dal principio guida per cui, a prescindere dalla complessità della catena del valore, la responsabilità per la sicurezza e la difettosità del prodotto verso gli utilizzatori è posta a carico del produttore che immette il prodotto sul mercato.

Da ultimo, il Parlamento europeo ha pubblicato una Risoluzione recante raccomandazioni alla Commissione europea su un regime di responsabilità civile per l'IA (di seguito anche "Risoluzione del 2020"). Tale Risoluzione contiene lo schema di una correlata Proposta di

---

[17] Cfr. COMMISSIONE EUROPEA, COM(2018) 246 final, *cit.*, pt. 6; COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale*, cit., pp. 14 ss.; A. BERTOLINI, *Artificial Intelligence and Civil Liability*, cit., pp. 50 ss.; A. AMIDEI, *Intelligenza Artificiale*, cit., pp. 1723 ss.

[18] Cfr. PARLAMENTO EUROPEO, *Norme di diritto civile sulla robotica*, cit., «considerando» AI.

[19] Cfr. COMMISSIONE EUROPEA, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*, cit., pp. 4 ss.; A. BERTOLINI, *Artificial Intelligence and Civil Liability*, cit., pp. 47 ss., per un approfondimento. Sempre sulla normativa europea applicabile cfr., altresì, L. LIGUORI, in M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di Intelligenza Artificiale*, cit., pp. 341 ss.; A. SANTOSUOSSO, C. BOSCARATO, F. CAROLEO, *Robot e diritto: una prima ricognizione*, in *NGCC*, 2012, da p. 494.

regolamento sulla responsabilità per il funzionamento dei sistemi di IA (di seguito "Schema di proposta di regolamento") [20].

Al riguardo, la fonte normativa regolamentare è stata pensata al fine di porre in essere una piena armonizzazione mediante una normativa uniforme di principio, tale da favorire lo sviluppo di un mercato unico digitale [21]. Il regolamento dovrebbe peraltro coordinarsi ed armonizzarsi con le normative testé menzionate ed in particolare con le direttive sui danni da prodotti difettosi e sulla sicurezza dei prodotti (*ultra*, § 8) [22].

La Risoluzione del 2020 e lo Schema di proposta di regolamento si fondano su una serie di risoluzioni, documenti e studi promossi dalle istituzioni europee negli ultimi anni.

Un rapido cenno, infine, andrà fatto rispetto alla ancor più recente 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» ("AI Act" o "AIA") [23], predisposta dalla Commissione europea e che però si pone in parte al di fuori degli schemi tracciati dal Parlamento europeo.

La legislazione *in fieri* in tema di IA va poi inserita in un più ampio contesto di "costituzionalismo digitale" dell'Unione europea, in cui

---

[20] PARLAMENTO EUROPEO, *Regime di responsabilità civile per l'intelligenza artificiale. Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale*, (2020/2014(INL) (P9_TA-PROV(2020)0276) e relativo Allegato, contenente *Raccomandazioni dettagliate per l'elaborazione di un regolamento del Parlamento europeo e del Consiglio sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale*, nonché la *Proposta di regolamento del Parlamento europeo e del Consiglio sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale*.

[21] Cfr. PARLAMENTO EUROPEO, *Raccomandazioni dettagliate per l'elaborazione di un regolamento*, cit., principio n. 1.

[22] Questa raccomandazione è contestuale ad altri due risoluzioni del Parlamento europeo. Cfr. PARLAMENTO EUROPEO, *Relazione recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate* (2020/2012(INL)) (A9 – 0186/2020), 8 ottobre 2020, su cui si è basata la Proposta di regolamento della Commissione, di cui si accennerà *infra* nel § 8; PARLAMENTO EUROPEO, *Relazione sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale* (2020/2015(INI)) (A9- 0176/2020), che si propone di stabilire a chi appartenga la proprietà intellettuale di qualcosa sviluppato completamente dall'IA. Per un inquadramento sistematico più ampio, cfr. A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Milano, 2020, pur se antecedente alle citate proposte.

[23] COM(2021) 206 final, 21st April 2021.

oltre al GDPR, dovrebbero in futuro aggiungersi il *Data Governance Act*, il *Digital Markets Act* e il *Digital Services Act* [24].

L'indagine, allora, non può che partire dal testo della Risoluzione del 2017, per poi svilupparsi tramite l'analisi di alcuni dei principali documenti delle istituzioni europee che le hanno fatto seguito.

12.4. I principi guida su cui si fonda la Risoluzione del Parlamento europeo in tema di norme di diritto civile sulla robotica: prospettiva antropocentrica e fondata sui diritti e i valori fondamentali dell'UE

Nella Risoluzione del 2017, il Parlamento europeo afferma che la questione legata alla responsabilità civile per i danni causati dai robot «sia una questione fondamentale», da analizzare ed affrontare anche a livello di Unione europea «al fine di garantire il massimo livello di *efficienza*, *trasparenza* e coerenza nell'attuazione della *certezza giuridica* in tutta l'Unione europea nell'interesse tanto dei *cittadini* e dei *consumatori* quanto delle *imprese*» [25].

Già in questo punto della Risoluzione del 2017 sono individuabili almeno tre principi guida per la regolamentazione della responsabilità robotica: *efficienza*, *trasparenza* e *certezza giuridica*.

Altro profilo giuridicamente rilevante è il riferimento non solo ai *consumatori*, alla cui tutela è limitata la direttiva sui prodotti difettosi, ma anche ai *cittadini* e alle *imprese*.

– Quanto all'*efficienza*, i «considerando» E, F ed S della Risoluzione del 2017 tradiscono in qualche modo un'impostazione utilitaristica ma anche attenta a non tarpare la fisiologica *spinta* dell'UE verso

[24] L'espressione "costituzionalismo digitale" è di L. FLORIDI, *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, in *Phil. & Techn.*, 3 June 2021. Cfr. COMMISSIONE EUROPEA, *Proposal for a regulation of the European Parliament and the Council on European data governance (Data Governance Act)*, 25 November 2020, COM(2020) 767 final; COMMISSIONE EUROPEA, *Proposal for a regulation of the European Parliament and the Council on contestable and fair markets in the digital sector (Digital Markets Act)*, 15 December 2020, COM(2020) 842 final; COMMISSIONE EUROPEA, *Proposal for a regulation of the European Parliament and the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, 15 December 2020, COM(2020) 825 final. Cfr., altresì, COMMISSIONE EUROPEA, *Fostering a European Approach to Artificial Intelligence*, 21 April 2021, (COM(3032) 205 Final).

[25] Cfr. PARLAMENTO EUROPEO, *Norme di diritto civile sulla robotica*, cit., pt. 49 (enfasi aggiunte).

l'innovazione tecnologica, con benefici per i cittadini (tra cui in particolare gli anziani e i malati), per l'occupazione e la sicurezza lavorativa, per il settore dei trasporti, manifatturiero, commerciale ed agricolo.

– Quanto alla *trasparenza*, il punto 12 della Risoluzione del 2017, incardinato nell'ambito dei «Principi etici», ne esplica il significato nel senso che (*i*) «dovrebbe sempre essere *possibile indicare la logica alla base di ogni decisione presa con l'ausilio dell'intelligenza artificiale* che possa avere un impatto rilevante sulla vita di una o più persone»; (*ii*) «debba sempre essere possibile ricondurre i calcoli di un sistema di intelligenza artificiale a una *forma comprensibile per l'uomo*»; (*iii*) «i robot avanzati dovrebbero essere dotati di una *"scatola nera" che registri i dati* su ogni operazione effettuata dalla macchina, compresi i passaggi logici che hanno contribuito alle sue decisioni» [26].

Al riguardo è chiaro il riferimento alla problematica degli sviluppi imprevedibili dell'algoritmo e del *black box algorithm*.

– Per quanto concerne la *certezza giuridica*, infine, (*a*) il «considerando» L della Risoluzione del 2017 afferma che «occorre chiarire la responsabilità giuridica per quanto concerne sia il *modello di impresa* sia le caratteristiche dei lavoratori, in caso di emergenza o qualora sorgessero problemi»; (*b*) il «considerando» M sottolinea che «la tendenza all'automazione esige che *i soggetti coinvolti nello sviluppo e nella commercializzazione di applicazioni dell'intelligenza artificiale integrino gli aspetti relativi alla sicurezza e all'etica fin dal principio*, riconoscendo pertanto che devono essere preparati ad accettare di essere legalmente responsabili della qualità tecnologica prodotta»; (*c*) il «considerando» S osserva che l'industria europea potrebbe trarre beneficio da una regolamentazione a livello di UE «che fornisca *condizioni prevedibili e sufficientemente chiare in base alle quali le imprese possano sviluppare applicazioni e pianificare i propri modelli commerciali su scala europea*, garantendo nel contempo che *l'Unione e i suoi Stati membri mantengano il controllo sulle norme regolamentari da impostare* e non siano costretti ad adottare e subire norme stabilite da altri, vale a dire quei paesi terzi che sono anche in prima linea nello sviluppo della robotica e dell'intelligenza artificiale» [27].

Se ne deduce che la *certezza giuridica* concerne, da un lato, la distribuzione della responsabilità tra diverse categorie di soggetti interessati (produttori, distributori, utilizzatori ecc.) e, dall'altro, la possibilità di

[26] Enfasi aggiunte.

[27] Tutte enfasi aggiunte.

sperimentare, produrre e commercializzare nuove tecnologie in un ambiente normativo protetto e armonizzato.

Ancora, la *certezza giuridica* rileva di per sé come strumento di autonomia e di protezione – per cittadini, imprese e istituzioni europee e degli Stati membri – dai principali *players* mondiali in campo di robotica e IA, la maggior parte dei quali, per natura imprenditoriale o per forme di Stato e di governo, possono insidiare il fondamento democratico dell'evoluzione civile e sociale.

– Ad ogni modo, i principi di *efficienza*, *trasparenza* e *certezza giuridica* sembrano disvelare il fondamento originario di comunità economica, ancor prima che di unione sociale, dell'Unione europea.

Ciò nondimeno si crede opportuno precisare da subito che, in una scala di valori – e in una prospettiva *unionale*, anziché comunitaria –, detti principi, seppure maggiormente prossimi alle problematiche segnalate, non debbano essere posti al vertice della regolamentazione in tema di responsabilità civile sulla robotica.

Al riguardo, proprio dall'analisi della stessa Risoluzione del 2017 si evince che (*i*) il «considerando» O pone attenzione a che «gli sviluppi nel campo della robotica e dell'intelligenza artificiale possono e dovrebbero essere pensati in modo da preservare la *dignità*, *l'autonomia e l'autodeterminazione degli individui*»; (*ii*) il punto 3 sottolinea che «lo sviluppo della tecnologia robotica dovrebbe mirare a *integrare le capacità umane e non a sostituirle*», così che «sia fondamentale, nello sviluppo della robotica e dell'intelligenza artificiale, garantire che *gli uomini mantengano in qualsiasi momento il controllo sulle macchine intelligenti*»; (*iii*) il punto 13, anch'esso incardinato nei «Principi etici», precisa che il quadro etico di orientamento dovrebbe essere basato, in primo luogo, sulle cc.dd. "leggi di Asimov", ossia sui «principi di beneficienza, non maleficenza, autonomia e giustizia» nonché, in secondo luogo e soprattutto, «sui *principi sanciti all'art. 2 del trattato sull'Unione europea* e nella *Carta dei diritti fondamentali dell'Unione europea* – quali la *dignità umana*, l'*uguaglianza*, la *giustizia* e l'*equità*, la *non discriminazione*, il consenso informato, la vita privata e familiare e la protezione dei dati, così come sugli *altri principi e valori alla base del diritto dell'Unione* come la *non stigmatizzazione*, la trasparenza, l'*autonomia*, la *responsabilità individuale e sociale* – e sulle *pratiche e i codici etici esistenti*» [28].

[28] Tutte enfasi aggiunte. E cfr. ora, COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale*, cit., p. 2, pp. 10 ss.

Al riguardo, il riferimento alle "leggi di Asimov" può far sorridere, trovandosi agevolmente i principi ivi contenuti nei principi fondamentali di tutti gli ordinamenti giuridici evoluti [29].

Gli altri riferimenti citati consentono invece di anticipare sin d'ora che l'ordinamento giuridico dell'Unione europea si caratterizza proprio per la sua *prospettiva antropocentrica* della regolamentazione sull'IA, attenta prima di tutto a tutelare *i diritti ed i valori fondamentali*, su cui si costruisce l'Unione e che accomunano gli Stati membri, nonché a delimitare l'IA quale *strumento d'integrazione* delle capacità umane – tra cui la capacità di autodeterminazione – e *mai di sostituzione* delle stesse.

Si anticipa altresì che l'esplicito riferimento alla Carta dei diritti fondamentali dell'Unione europea e agli «altri principi e valori alla base del diritto dell'Unione» è rilevante per orientare un'interpretazione ampia dell'impostazione appena delineata.

12.5. Il rischio "etico" del dominio dell'IA sull'essere umano. L'approccio procedimentale delle linee guida etiche dell'HLEG

Si è accennato in apertura al rischio di parificare in qualche modo esseri umani e sistemi di IA nonché di comprimere eccessivamente gli affari e le attività umane se non addirittura l'essenza degli esseri umani.

Concentrandosi su un'impresa organizzata in forma societaria, basti pensare alle difficoltà che possono incontrare gli amministratori di una società che adoperi un sistema di IA per ricevere una consulenza in merito ad una "scelta" d'impresa decisiva: in tale ipotesi gli amministratori "consenzienti" potrebbero appiattirsi rispetto all'*output* del sistema, confidando in un'alta aspettativa di *accuracy*; d'altro canto, gli amministratori "dissenzienti" incontrerebbero notevoli difficoltà nel motivare in maniera dialettica le ragioni della loro differente opinione.

Va pertanto accolta con favore la conferma della Commissione europea verso il sostegno a un approccio antropocentrico nei confronti

[29] Sulle tre "leggi di Asimov" cfr. M. BASSINI, in M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di Intelligenza Artificiale*, cit., pp. 339 s.; G. LEMME, *Gli* smart contracts *e le tre leggi della robotica*, in *AGE*, 1/2019, da p. 19; D. ETZERI, *Liability for operation and damages caused by artificial intelligence – with a short outlook to online games*, in 153 *Studia Iuridica Auctoritate Universitatis Pecs Publicata* (2015), da p. 57.

dell'IA. Al riguardo, detta istituzione ha precisato che la *fiducia* verso l'IA costituisce una condizione indispensabile: in particolare «l'intelligenza artificiale non è fine a se stessa, ma *è uno strumento a servizio delle persone* che ha come fine ultimo quello di migliorare il benessere degli esseri umani» [30].

La strumentalità dell'IA all'uomo aiuta a porre quest'ultima altresì in una prospettiva funzionale al rispetto della dignità umana, anche quale capacità autodeterminazione dell'individuo [31].

La questione sconfina nell'etica e proprio le recenti *Ethic Guidelines for Trustworthy AI* pubblicate dall'*Independent High-Level Expert Group on Artificial Intelligence* (HLEG) forniscono preziosi spunti per una corretta soluzione dei problemi enunciati [32].

Segnatamente le menzionate linee-guida declinano i requisiti del *rispetto dell'autonomia umana*; della *fairness*; dell'*explicability*; dell'*intervento e* della *sorveglianza umani*; della *robustezza*; della *riservatezza* e della *governance dei dati*; della *diversità, non discriminazione* ed *equità*; del *benessere sociale e ambientale*.

Per ciò che qui interessa, riguardo al primo requisito, secondo l'HLEG i sistemi di IA non dovrebbero subordinare, forzare, sviare, manipolare, condizionare gli esseri umani in maniera ingiustificabile. Al contrario tali sistemi dovrebbero *aumentare, completare e rafforzare* le capacità cognitive, sociali e culturali degli esseri umani [33].

Il requisito della *fairness* (tradotto con l'espressione «equità»), (*i*) nell'accezione *sostanziale* si esplica nell'impegno a garantire una distribuzione giusta ed equa di costi e di benefici, in ossequio al principio di proporzionalità, nonché a garantire che sia gli individui sia i gruppi

---

[30] Cfr. COMMISSIONE EUROPEA, *Creare fiducia nell'intelligenza artificiale antropocentrica*, COM(2019) 168 final, Bruxelles, 8 aprile 2019, p. 2 (enfasi aggiunta).

[31] Cfr. R. MESSINETTI, *La tutela della persona umana* versus *l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contr. impr.*, 2019, da p. 861, pp. 868 s., secondo cui «Garantire che l'uomo possa comprendere la macchina persegue infatti una palese finalità: assicurare che l'intelligenza artificiale sia – e rimanga – strumentale rispetto a quella umana. Ciò attiene al nucleo essenziale del concetto filosofico e del principio giuridico della dignità dell'uomo». Sia consentito, inoltre, il rinvio a F. PACILEO, *L'uomo al centro. IA tra etica e diritto nella responsabilità d'impresa*, in *Etica digitale. Verità, responsabilità e fiducia nell'era delle macchine intelligenti*, a cura di M. Bertolaso, G. Lo Storto, Roma, 2021, da p. 83.

[32] Cfr. HLEG, *Ethics Guidelines for Trustworthy AI*, Brussels, 8 aprile 2019, reperibile sul sito *www.europa.eu*.

[33] Cfr. HLEG, *op. cit.*, p. 12, p. 16.

non patiscano distorsioni inique, discriminazioni e stigmatizzazioni; (*ii*) nella sua versione *procedurale*, attiene alla capacità di contestare, di cercare una soluzione effettiva contro, gli *output* prodotti da sistemi di IA: a tal fine, il relativo processo decisionale dovrebbe essere esplicabile. Il contesto di riferimento della *fairness sostanziale* è evidentemente quello già menzionato della *trasparenza*, incardinato nei principi etici [34].

E proprio nel comune senso della trasparenza, il requisito dell'*explicability* prevede che i processi decisionali (*rectius*, di funzionamento dell'IA) dovrebbero essere trasparenti, che le capacità e le funzioni dei sistemi di IA dovrebbero essere apertamente comunicate, ed infine che gli *output* siano il più possibile esplicitabili e comprensibili per coloro che vengono coinvolti, in modo che una decisione possa essere debitamente contestata. In particolare, nel caso dei *black box algorithm* si potrebbero richiedere altre misure di *explicability*, quali ad esempio la tracciabilità, la controllabilità, la verificabilità e la trasparenza nelle comunicazioni sui sistemi nel senso di assicurare che detti sistemi rispettino nel complesso i diritti fondamentali [35].

Le linee-guida hanno poi ben presente il potenziale *trade-off* tra *explicability* e *accuracy* e cercano di risolverlo nel senso che la prima può essere sacrificata a favore della seconda nella misura in cui i conseguenti benefici prevalgano sui singoli prevedibili rischi [36].

Inoltre, l'IA deve essere *robusta* nel senso che gli algoritmi debbono essere idonei a far fronte a errori o incongruenze durante tutte le fasi del ciclo di vita del sistema di IA. Detti algoritmi devono essere altresì capaci di gestire risultati sbagliati ed essere resilienti agli attacchi palesi e occulti tesi alla manipolazione dei dati o degli algoritmi. Deve essere infine garantita l'esistenza di un piano di emergenza. Gli *output*,

---

[34] Cfr. HLEG, *op. cit.*, pp. 12 s. Cfr., altresì, KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YUT, *Accountable Algorithms*, cit., p. 642 e p. 685, ove si distingue tra *individual fairness* e *group fairness* e inoltre si aggiunge che «a fair process will give similar participants a similar probability of receiving each possible outcome».

[35] Cfr. HLEG, *op. cit.*, p. 13; COMMISSIONE EUROPEA, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*, cit., p. 10, secondo cui «Non è necessario che gli esseri umani comprendano ogni singola fase del processo decisionale, ma dato che gli algoritmi di intelligenza artificiale sono sempre più avanzati e sono utilizzati in settori critici, è fondamentale che gli esseri umani possano capire come il sistema ha preso le decisioni algoritmiche».

[36] Cfr. HLEG, *op. cit.*, p. 17.

poi, devono essere accurati, o almeno rispecchiare correttamente il loro livello di accuratezza, e i risultati devono essere riproducibili [37].

I sistemi di IA dovrebbero inoltre contenere meccanismi di *sicurezza fin dalla progettazione* (*by design*), per garantire che siano sicuri in modo verificabile in ogni fase. Ciò comprende anche la possibilità di ridurre al minimo e, ove possibile, rendere reversibili gli effetti involontari o gli errori del funzionamento del sistema. È opportuno, pertanto, prevedere processi in grado di chiarire e valutare i potenziali rischi associati all'uso dei sistemi di IA nei vari settori di applicazione [38].

Strettamente interconnessa a tutti questi requisiti è poi la *sorveglianza umana sin dalla progettazione*.

Secondo la Commissione europea a tale requisito può essere rispettato organizzando meccanismi di *governance* secondo tre possibili approcci: (*a*) con intervento umano ["*human-in-the-loop*" (HITL)], che contempla l'intervento umano in ogni ciclo decisionale del sistema, anche se la Commissione stessa avverte che ciò «in molti casi non è né possibile né auspicabile»; (*b*) con supervisione umana [("h*uman-on-the-loop*" (HOTL)], che implica la capacità di intervento umano durante il ciclo di progettazione del sistema e di monitoraggio del funzionamento del sistema; (*c*) con controllo umano [("*human-in-command*" (HIC)], che include sia la capacità di sorvegliare l'attività complessiva del sistema di IA (tra cui il più ampio impatto economico, sociale, giuridico ed etico) sia la capacità di decidere quando e come utilizzare il sistema in una particolare situazione [39].

Anche per ciò che concerne *la riservatezza e la governance dei dati* le Linee-guida e la Commissione delineano un procedimento per la raccolta e l'elaborazione dei *big data* e per gestire il rischio di discriminazioni. In particolare, la Commissione osserva che deve essere garantita l'integrità dei dati. A tal fine, i processi e i set di dati utilizzati devono essere testati e documentati in ogni fase, ed in particolare nella pianificazione, nell'addestramento, nei test e nella diffusione. Ciò dovrebbe valere altresì per i sistemi di IA che non sono stati sviluppati *in house* ma acquisiti altrove [40].

---

[37] Cfr. HLEG, *op. cit.*, pp. 16 s.; COMMISSIONE EUROPEA, *Creare fiducia nell'intelligenza artificiale antropocentrica*, cit., p. 5.

[38] Cfr. HLEG, *op. cit.*, pp. 16 s.; COMMISSIONE EUROPEA, *Creare fiducia nell'intelligenza artificiale antropocentrica*, cit., p. 5.

[39] Cfr. COMMISSIONE EUROPEA, *Creare fiducia nell'intelligenza artificiale antropocentrica*, cit., p. 5, testo e nt. 13; HLEG, *op. cit.*, p. 16.

[40] Cfr. HLEG, *op. cit.*, p. 17; COMMISSIONE EUROPEA, *Creare fiducia nell'intelligenza artificiale*

La *fairness*, la *sorveglianza umana* e la *riservatezza e governance dei dati*, infine, si coordinano per *evitare discriminazioni e disparità di trattamento*, dovute all'internalizzazione, anche involontaria, di pregiudizi all'interno degli algoritmi e dei sistemi di IA [41].

Ad una visione d'insieme, le menzionate Linee-guida si pongono in una prospettiva che appare coerente ad un'impostazione di ordine *procedimentale*, impostazione, si anticipa, che potrebbe risultare quale migliore soluzione per la regolamentazione e gestione dei rapporti tra innovazione tecnologica e diritto dell'impresa organizzata in forma societaria.

Più in generale, l'opzione del legislatore verso la trasparenza e la sicurezza degli algoritmi *fin dalla progettazione* implica una scelta diversa rispetto alla *neutralità tecnologica* (dal punto di vista del programmatore e del produttore nonché dello stesso sistema di AI), scelta che certamente richiede una seria riflessione circa i conseguenti possibili costi e benefici.

12.5.1. Necessità di un'organizzazione e di professionalità. Probabile impiego del metodo economico. Ergo, importanza dell'impresa

E proprio la complessità applicativa di dette Linee-guida e il loro approccio procedimentale implicano un'*organizzazione*, poi un'organizzazione *adeguata*.

Ne deriva che, lasciando da parte i soggetti di natura pubblicistica tra coloro che in qualche modo hanno a che fare con l'IA, i soggetti privati devono avere un'organizzazione che difficilmente può essere sostenuta da un metodo diverso da quello del rispetto del principio di *economicità*.

Ecco allora che, non potendo mancare il requisito della *professionalità*, la maggior parte dei soggetti privati che operano con l'IA saranno organizzati in forma di *impresa*.

Ciò posto, occorre distinguere tra imprese che *producono* sistemi di IA e imprese che *utilizzano* tali sistemi per effettuare "scelte" imprenditoriali strategiche e suscettibili di incidere su diritti fondamentali di soggetti che per varie ragioni vi si rapportano. Si pensi, per

antropocentrica, cit., pp. 5 s.

[41] Cfr. HLEG, *op. cit.*, pp. 18 s.

semplificare, da un lato a una start-up innovativa che produce ovvero offre al mercato un certo sistema di IA e, dall'altro, a una s.p.a. che utilizzi detto sistema per ottenere informazioni decisive, se non una vera propria consulenza, in merito a una scelta strategica (es., investire o non in una operazione complessa oppure liquidare o meno la società).

Al riguardo, in considerazione dell'orizzonte limitato di controllo sui sistemi di IA, di cui si è detto, occorre comprendere come possa distribuirsi una responsabilità per un suo cattivo funzionamento nell'ambito di una così complessa catena di valore.

12.6. Il Libro bianco sull'intelligenza artificiale e l'approccio basato sul rischio

Ulteriori spunti sul tema della responsabilità da funzionamento dei sistemi di IA si ricavano dal Libro bianco sull'intelligenza artificiale [42].

In tale documento la Commissione europea riprende il percorso istituzionale finora descritto, in merito alla regolamentazione dell'IA.

Limitatamente a ciò che qui interessa, si afferma che le maggiori lacune normative si riscontrano sul tema della trasparenza, della tracciabilità e della sorveglianza umana, nonché sulla difficoltà di distinguere le responsabilità del produttore, dell'utilizzatore per i danni derivanti dalla programmazione o dall'apprendimento/uso dell'algoritmo.

Viene inoltre promosso *un approccio basato sul rischio* nel duplice significato di (*i*) prevedere una regolamentazione più stringente nei settori con rischi significativi o laddove siano gli stessi sistemi di IA a generare rischi significativi; (*ii*) distribuire la responsabilità agli operatori che si trovano nella posizione migliore per affrontare i rischi potenziali.

Riguardo al primo profilo, si può innanzi tutto segnalare la difficoltà di individuare criteri oggettivi di distinzione fra situazioni a rischio significativo e situazioni meno rischiose [43], rinviando poi allo

[42] Cfr. COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale*, cit.

[43] Su tale distinzione cfr. EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES, *Liability for Artificial Intelligence and Other Emerging Digital Technologies*, commissionato dalla Commissione europea, 2019, pp. 39 ss.; critico verso i suddetti criteri di distinzione A. BERTOLINI, *Artificial Intelligence and Civil Liability*, cit., pp. 77 ss.

Schema di proposta di regolamento e alla Proposta di regolamento (*ultra*, §§ 8 e 9).

Riguardo al secondo, si rinvia a quanto si dirà nei prossimi paragrafi (*ultra*, §§ 7 e 8).

12.7. Principali raccomandazioni della Risoluzione del 2017 del Parlamento europeo, riguardo allo specifico tema della responsabilità civile sulla robotica

Quanto alle principali raccomandazioni fornite dalla Risoluzione del 2017 alla Commissione europea *stricto sensu* riferite alla responsabilità civile sulla robotica (punti 49-59), fissati i principi fondamentali di riferimento (*supra*, § 4), vale la pena di evidenziare i principali profili che emergono dalla lettura della Risoluzione del 2017.

– Così, il punto 50 fa riferimento alla necessità di «una maggiore comprensione per trovare il terreno comune necessario ai fini dell'*attività congiunta umano-robotica* e che dovrebbe basarsi su due relazioni interdipendenti essenziali, quali la *prevedibilità* e la *direzionalità*». Sempre il punto 50 precisa che «queste due relazioni interdipendenti sono cruciali per determinare quali informazioni è opportuno che gli umani e i robot condividano e come individuare una base comune tra umani e robot che consenta un'efficace *azione congiunta umano-robotica*» [44]. L'esplicito riferimento all'*attività/azione congiunta umano-robotica* appare ispirato alla dottrina che, si crede, ad oggi ha fornito alcuni tra gli spunti più interessanti in materia di responsabilità civile sulla robotica [45]. Detta raccomandazione si colloca evidentemente nel solco del principio della *sorveglianza umana* (*supra*, § 5).

– Ancora la Risoluzione del 2017 raccomanda al punto 52 che la responsabilità civile «per danni causati dai robot diversi dai danni alle cose», non dovrebbe limitare (*i*) il tipo e l'entità dei danni risarcibili; (*ii*) le forme di risarcimento che potrebbero essere offerte alla parte lesa «per il semplice fatto che il danno è provocato da un soggetto non umano».

In buona sostanza tale previsione suggerisce di porre al riparo la parte lesa da eventuali lacune normative che non permettano di individuare in modo chiaro il soggetto responsabile e la ripartizione delle

[44] Enfasi aggiunte.

[45] Il riferimento è a G. TEUBNER, *Digitale Rechtssubjekte?*, cit.

responsabilità. Qui il riferimento va al summenzionato principio di *certezza giuridica* (*supra*, § 4).

– Il Parlamento europeo circoscrive la futura regolamentazione della responsabilità *de qua* all'approccio della «responsabilità oggettiva» o a quello della «gestione dei rischi» (punto 53), osservando al riguardo che (*a*) «la responsabilità oggettiva richiede una semplice prova del danno avvenuto e l'individuazione di un nesso di causalità tra il funzionamento lesivo dei robot e il danno subito dalla parte lesa» (punto 54); (*b*) «l'approccio di gestione dei rischi non si concentra sulla persona "che ha agito con negligenza" in quanto responsabile a livello individuale bensì sulla persona che, in determinate circostanze, è in grado di minimizzare i rischi e affrontare l'impatto negativo» (punto 55).

L'approccio di gestione dei rischi (*risk management approach* o RMA) è stato rielaborato dalla Commissione nel Libro bianco, ove si precisa che «in un futuro quadro normativo ciascun obbligo debba essere stabilito a carico dell'operatore o degli operatori che si trovano nella posizione migliore per affrontare eventuali rischi potenziali».

– Soprattutto il RMA impone la distinzione fra (*a*) una responsabilità connessa alle «competenze derivanti dalla "formazione" di un robot» e (*b*) una responsabilità invece connessa alle «competenze che dipendono strettamente dalle sue [del robot, n.d.r.] abilità di apprendimento» (punto 56).

Al riguardo, se nell'ambito della formazione si possono individuare profili di negligenza o di minimizzazione dei rischi da parte dei programmatori, sembra invece più arduo delineare una correlazione fra una condotta quanto meno colposa e le «abilità di apprendimento» del robot. Qui il problema è ancora una volta quello degli sviluppi imprevedibili dell'algoritmo, del *black box algorithm* unitamente a quello della certezza giuridica.

In ogni caso, sempre nel medesimo paragrafo il Parlamento europeo precisa che «una volta individuati i soggetti responsabili in ultima istanza, la loro responsabilità dovrebbe essere *proporzionale* all'effettivo livello di istruzioni impartite ai robot e al grado di autonomia di quest'ultimo, di modo che quanto maggiore è la capacità di apprendimento o l'autonomia di un robot e quanto maggiore è la durata della formazione di un robot, tanto maggiore dovrebbe essere la responsabilità del suo formatore» [46].

[46] Enfasi aggiunta.

Su questo aspetto, soprattutto per i sistemi di IA e/o robotici che sono il frutto di una catena complessa di valore, è difficile individuare colui che si trova nella posizione migliore per gestire i rischi potenziali. A tal proposito, la Commissione europea promuove il principio della "responsabilità condivisa". In buona sostanza occorrono disposizioni normative esplicite che impongano la cooperazione tra gli operatori economici nella catena di approvvigionamento e gli utilizzatori, al fine di creare certezza giuridica, anche in termini di *accountability*. In base a tale principio ogni partecipante alla catena di valore avente un impatto sulla sicurezza del prodotto (ad esempio i produttori di *software*) e sugli utilizzatori (ad esempio, se modificano il prodotto) dovrebbe assumersi la propria responsabilità e fornire al partecipante successivo nella catena le informazioni e le misure necessarie [47].

– Il Parlamento europeo osserva che, *de iure condito* e allo stato dell'arte, «la responsabilità deve essere imputata ad un essere umano e non a un robot» (punto 56).

Tale assunto dovrebbe essere scontato ma, alla luce della possibilità di attribuire *de iure condendo* una responsabilità ai robot più autonomi, è bene tenere fermo questo punto di partenza d'indagine.

12.8. La Risoluzione del Parlamento europeo sul regime di responsabilità civile per l'intelligenza artificiale e l'allegato Schema di proposta di regolamento

Si è accennato precedentemente alla Risoluzione del 2020 del Parlamento europeo e all'allegato Schema di proposta di regolamento (*supra*, §§ 2 e 3).

– Al riguardo, il Parlamento europeo innanzi tutto sembra escludere l'ipotesi della "personalità elettronica", dallo stesso formulata, nonché sottolineare la strumentalità dei sistemi di IA all'uomo. Il «considerando» n. 6 dello Schema di proposta di regolamento prevede infatti che «Qualsiasi cambiamento richiesto riguardante il quadro giuridico esistente dovrebbe iniziare con il chiarimento che i *sistemi di IA*

[47] Cfr. COMMISSIONE EUROPEA, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*, cit., pp. 12 s. Cfr., altresì, G. COMANDÉ, *Intelligenza artificiale e responsabilità tra* liability *e* accountability. *Il carattere trasformativo dell'IA e il problema della responsabilità*, in *AGE*, 1/2019, da p. 169.

non possiedono né una personalità giuridica né una coscienza umana e che *il loro unico compito consiste nel servire l'umanità*» [48].

È questo un punto di riferimento davvero importante per uno studio sulle implicazioni giuridiche dell'impiego dei sistemi di IA.

– L'art. 3 dello Schema di proposta di regolamento *definisce* poi (*i*) *il sistema di IA* come «un sistema basato su software o integrato in dispositivi hardware che mostra un comportamento che simula l'intelligenza, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici»; (*ii*) *il sistema di IA "autonomo"* come quello che «che opera interpretando determinati dati forniti e utilizzando una serie di istruzioni predeterminate, senza essere limitato a tali istruzioni, nonostante il comportamento del sistema sia legato e volto al conseguimento dell'obiettivo impartito e ad altre scelte operate dallo sviluppatore in sede di progettazione».

Ad una prima lettura, colpisce subito la puntualizzazione circa il comportamento del sistema autonomo di IA comunque connesso al perseguimento di *obiettivi ed interessi di un soggetto, altro*, nonché alle *scelte operate dallo sviluppatore in sede di progettazione*. Ciò evidenzia la descritta prospettiva antropocentrica. E vale la pena di anticipare che, significativamente, l'art. 3 della proposta di AIA, sempre nel definire un "sistema di intelligenza artificiale", fa riferimento a «una determinata serie di obiettivi *definiti dall'uomo*» [49].

– Lo Schema di proposta di regolamento pone anch'esso attenzione alla distinzione tra *i diversi soggetti che compongono la catena di valore dei sistemi di IA* – produttore, operatori, persone interessate e qualsiasi terzo coinvolto [50] – e dà seguito alla condivisione delle responsabilità di tali soggetti, promossa nel Libro bianco, secondo il criterio del RMA.

In particolare, sempre nell'ambito delle definizioni di cui all'art. 3, si distingue (*a*) la nozione di "operatore di front-end", quale «persona fisica o giuridica *che esercita un certo grado di controllo su un rischio connesso* all'operatività e al funzionamento del sistema di IA e che *beneficia* del suo funzionamento»; (*b*) la nozione di "operatore di back-end",

[48] Enfasi aggiunta.

[49] Enfasi aggiunta.

[50] Cfr. PARLAMENTO EUROPEO, *Raccomandazioni dettagliate per l'elaborazione di un regolamento*, cit., principio n. 2; nonché l'art. 3 dello Schema di proposta di regolamento, ove si definisce "persona interessata" «qualsiasi persona che subisca i danni o pregiudizi causati da un'attività, dispositivo o processo fisico o virtuale guidato da un sistema di IA e che non sia l'operatore di tale sistema».

quale «persona fisica o giuridica che, su base continuativa, *definisce le caratteristiche della tecnologia e fornisce i dati e il servizio di supporto* di back-end essenziale e pertanto *esercita anche un elevato grado di controllo su un rischio connesso* all'operatività e al funzionamento del sistema di IA» [51].

Entrambe le fattispecie di "operatore" sono accomunate dall'"esercizio" di un «controllo su un rischio connesso all'operatività e al funzionamento del sistema di IA»: un «certo grado di controllo» per l'operatore di front-end e un «elevato grado di controllo» per l'operatore di back-end.

E sempre l'art. 3 definisce il "controllo" come «qualsiasi *azione di un operatore* che *influenza* il funzionamento di un sistema di IA e quindi *il grado in cui l'operatore espone terzi ai potenziali rischi associati all'operatività e al funzionamento del sistema di IA*; tali azioni possono avere un impatto sul funzionamento *in qualsiasi fase* determinando gli input, gli output o i risultati, o possono modificare funzioni o processi specifici all'interno del sistema di IA; *il grado* in cui tali aspetti del funzionamento del sistema di IA sono determinati dall'azione *dipende dalla misura in cui l'operatore può influenzare il rischio* connesso all'operatività e al funzionamento del sistema di IA» [52].

In particolare, il «considerando» n. 10 dello Schema di proposta di regolamento puntualizza che «Maggiore è il grado di sofisticazione e di autonomia di un sistema, maggiore sarà l'impatto dato dal fatto di definire e influenzare gli algoritmi, ad esempio attraverso continui aggiornamenti».

Già da questa prima analisi del testo emerge subito una stretta correlazione – una sorta di "spina dorsale" della normativa *in fieri* – tra *operatori-controllo-grado di rischio*.

– Il Capo IV dello Schema di proposta di regolamento (artt. 10 ss.) disciplina poi la *ripartizione delle responsabilità* dei soggetti facenti parte della catena di valore, secondo il criterio della *solidarietà* tra gli operatori ma anche di un *regresso proporzionale* al grado di controllo sul rischio.

Ancora nell'ambito della responsabilità condivisa, qualora non sia possibile o sia eccessivamente oneroso individuare il singolo soggetto

---

[51] Enfasi aggiunte. Per un approfondimento sulla nozione di "operatore", cfr. EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES, *Liability for Artificial Intelligence*, cit., pp. 39 ss.

[52] Enfasi aggiunte.

responsabile, al punto n. 7 della Risoluzione del 2020 si osserva che «è tuttavia possibile aggirare tale ostacolo considerando responsabili le varie persone nella catena del valore che creano il sistema di IA, ne eseguono la manutenzione o ne controllano i rischi associati».

L'impostazione dello Schema di proposta di regolamento appare paragonabile a quella adottata nella direttiva sulla responsabilità per danno da prodotti difettosi. Tale ultima direttiva, peraltro è più volte presa in considerazione dal Parlamento europeo (unitamente alla direttiva sulla sicurezza generale dei prodotti), che suggerisce anche di aggiornarla all'evoluzione delle tecnologie digitali e di armonizzarla con il regolamento *in fieri*. In particolare, il ruolo dell'*operatore* (*rectius*, degli operatori) quale soggetto *accountable* è comparabile a quello del *produttore* nell'ambito delle direttive sui danni da prodotti difettosi e sulla sicurezza dei prodotti [53].

– In ossequio al RMA vengono delineate distinte *fattispecie di sistemi di IA*, a cui poi si dovrebbero applicare distinte discipline di responsabilità: occorre invero individuare se il *sistema di IA* sia *"ad alto rischio" o meno*.

Sempre l'art. 3 dell Schema di proposta di regolamento definisce "ad alto rischio" «un potenziale significativo in un sistema di IA che opera in modo autonomo di causare danni o pregiudizi a una o più persone in modo casuale e che va oltre quanto ci si possa ragionevolmente aspettare; l'importanza del potenziale dipende dall'interazione tra la gravità dei possibili danni o pregiudizi, dal grado di autonomia decisionale, dalla probabilità che il rischio si concretizzi e dalla modalità e dal contesto di utilizzo del sistema di IA».

---

[53] Cfr. PARLAMENTO EUROPEO, *Regime di responsabilità civile per l'intelligenza artificiale*, cit., «considerando» n. 8, ove (*i*) si esorta la Commissione europea «a valutare se la direttiva sulla responsabilità per danno da prodotti difettosi debba essere trasformata in un regolamento, a chiarire la definizione di "prodotti" determinando se i contenuti e i servizi digitali rientrino nel suo ambito di applicazione, nonché a esaminare l'adeguamento di concetti quali "pregiudizio", "difetto" e "produttore"»; (*ii*) si esprime il parere «che, ai fini della certezza giuridica nell'intera Unione, in seguito alla revisione della direttiva sulla responsabilità per danno da prodotti difettosi, il concetto di "produttore" dovrebbe includere i produttori, gli sviluppatori, i programmatori, i prestatori di servizi e gli operatori di back-end». Cfr., altresì, COMMISSIONE EUROPEA, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*, cit., pp. 17 s.; EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES, *Liability for Artificial Intelligence*, cit., pp. 55, circa la responsabilità solidale della *commercial or technological unit*.

Riguardo all'*importanza del potenziale di danni e pregiudizi*, il «considerando» n. 13 della medesimo Schema precisa i criteri con cui può individuarsi (*a*) il *livello di gravità dei danni o pregiudizi*, i cui fattori rilevanti sono «l'entità del danno potenziale derivante dal funzionamento sulle persone interessate, inclusi in particolare gli effetti sui diritti fondamentali, il numero di persone interessate, il valore totale del danno potenziale e il pregiudizio inflitto alla società nel suo insieme»; (*b*) *la probabilità che il danno o il pregiudizio si verifichi*, i cui fattori rilevanti sono «il ruolo dei calcoli algoritmici nel processo decisionale, la complessità della decisione e la reversibilità degli effetti; (*c*) *la modalità di utilizzo*, i cui fattori rilevanti sono «il contesto e il settore in cui opera il sistema di IA, eventuali effetti giuridici o reali su diritti importanti della persona interessata tutelati dalla legge e l'eventuale e ragionevole possibilità di evitare gli effetti».

Ad ogni modo, l'art. 4.2 dello Schema di proposta di regolamento prevede un *elenco* dei sistemi di IA "ad alto rischio" e dei settori fondamentali in cui essi vengono utilizzati. Si conferisce inoltre alla Commissione europea il potere di *aggiornare* l'elenco, anche a cadenza periodica, (*i*) inserendo nuovi tipi di sistemi di IA "ad alto rischio" e settori fondamentali in cui vengono utilizzati; (*ii*) eliminando tipi di sistemi di IA non più qualificabili "ad alto rischio"; (*iii*) modificando i settori fondamentali per i sistemi di IA "ad alto rischio" esistenti.

– Orbene, riguardo alla *disciplina della responsabilità*, per i sistemi di IA "ad alto rischio" lo Schema di proposta di regolamento prevede la *responsabilità oggettiva* dell'operatore in controllo (art. 4), laddove per gli altri sistemi di IA è prevista invece la *responsabilità* per colpa, *aggravata* dall'inversione dell'onere probatorio (art. 8).

In ogni caso, l'approccio è legato all'immissione di un *rischio* nel mercato e/o tra il pubblico ed alla capacità o meno di controllarlo [54].

Riguardo alla responsabilità oggettiva è individuato il limite della *forza maggiore* (art. 10.3).

Per quanto concerne la responsabilità aggravata, invece, l'*inversione dell'onere probatorio* impone all'operatore di dimostrare (*a*) che il

[54] Cfr. il «considerando» n. 8 dello Schema di proposta di regolamento, ove si legge che «chiunque crei un sistema di IA, ne esegua la manutenzione, lo controlli o interferisca con esso dovrebbe essere chiamato a rispondere del danno o pregiudizio che l'attività, il dispositivo o il processo provoca. Ciò discende da concetti di giustizia generali e ampiamente accettati in materia di responsabilità, secondo i quali la persona che crea o mantiene un rischio per il pubblico è responsabile se il rischio causa un danno o un pregiudizio e pertanto dovrebbe minimizzarlo ex ante o risarcirlo ex post».

sistema di IA si è attivato senza che egli ne fosse a conoscenza e sono state adottate tutte le misure ragionevoli e necessarie per evitare tale attivazione al di fuori del suo controllo, o (*b*) che è stata rispettata la dovuta diligenza, o (*c*) la forza maggiore (art. 8.2).

Segnatamente, l'*obbligo di diligenza* è connesso (*i*) alla selezione di un sistema di IA idoneo al compito e alle competenze; (*ii*) alla debita messa in funzione del sistema di IA; (*iii*) al monitoraggio delle attività e al mantenimento dell'affidabilità operativa mediante la periodica installazione di tutti gli aggiornamenti disponibili.

Nel «considerando» n. 18 dello Schema di proposta di regolamento, poi, si aggiunge che «La diligenza che ci si può attendere da un operatore dovrebbe essere commisurata i) alla natura del sistema di IA, ii) al diritto giuridicamente tutelato potenzialmente interessato, iii) al danno o pregiudizio potenziale che il sistema di IA potrebbe causare e iv) alla probabilità di tale danno».

Il medesimo «considerando» contiene due criteri *presuntivi*, rispettivamente afferenti (*a*) la *diligenza* richiesta *durante il funzionamento* del sistema di IA, la cui sussistenza si dovrebbe presumere «laddove l'operatore possa dimostrare di avere effettivamente e regolarmente monitorato il sistema di IA durante il funzionamento e di avere notificato al costruttore le possibili irregolarità riscontrate nel corso del funzionamento»; (*b*) la *diligenza* richiesta riguardo al *mantenimento dell'affidabilità operativa* del sistema di IA, la cui sussistenza si dovrebbe presumere «laddove [l'operatore, n.d.a.] abbia installato tutti gli aggiornamenti disponibili forniti dal produttore del sistema di IA».

Sempre il «considerando» n. 18 puntualizza che «Poiché il livello di sofisticazione degli operatori può variare a seconda che si tratti di semplici consumatori o professionisti, è opportuno adeguare di conseguenza gli obblighi di diligenza».

Tornando alla distribuzione delle responsabilità tra i soggetti coinvolti, il «considerando» n. 11 dello Schema di proposta di regolamento prevede che l'*utilizzatore* di un sistema di IA coinvolto in un evento dannoso dovrebbe essere qualificato *responsabile* a norma del regolamento «*solo laddove si qualifichi anche come operatore*. In caso contrario, l'entità del contributo al rischio da parte dell'utente, per negligenza grave o intenzionale, potrebbe comportare la responsabilità *per colpa* dell'utente nei confronti del ricorrente». In buona sostanza, l'utilizzatore-operatore dovrebbe essere assoggettato a un regime di responsabilità oggettiva o aggravata – a seconda che controlli un sistema di IA

"ad alto rischio" o meno – laddove l'utilizzatore-non operatore dovrebbe essere in qualche modo tutelato mediante assoggettamento ad un regime di responsabilità circoscritto alla colpa grave o al dolo.

Vengono poi fissati *massimali* per i risarcimenti e *prescrizioni ad hoc*.

Anche in correlazione agli accennati massimali, è prevista una disciplina di *assicurazione obbligatoria* quanto meno per gli operatori dei sistemi di IA "ad alto rischio".

Orbene, riprendendo l'esemplificazione precedentemente effettuata (*supra*, § 6), la start-up innovativa che produce ovvero offre al mercato un certo sistema di IA potrebbe essere agevolmente qualificata come persona giuridica-operatore di back-end.

È più complicato, invece, stabilire se la s.p.a. che utilizzi detto sistema per "scelte" strategiche, così come i suoi amministratori, possano essere qualificati come operatori di front-end. La questione qui può essere solo accennata, ma (*i*) occorrerebbe comprendere che cosa si intenda per "beneficio" ai sensi dell'art. 3, facilmente attribuibile alla s.p.a. ma di più ardua attribuzione per gli amministratori; (*ii*) quale possa essere il «controllo» dell'utilizzatore e quali siano i «potenziali rischi associati all'operatività e al funzionamento del sistema di IA»; (*iii*) l'importanza dei danni e dei pregiudizi legati al processo decisionale e il correlativo ruolo degli algoritmi.

Immaginando allora un possibile scenario d'indagine, si crede che potrebbero svolgere un ruolo significativo (*a*) la *due diligence* effettuata nei confronti del produttore (in *outsourcing*)-operatore di back-end e del sistema di IA prodotto, prendendo spunto anche dai criteri di diligenza indicati dallo Schema; (*b*) il corretto impiego del sistema di IA da parte della s.p.a. utilizzatrice, pure in termini di aggiornamento e di manutenzione; (*b*) la valutazione critica dell'*output* dell'algoritmo da parte dell'utilizzatore, anche in comparazione con altri elementi funzionali alla decisione effettuata, cercando di evitare una sorta di *ipse dixit*.

12.9. La proposta di regolamento c.d. "*AI Act*", apparentemente scollegata con i pregressi lavori

Si è fatto cenno in apertura alla Proposta di regolamento predisposta dalla Commissione europea, c.d. *Artificial Intelligence Act* (AIA), che però si pone in parziale discontinuità con gli altri documenti precedentemente analizzati.

Il tema non può essere qui approfondito, ma va segnalato, in primo luogo, il criterio non chiaro e piuttosto rigido con cui l'AIA distingue sistemi di IA "ad alto rischio" da sistemi di IA "non ad alto rischio" [55].

In secondo luogo, e soprattutto per ciò che qui interessa, l'AIA prevede una serie obblighi di *compliance* a carico degli operatori che impiegano sistemi di IA "ad alto rischio", chiaramente ispirati alle Linee-guida etiche. Nondimeno, detti obblighi di *compliance* non sono previsti per gli operatori che impiegano sistemi di IA "non ad alto rischio". Manca, inoltre, qualsiasi riferimento al regime di responsabilità civile [56].

Da tutto ciò consegue un evidente scollamento tra lo Schema di proposta del Parlamento e la Proposta dell'AIA della Commissione: non è facilmente riscontrabile la compatibilità tra un regime di responsabilità oggettiva e la previsione dei menzionati obblighi di *compliance*, per

---

[55] Cfr., in particolare, l'art. 6 AIA. Al riguardo, i sistemi di IA "ad alto rischio" concernerebbero tecnologie di IA che possono avere un impatto significativo sulla salute, la sicurezza o i diritti fondamentali delle persone fisiche; ovvero che possono essere componenti di sicurezza di un prodotto; ovvero che possano essere essi stessi un prodotto (*i*) regolato dalla legislazione dell'UE in tema di sicurezza dei prodotti e che richieda una valutazione di conformità da parte di un terzo, al fine di essere collocato sul mercato o messo in funzione secondo una normativa dell'UE, ovvero (*ii*) incluso in un'ulteriormente ristretta lista tassonomica. Per una prima analisi critica dell'AIA, cfr. M. EBERS, V.R.S. HOCH, F. ROSENKRANZ, H. RUSCHEMEIER, B. STEINRÖTTER, *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)*, in 4 *J* (2021) https://doi.org/10.3390/j4040043, pp. 589 ss., spec. pp. 593 ss.; M. VEALE, F. ZUIDERVEEN BORGESIUS, *Demystifying the Draft EU Artificial Intelligence Act Analysing the good, the bad, and the unclear elements of the proposed approach*, in J. of Information L. and Tech., 4/2021, pp. 97 ss., spec. 102 ss.; N. 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, in https://ssrn.com/abstract=3899991.

[56] La *ratio legis* di tali previsioni consisterebbe nel promuovere un mercato unico in tema di IA, nonché di incentivare l'innovazione, evitando i cc.dd. *chilling effects* dovuti ad un eccesso di regolamentazione e all'incertezza giuridica. Ma l'obiettivo principale è quello di rendere l'UE competitiva con gli Stati Uniti e la Cina nell'evoluzione delle tecnologie digitali. Cfr. i «considerando» (23) e (24) della Proposta. In dottrina, cfr. L. FLORIDI, *The European Legislation on AI*, cit.; A. BRADFORD, *Effetto Bruxelles. Come l'Unione Europea regola il mondo*, trad. it. P. Micalizzi, Milano, 2021. Sull'approccio etico, economico e normativo dell'UE in tema di IA, rispetto a U.S.A. e Cina, cfr., altresì. E. HINE, L. FLORIDI, *Artificial Intelligence with American Values and Chinese Characteristics: A Comparative Analysis of American and Chinese Governmental AI Polici*es, in https://ssrn.com/abstract=4006332, 2022; R. RIBERA D'ALCALÀ, *La bussola etica dell'intelligenza artificiale. Visioni e prospettive dell'Unione europea*, in *Etica digitale*, cit., da p. 101.

quanto concerne l'impiego di sistemi di IA "ad alto rischio". D'altro canto, l'impiego dei sistemi di IA "ad alto rischio" parrebbe soggetto a un rischio di *deregulation* eccessivo.

La sensazione è allora che tale Proposta dovrà essere significativamente rivista nella sua stessa struttura.

12.10. Impostazione per una responsabilità da organizzazione d'impresa

Il rapido *excursus* sull'evoluzione normativa in corso in tema di regolamentazione europea sull'IA permette di esporre alcune riflessioni che possono essere utili ai fini di uno studio *ex professo* del tema.

Si crede che l'utilizzo della "personalità elettronica", quand'anche in una prospettiva funzionale, non costituisca la soluzione più opportuna da adottare. Alcune tra le principali ragioni possono essere qui solo accennate: il veloce progresso tecnologico e l'inserimento di un (ulteriore) diaframma nell'interrelazione fra esseri umani, danni cagionati dall'impiego dell'IA e connessa responsabilità potrebbero favorire abusi, elusioni e frodi alla legge, o peggio, progetti criminali [57]; adottare una prospettiva "a soggetto" nei confronti dei sistemi di IA, pensando che essi decidano/agiscano e rispondano dei danni, rischierebbe, in ogni caso, di disincentivare e de-responsabilizzare coloro che devono rendere sicuro il sistema di IA; allo stesso tempo aumenterebbero le probabilità di innescare l'idea di attribuire diritti proprietari o addirittura diversi diritti della personalità ad entità inanimate, con rischi etici e di deriva dei diritti umani; sorgerebbero poi notevoli difficoltà di inserimento della "persona elettronica" nell'ambito dell'ordinamento vigente, soprattutto se si condivide l'idea che già per le persone giuridiche il rapporto tra diritti della personalità, diritti di proprietà industriale e impresa collettiva vadano regolati secondo principi diversi da quelli delle persone fisiche [58]. E d'altronde lo stesso Parlamento europeo (che, si ricorda, aveva formulato l'ipotesi della "personalità elettronica"), insieme a numerosi esponenti del mondo scientifico ed all'evoluzione normativa di importanti Stati membri, si è mostrato contrario a tale soluzione nello Schema di proposta di

[57] Su tale criticità, cfr. L. LOPUCKY, *Algorithmic Entities*, cit.

[58] Cfr., su tale ultimo aspetto e in termini generali, A. ZOPPINI, *I diritti della personalità*, cit., pp. 864 s., 884 s.

regolamento [59]. Nello stesso Schema di proposta di regolamento oltre che nel Libro Bianco, inoltre, l'attenzione posta alla correlazione tra responsabilità e *rischio* si sposa perfettamente con la responsabilità dell'imprenditore commisurata a come venga gestito il rischio d'impresa assunto tramite l'*organizzazione* d'impresa.

Seguendo l'impostazione dei documenti finora menzionati, appare preferibile tener ferma la prospettiva secondo cui un sistema di IA deve essere inteso *come un mero strumento a disposizione dell'uomo*: in tal senso, la tripartizione gaiana (*supra*, § 2) porterebbe a classificare l'IA quanto meno come *res*, seppure con un'anomala vicinanza alle *actiones*. Tuttavia, tale schema elementare non contempla l'*impresa* come *organizzazione* produttiva e come *attività* organizzata.

E allora si può proseguire il discorso, limitatamente a ciò che qui interessa, intendendo l'IA come strumento a disposizione di un uomo-imprenditore. Che poi detto imprenditore sia organizzato in forma di società di capitali, specie se imprenditore collettivo, non implica una minore centralità dell'uomo [60].

Al contrario, lo studio delle dottrine tradizionali e più recenti in tema di personalità giuridica può confermare l'imprescindibilità e la

---

[59] Per una critica all'ipotesi della "personalità elettronica" cfr. EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES, *Liability for Artificial Intelligence*, cit., pp. 37 ss.; OPEN LETTER TO THE EUROPEAN COMMISSION, *Artificial Intelligence and Robotics*, redatta da un gruppo di intellettuali, reperibile sul sito http://www.robotics-openletter.eu (ultimo accesso 10 settembre 2020). Cfr., altresì, in Francia la *Proposition de loi constitutionnelle* n. 2585 del 15 gennaio 2020, relativa alla *Charte de l'intelligence artificielle et des algorithmes*, la quale prevede espressamente, a protezione dei diritti dell'Uomo, che «Un système [«qui se compose d'une entité qu'elle soit physique (par exemple un robot) ou virtuelle (par exemple un algorithme) et qui utilise de l'intelligence artificielle», n.d.r.] *n'est pas doté de la personnalité juridique et par conséquent inapte à être titulaire de droits subjectifs*. Cependant les obligations qui découlent de la personnalité juridique incombent à la personne morale ou physique qui héberge ou distribue ledit système devenant de fait son représentant juridique» (enfasi aggiunta). Tra coloro che sono invece possibilisti verso l'impiego della "personalità elettronica" cfr. A. BERTOLINI, *Artificial Intelligence and Civil Liability*, cit., pp. 34 ss., seppure in una prospettiva funzionale e circoscritta ad alcuni casi di sistemi di IA e/o robotici particolarmente complessi e di cui appare difficile ricostruire profili individuali di responsabilità di programmatori, fornitori, utilizzatori ecc., come ad esempio l'autovettura a guida autonoma. Cfr., altresì, l'importante tesi autopoietica di G. TEUBNER, *Digitale Rechtssubjekte?*, cit., secondo cui l'agente digitale potrebbe essere inquadrato come un "ibrido", consistente in un'associazione uomo-macchina percepita unitariamente dall'ambiente sociale; *adde* C.P. CIRILLO, *I soggetti giuridici digitali*, in *Contr. impr.*, 2020, da p. 573.

[60] Cfr., in tal senso, MÖSLEIN, *Robots in the Boardroom*, cit., pp. 650 ss.

centralità del fattore umano anche in tale ambito [61]. Ciò, si crede, va tenuto ben presente laddove si paventi l'impiego di meccanismi analoghi alla persona giuridica per regolare la responsabilità per danni cagionati dall'impiego dell'IA.

Sempre esaminando le dottrine generali civilistiche ed anche autorevole dottrina giuscommercialistica in tema di società, si possono trovare invece importanti argomenti per inquadrare l'impiego di sistemi di IA nella prospettiva, oggettiva, dell'*organizzazione dell'attività* imprenditoriale [62].

In buona sostanza, si può immaginare *un sistema di IA come un'articolazione dell'organizzazione dell'impresa societaria* o comunque come *parte dell'attività* il cui (specifico) *rischio* deve essere gestito nell'ambito dell'organizzazione imprenditoriale ed in qualche modo garantito dal patrimonio dell'imprenditore.

Secondo tale prospettiva – concentrando l'attenzione sulle imprese che *utilizzano* sistemi di IA [63] – anche *de iure condito* si può individuare una regolamentazione della responsabilità civile per l'impiego di queste nuove tecnologie traendo spunto dagli istituti della responsabilità in qualche modo connessi ad un'organizzazione d'impresa non conforme ai criteri testé menzionati. Nell'ordinamento giuridico italiano è il caso della responsabilità per danni cagionati da cose in custodia (art.

---

[61] La letteratura al riguardo è vastissima, a partire dalla pandettistica tedesca. Cfr., per tutti, T. ASCARELLI, *Considerazioni in tema di società e personalità giuridica*, in *Riv. dir. comm.*, 1954, I, da p. 245 e da p. 333; ID., *Personalità giuridica e problemi delle società*, in *Riv. Soc.*, 1957, da p. 981; M. BASILE, A. FALZEA, voce «Persona giuridica (dir. priv.)», in *Enc. Dir.*, XXIII, Milano, 1983, da p. 234.; A. FALZEA, *Il soggetto nel sistema dei fenomeni giuridici*, Milano, 1939, pp. 171 ss.; ID., voce «Capacità (teoria gen.)», in *Enc. Dir.*, VI, Milano, 1960, da p. 8; F. D'ALESSANDRO, *Personalità giuridica e analisi del linguaggio*, rist. a cura di N. Irti, Padova, 1991; N. IRTI, *Sul concetto di titolarità (persona fisica e obbligo giuridico)*, in *Riv. dir. civ.*, 1970, I, da p. 501, pp. 519 ss.; R. ORESTANO, *Diritti soggettivi e diritti senza soggetto*, in *Jus*, 1960, da p. 142; ID., *Il « problema delle persone giuridiche » in diritto romano*, Torino, s.d. ma 1968, pp. 55 ss.; G.G. SCALFI, *L'idea di persona giuridica e le formazioni sociali titolari di rapporti nel diritto privato*, Milano, 1968; P. ZATTI, *Persona giuridica e soggettività*, Padova, 1975. Cfr., altresì, F. RANIERI, *L'invenzione della persona giuridica*, Milano, 2020.

[62] Cfr., in termini generali, P. FERRO-LUZZI, *I contratti associativi*, Milano, 1971, spec. pp. 170 ss.; C. ANGELICI, *La società per azioni. Principi e problemi*, vol. I, in *Trattato di diritto civile e commerciale*, a cura di P. Schlesinger, Milano, 2012, pp. 126 ss., pp. 139 ss., pp. 345 ss.; P. ZATTI, *Persona giuridica e soggettività*, cit., pp. 172 s.

[63] Relativamente più semplice può essere il discorso per le imprese che programmano ovvero pongono sul mercato sistemi di AI, quale *prodotto* o *servizio*. In tale ipotesi, seppure con i dovuti *distinguo*, si può ragionare prendendo spunto dalla responsabilità da prodotto difettoso o non sicuro.

2051 c.c.) ma anche della responsabilità per fatto di dipendenti/ausiliari (artt. 1228 e 2049 c.c.) o comunque institoria o legata alla rappresentanza, legale o volontaria. Il discorso può valere persino per la responsabilità da rischio (art. 2050 c.c.), a seconda di come vada collocato lo sviluppo inatteso o il mal funzionamento del sistema di IA nell'ambito del rischio d'impresa.

Al riguardo, traendo spunto anche dall'evoluzione normativa in tema di responsabilità da reato delle persone giuridiche, la dottrina che ha approfondito il tema propende per una *responsabilità da organizzazione scorretta e inadeguata*, da preferire alla responsabilità oggettiva [64]. Tale impostazione non è estranea neppure all'evoluzione di altri ordinamenti giuridici europei o di *common law* [65] ed è ulteriormente avvalorata dalla codificazione dei principi di corretta gestione imprenditoriale e societaria, anche sotto il profilo dell'adeguatezza degli assetti organizzativi (artt. 2381, 2403, 2497, 2086 2° co., c.c.), avvenuta con la riforma del diritto societario del 2003 e con la recente riforma del diritto della crisi d'impresa.

Ed allora si può pensare, in primo luogo, che un simile approccio valorizzi e incentivi opportunamente le imprese che si organizzano in maniera adeguata per un corretto impiego dei sistemi di IA. Adottando il criterio della responsabilità oggettiva si rischierebbe invero di provocare una selezione avversa a svantaggio delle imprese più efficienti, che pagherebbero due o persino tre volte (in caso di assicurazione obbligatoria con rivalsa) i costi di tale impiego. In tal modo si disincentiverebbero l'efficienza ed il progresso tecnologico, a discapito dell'utilità sociale dell'iniziativa economica (artt. 3, 2° co. e 41, 2° co., Cost.) [66].

In secondo luogo, tale approccio individua un modello giuridico consolidato di riferimento che consente di chiarire non solo i *criteri di imputazione della responsabilità* ma anche *i criteri di imputazione di*

---

[64] Cfr. F. GUERRERA, *Illecito e responsabilità nelle organizzazioni collettive*, Milano, 1991; M. CAMPOBASSO, *L'imputazione di conoscenza nelle società*, Milano, 2002; A. ZOPPINI, *Imputazione dell'illecito penale e «responsabilità amministrativa» della persona giuridica*, in *Riv. soc.*, 2005, da p. 1314; E. GINEVRA, *Identità e rilevanza della persona giuridica alla luce del d.lgs. n. 231/2001*, in *Riv. soc.*, 2020, da p. 72. Cfr., altresì, C. ANGELICI, *op. loc. ult. cit.*

[65] Per un approfondimento sul tema, anche con riferimenti dottrinali, cfr. M. CAMPOBASSO, *op. cit.*, pp. 37 ss., pp. 80 ss.; F. GUERRERA, *op. cit.*, pp. 303 ss. Cfr., altresì, EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES, *Liability for Artificial Intelligence*, cit., pp. 19 ss.

[66] Circa il rilievo giuridico dell'utilità sociale dell'iniziativa economica nella responsabilità da organizzazione imprenditoriale, cfr. E. GINEVRA, *Identità*, cit.

conoscenza e della volontà negoziale. Sempre al fine di risolvere l'opzione fra responsabilità per colpa, aggravata od oggettiva – se si condividono i risultati della dottrina che propende per la responsabilità da scorretta/inadeguata organizzazione – si crede che sarebbe pregiudizievole per l'imprenditore che impiega sistemi di IA adoperare un criterio d'imputazione di responsabilità più severo (la responsabilità oggettiva) rispetto a quello previsto per gli imprenditori che utilizzano rappresentanti/ausiliari o cose meno evolute [67].

12.10.1. (segue) Riflessi nel diritto societario: il ruolo dell'adeguatezza degli assetti societari

Nell'ambito di questa impostazione, l'organizzazione imprenditoriale in forma di società, e in particolare di società di capitali, permette di inquadrare il dovere di corretta organizzazione dell'impresa per l'impiego dell'IA nell'ambito del dovere degli amministratori di istituire un assetto imprenditoriale e societario adeguato alla natura ed alle dimensioni dell'impresa (artt. 2086, 2° co., 2381 e 2403 c.c.).

Al riguardo, esigenze di sintesi impongono di accennare solamente che tale ultimo dovere, da un lato, richiede che gli amministratori dispongano in qualche modo (direttamente o indirettamente) di competenze specifiche in tema di di IA [68] e, dall'altro, l'adozione di una prospettiva *procedimentale* [69] non dissimile da quella contemplata nei documenti menzionati nei precedenti paragrafi. In particolare, la codificazione normativa dei doveri di corretta gestione imprenditoriale (art. 2497 c.c.) consente di attribuire un rilievo giuridico significativo all'osservanza delle migliori prassi e norme tecniche esistenti, da

[67] In termini non dissimili sul punto, G. TEUBNER, *Digitale Rechtssubjekte?*, cit., pp. 187 s.

[68] Una spia normativa in tal senso si rinviene nell'art. 2392 c.c. ove è previsto che gli amministratori di una s.p.a. devono adempiere ai doveri imposti dalla legge e dallo statuto «con la diligenza richiesta *dalla natura dell'incarico e dalle loro specifiche competenze*» (enfasi aggiunta). E sul problema delle competenze degli amministratori cfr., altresì, il «considerando» n. 18 dello Schema di proposta di regolamento, ove si legge che «l'operatore potrebbe avere una conoscenza limitata degli algoritmi e dei dati utilizzati nel sistema di IA. Si dovrebbe presumere che l'operatore abbia osservato la dovuta diligenza che ci si può ragionevolmente attendere da questi nel selezionare un sistema di IA idoneo, laddove l'operatore abbia scelto un sistema di IA certificato».

[69] Cfr. C. ANGELICI, *La società per azioni*, cit., p. 417 *sub* nt. 140; ID., *Interesse sociale e business judgment rule*, in *Riv. dir. comm.*, 2012, I, da p. 573.

canalizzare entro sistemi di controllo interno e di procedure di gestione dei rischi.

In tale ambito, si crede, *possono essere annoverati i documenti precedentemente citati ed anche le linee guida etiche*. Il risultato è degno di nota già per il solo fatto che si individua una cornice giuridica anche a prescrizioni *prima facie* meramente etiche.

E sempre all'interno dei principi di corretta gestione imprenditoriale e di adeguatezza degli assetti, l'osservanza, da parte degli amministratori di società, di una *due diligence* verso le controparti contrattuali nonché verso gli strumenti adottati per l'esercizio dell'impresa, può contribuire in maniera decisiva a sviluppare la cooperazione tra i vari operatori economici nella catena di approvvigionamento e tra gli utilizzatori. Detta cooperazione, si ricorda, è auspicata dalla Commissione europea al fine di conseguire l'obiettivo della *certezza giuridica* mediante i principi della "responsabilità condivisa" e dell'*accountability* e inoltre è parte dello Schema di proposta di regolamento (*supra*, § 8) [70].

A tal proposito, la contrattazione tra le varie componenti, prevalentemente imprenditoriali, della catena di valore può contribuire a regolamentare chiaramente i confini di ciascuna responsabilità, con opportune clausole di salvaguardia, ad esempio tese a chiarire i rispettivi doveri di monitoraggio e aggiornamento del *software*, specie se indipendente.

12.11. Impressioni di sintesi: una normativa in costruzione che può incentivare il progresso, favorire una corretta organizzazione d'impresa e tutelare i diritti fondamentali

Il *rilievo centrale* che l'approccio dell'Unione europea attribuisce all'*essere umano* e all'osservanza dei *diritti fondamentali* costituisce certamente un fattore decisivo per impedire l'appiattimento, o peggio la

[70] Cfr., altresì, art. 8.4 dello Schema di proposta di regolamento, ove si legge che «Il produttore di un sistema di IA è tenuto a cooperare con l'operatore o con la persona interessata, su loro richiesta, e a fornire loro informazioni, nella misura giustificata dall'importanza della pretesa, al fine di consentire l'individuazione delle responsabilità».

sudditanza, nei confronti degli *output* dei sistemi di IA e quindi di una società o di un'economia *data driven*.

Un segnale, inquietante, dell'importanza del tema si scorge nell'epigrafe della *Proposition de loi constitutionnelle* n. 2585 del 15 gennaio 2020, relativa alla *Charte de l'intelligence artificielle et des algorithmes*, ove si legge che « Au même titre que les virus s'intègrent au long cours au patrimoine génétique des humains, les technologies du quotidien entrent de fait dans les réflexions».

Volendo seguire l'impostazione incentrata sulla *responsabilità, aggravata, da scorretta o inadeguata organizzazione d'impresa*, la prima impressione corre nel senso di auspicare che il futuro quadro normativo in tema di responsabilità civile per il funzionamento di sistemi di intelligenza artificiale consideri in maniera in qualche modo "transitoria" la responsabilità oggettiva dei sistemi di IA. Si vuol dire che, al di fuori di casi eccezionali particolarmente rischiosi, si potrebbe immaginare che vengano inclusi nell'elenco dei sistemi di IA "ad alto rischio" soprattutto quelli più innovativi e che proprio a causa della loro innovatività non consentono in una fase iniziale di governare del tutto i rischi connessi.

D'altronde le principali innovazioni tecnologiche in tema di sistemi di IA dovrebbero svilupparsi in un ambiente normativo protetto, in stretta collaborazione con le autorità di vigilanza competenti. In tal senso depone il «considerando» L della Risoluzione del 2020, ove si legge che «sarebbe opportuno adottare un approccio in cui si ricorra a sperimentazioni, progetti pilota e spazi di sperimentazione normativa per trovare soluzioni proporzionate e basate su dati concreti che affrontino, ove necessario, situazioni e settori specifici».

Detto approccio è particolarmente condiviso nell'ambito dell'intero fenomeno del *fintech*, ove la Commissione europea intende favorire l'aggiornamento delle autorità di vigilanza nonché il dialogo fra queste, le imprese vigilate e le imprese *fintech*, mediante «facilitatori *fintech*» (*innovation hub*, *sandbox* o *incubator*) istituiti presso le autorità di vigilanza nazionali nonché tramite istituzione di laboratori per le tecnologie finanziarie e la costituzione di un gruppo di esperti che valutino la compatibilità tra il quadro normativo regolamentare, attuale e *in fieri*, ed il progresso tecnologico [71].

[71] Cfr. COMMISSIONE EUROPEA, *Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo*, Bruxelles, 8 marzo 2018, COM(2018) 109 final; ESAS, *FinTech: Regulatory sandboxes and innovation hubs*, 2018, in

I rischi non governabili dovrebbero allora essere minimi e in ogni caso il problema del *black box* dovrebbe essere presto superato perfezionando il sistema di IA innovativo o la sua applicazione innovativa.

Inoltre, i vantaggi per la collettività devono notevolmente oltrepassare i pregiudizi, anche potenziali, come chiaramente espresso dal principio di *efficienza* (*supra*, § 4), dalle Linee-guida etiche riguardo al *trade-off* tra *accuracy* e trasparenza (*supra*, § 5) nonché dal «considerando» n. 4 dello Schema di proposta di regolamento, ove si puntualizza che «i vantaggi della diffusione dei sistemi di IA saranno di gran lunga superiori agli svantaggi».

A favore della tendenziale temporaneità della situazione di "alto rischio" e della connessa responsabilità oggettiva giovano, nella Schema di proposta di regolamento, (*i*) l'art. 4.2, che delega alla Commissione il potere anche di *eliminare* sistemi di IA dall'elenco di quelli "ad alto rischio", così assoggettandoli ad un regime responsabilità aggravata in luogo della responsabilità oggettiva; (*ii*) il «considerando» n. 2, ove si legge che «*Specialmente all'inizio del ciclo di vita di nuovi prodotti e servizi*, dopo che questi hanno superato i test preliminari, per l'utente e per i terzi è presente un certo grado di rischio che qualcosa non funzioni correttamente» [72].

D'altra parte, pur sempre ad una prima sensazione, l'approccio procedimentale promosso soprattutto attraverso le Linee guida etiche e il Libro bianco sembra non trovare piena realizzazione nei sistemi di IA "ad alto rischio", così come definiti e disciplinati. Così, nel «considerando» n. 3 dello Schema di proposta di regolamento si avverte la consapevolezza di un possibile affievolimento, tra gli altri, della *fairness*, dell'*explicability*, dell'*intervento e sorveglianza umani* oltre che della *robustezza* [73].

Tutto ciò potrebbe essere interpretato come una *tensione proattiva al raggiungimento di tutti i requisiti previsti dalle Linee-guida e dal Libro*

www.europa.esma.eu.

[72] Enfasi aggiunta.

[73] Ed infatti vi si legge che «L'uso di sistemi di IA nella vita quotidiana porterà a situazioni in cui la loro opacità (elemento "scatola nera") e la pluralità di soggetti che intervengono nel loro ciclo di vita renderanno estremamente oneroso o addirittura impossibile identificare chi avesse il controllo del rischio associato all'uso del sistema di IA in questione o quale codice o input abbia causato l'attività pregiudizievole. Tale difficoltà è aggravata dalla connettività tra un sistema di IA e altri sistemi, di IA e non di IA, dalla sua dipendenza dai dati esterni, dalla sua vulnerabilità a violazioni della cibersicurezza e dalla crescente autonomia di sistemi di IA attivati dall'apprendimento automatico e dalle capacità di apprendimento profondo».

bianco, promossa dal legislatore *in fieri*. Uno dei principali strumenti per raggiungere tale risultato sarebbe costituito proprio dalla responsabilità oggettiva, da intendersi allora come sprone al perfezionamento delle innovazioni tecnologiche immesse nel mercato e tra il pubblico, al fine di beneficiare del più clemente strumento della responsabilità aggravata.

Se così fosse, quest'ultimo regime andrebbe a costituire la regola, laddove l'assunzione di un "alto rischio" e la connessa responsabilità oggettiva potrebbero essere l'eccezione.

* Postilla. Nelle more della pubblicazione di questo scritto la Commissione europea ha pubblicato due proposte di direttiva molto rilevanti rispetto ai temi qui trattati. Si fa riferimento alla Proposta di direttiva del Parlamento europeo e del Consiglio «on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)» [COM(2022) 496 final (di seguito "AILD")] e alla Proposta di direttiva del Parlamento europeo e del Consiglio «on liability for defective products» [COM(2022) 495 final (di seguito "PLD")], entrambe del 28.09.2022.
Al riguardo, l'AILD prevede una serie di incentivi di *disclosure* verso i soggetti danneggiati da sistemi di IA nonché di presunzioni *iuris tantum* a favore di questi ultimi, al fine di non rendere più onerosa la loro azione di responsabilità extracontrattuale, rispetto a chi abbia subìto un danno derivante da diverse circostanze.
La stessa AILD si coordina poi con la PLD per agevolare l'individuazione del responsabile nell'ambito della catena di valore dei sistemi di IA, con particolare attenzione al produttore.
A tal proposito, la PLD mira a colmare i limiti della normativa originaria in tema di danno da prodotti difettosi, limiti che sono stati segnalati nelle pagine che precedono.