D'Alfonso G, 'Danni algoritmici e sviluppi normativi europei tra "liability" e "permittance" rules' (2022) 2 EJPLT, 18-66.
DOI: https://doi.org/10.57230/ejplt222GDA

EJPLT
ISSN 2704-8012



Danni algoritmici e sviluppi normativi europei tra "liability" e "permittance" rules.

Algorithmic damages and European regulatory developments between liability and permittance rules.

GIOVANNA D'ALFONSO
Associate Professor of Private Law
Università degli Studi della Campania Luigi Vanvitelli

Abstract

Le nuove forme di tecnologia intelligente, più o meno automatizzata, applicata ai processi di produzione di beni e di erogazione di servizi, possono dar luogo ad una pluralità di scenari dannosi completamente diversi rispetto a quelli tradizionalmente affrontati a livello giurisprudenziale, aprendosi nuove problematiche di responsabilità civile. L'articolo analizza criticamente le soluzioni offerte dai più rilevanti provvedimenti europei in fieri, dettati in materia di responsabilità civile "algoritmica" extracontrattuale, e i capisaldi della disciplina introdotta dalla proposta di regolamento, la c.d. legge sull'intelligenza artificiale. Si evidenzia il rapporto di complementarietà tra le "liability" rules, attinenti alle tematiche di natura prettamente civilistica, e le "permittance" rules, concernenti le esigenze di regolamentazione pubblicistica del settore.

The new types of intelligent technology, more or less automated, applied to the processes of production of goods and delivery of services can give rise to a multitude of damage scenarios completely different from those traditionally approached, at a jurisprudential level, opening up new issues of civil liability. The article critically analyses the solutions offered by the most relevant European regulations in progress, laid down on the subject of tort "algorithmic" liability, and the fundamentals of the discipline introduced by the proposal for a regulation, the so-called Artificial Intelligence Act. The complementary relationship between the "liability" rules, relating to issues of a strictly civil nature, and the "permittance" rules, concerning the requirements of public regulation of the sector, is highlighted.

© The author(s) 2022, published by Suor Orsola Benincasa Università Editrice. This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: algorithmic damages; civil liability models; multi-layered system of responsibility; "liability" rules; "permittance" rules; European regulatory perspectives; critical remarks.

Summary: Introduzione. – 1. I "nuovi" danni algoritmici: quali modelli di responsabilità civile? – 2.1. Le questioni affrontate dal legislatore europeo. L'individuazione del soggetto responsabile nell'ambito della "catena di valore" del sistema digitale. – 2.2. (*segue*) La probatio "diabolica" del nesso di causalità tra l'operato del sistema intelligente e l'evento dannoso. – 2.3. (*segue*) Principio di accountability e "sistema multilivello" di responsabilità. – 3.1.1. Scenari normativi. Le "*permittance" rule*s e la proposta della c.d. legge sull'intelligenza artificiale. – 3.1.2. (*segue*) Punti di forza e profili critici della disciplina. – 3.2.1. (*segue*) Le "*liability rules*". La Risoluzione del Parlamento europeo «recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale». – 3.2.2. (*segue*) La proposta di revisione della direttiva sulla responsabilità per danni da prodotto difettoso. – 3.2.3.(*segue*) La proposta c.d. *AI Liability Directive*. – Conclusioni.

Introduzione.[1]

Le nuove forme di tecnologia intelligente, più o meno automatizzata, applicata ai processi di produzione di beni ed erogazione di servizi, possono dar luogo ad una pluralità di scenari dannosi completamente diversi rispetto a quelli tradizionalmente affrontati a livello giurisprudenziale, aprendosi nuove problematiche di responsabilità civile[2].

[1] Questo lavoro è il risultato del Progetto di Ricerca finanziato "Diritto e Intelligenza Artificiale: nuovi orizzonti giuridici della personalità e responsabilità robotica" (PID2019-108669RBI00 /AEI/ 10.13039/501100011033), di cui la Prof.ssa Margarita Castilla Barea è la principale ricercatrice

[2] Cfr. A. Amidei, *Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo*, in *Giur.it*. 2021, p. 100. Numerosi sono i contributi della letteratura giuridica che si è interrogata sulle problematiche sollevate dallo sviluppo esponenziale delle intelligenze artificiali, sulle complessità dell'adattamento della normativa vigente alle nuove esigenze del mondo digitale e che ha approfondito i capisaldi dei provvedimenti *in fieri*, elaborati in ambito europeo. E*x multis*, cfr. G. Alpa (a cura di), *Diritto e intelligenza artificiale. Profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile,* Pisa, 2020, *passim*; M. Castilla Barea, *La universidad ante los desafíos éticos de la inteligencia artificial. Reflexiones a propósito del nuevo «marco europeo de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas»*, in Edunovatic 2020, Conference Proceedings: 5th Virtual International Conference on Education, Innovation and ICT, December 10 - 11, 2020, pp. 630 ss.; S. Faro, T.E. Frosini, G. Peruginelli (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, Bologna, 2020, *passim*; P. Perlingieri, S. Giova, I. Prisco (a cura di), *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, Napoli, 2020, *passim*; ID. (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto e economia*, Napoli, 2020, *passim*; U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Torino, 2020, *passim*; A. Santosuosso, *Intelligenza e diritto. Perché le nuove tecnologie sono una grande opportunità per il diritto,* Milano, 2020, *passim*; I. Zurita Martín, *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*, Reus, Madrid, 2020, *passim*, recensito da F. J. Jiménez Muñoz, in *Actualidad Jurídica Iberoamericana*, Nº 14, febrero 2021, pp. 1141 ss.; U. Ruffolo (a cura di), *XXVI Lezioni di Diritto dell'intelligenza artificiale*, Torino, 2021, *passim*; D. Buzzelli, M. Palazzo (a cura di), *Intelligenza artificiale e diritti della persona*, Pisa, 2022, *passim*; A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?, Volume 1., Diritti fondamentali, dati personali e regolazione*, Bologna, 2022, *passim*; ID. (a cura di), *Intelligenza*

La portata dei "nuovi danni" è strettamente correlata alle modalità operative delle tecnologie digitali 'emergenti'[3].

Quando le regole comportamentali e relazionali della macchina sono predeterminate, al momento della programmazione, la stessa indirizzerà le proprie scelte, azioni e risoluzioni, sulla base delle prescrizioni e dei dati forniti dal programmatore e, di conseguenza, i danni cagionati ai destinatari delle stesse potranno essere generati da un difetto di progettazione o di programmazione[4].

Diversamente, nei sistemi di intelligenza artificiale "di ultima generazione" [5], dotati di capacità di autoapprendimento, l'operato della macchina nel mondo esterno non discende da regole predeterminate, dal momento che le scelte sono assunte, in base all'elaborazione di algoritmi di *machine learning*[6], in maniera autonoma dal controllo e dall'intervento umano. Il sistema digitale, oltre a basarsi sul *training* ricevuto, si confronta con la realtà e si trasforma, in base alle interazioni con l'ambiente esterno in cui opera, dal quale può ricevere *input*; per, poi, adottare comportamenti e decisioni coerentemente con i dati esperienziali acquisiti nel tempo[7]. In tal caso, i danni possono discendere dai meccanismi di *self-learning* che elaborino opzioni difformi da quanto previsto in fase di programmazione[8].

Nel variegato panorama dei cc.dd. danni "algoritmici", viene in rilievo l'ipotesi che un sistema informatico, debitamente programmato, finisca col ledere il diritto di determinati soggetti a non essere discriminati e ad avere un

---

artificiale e diritto: una rivoluzione?, Volume 2. *Amministrazione, responsabilità e giurisdizione*, Bologna, 2022, *passim*; M. TAMPERI, *Intelligenza artificiale e le sue evoluzioni. Prospettive civilistiche,* Padova, 2022, *passim*; G. SARTOR, *L'intelligenza artificiale e il diritto*, Torino, 2022, *passim*; L. DI DONNA, *Intelligenza artificiale e rimedi risarcitori*, 2022, Padova, *passim*.

[3] Le tecnologie digitali sono riconducibili alla categoria delle c.dd. tecnologie emergenti, in ragione della velocità con la quale vengono sviluppate e del loro impatto "rivoluzionario" nei settori economici, sociali ed ambientali in cui sono impiegate. Cfr. R. MONTINARO, *Responsabilità da prodotto difettoso. Tecnologie digitali tra soft law e hard law*, in *Pers.merc.*, 2020, p. 351.

[4] Cfr. A. SANTOSUOSSO, C. BOSCARATO, F. CAROLEO, *Robot e diritto: una prima ricognizione*, in *Nuova giur. comm.*, 2012, p. 494 ss.

[5] L'art. 3, proposta della c.d. Legge sull'intelligenza artificiale (Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione, Bruxelles, 21.4.2021 COM(2021) 206 final, 2021/0106(COD)), definisce «sistema di intelligenza artificiale» un *software*, sviluppato con una o più delle tecniche e degli approcci (elencati nell'allegato I), che può generare, per una determinata serie di obiettivi definiti dall'uomo, «*output* quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono». Può, dunque, affermarsi che l'intelligenza artificiale consiste in una famiglia di tecnologie, in grado di generare *output*. Occorre precisare che non si può parlare di un'unica intelligenza artificiale, ma bisogna parlare di intelligenze artificiali al plurale, poiché possono differenziarsi, a seconda dei tipi di *machine learning* e di agenti di *software*, più o meno autonomi. Cfr. L. COPPINI, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, in *Politica del diritto*, 2018, p. 720.

[6] Stimata dottrina puntualizza che la caratteristica essenziale dell'intelligenza artificiale è di poter dar luogo ad un processo di autoapprendimento ed essere *self-learning,* chiarendo che il *machine learning* ed il suo molteplice atteggiarsi si caratterizza per la capacità di apprendimento della "macchina", sia che si tratti di entità robotica, sia che sia un'entità meramente immateriale. Nell'ambito dei sistemi di *machine learning*, si erge lo specifico settore applicativo del *deep learning*, che solleva ulteriori problemi, a causa della complessità dei modelli matematici usati (cd. "reti neurali" artificiali). Cfr. U. RUFFOLO, *La responsabilità da produzione e gestione dell'intelligenza artificiale self learning*, in ID. (a cura di), *XXVI Lezioni*, *op.cit.*, p. 132, s.

[7] Cfr. U. SALANITRO, *Intelligenza artificiale e responsabilità: la strategia della Commissione Europea*, in *Riv.dir.civ.*, 2020, p. 1247.

[8] Cfr. V. DI GREGORIO, *Intelligenza artificiale e responsabilità civile: quale paradigma per le nuove tecnologie?,* in *Danno e resp.*, 2022, p. 53.

libero ed equo accesso a beni e servizi[9]. I meccanismi di '*scoring*', ampiamente impiegati nella prassi digitale, per selezionare gli aspiranti ad una posizione lavorativa, possono condurre all'inammissibilità ad un colloquio, oltre che alla mancata assegnazione di un posto di lavoro[10]. I medesimi, utilizzati nel vaglio della potenziale solvibilità di chi miri ad ottenere un fido bancario[11] oppure nella valutazione delle caratteristiche dei clienti con cui stipulare polizze assicurative[12], possono portare ad esiti negativi della pratica bancaria o assicurativa.

Il ricorso all'algoritmo può determinare la compromissione delle libertà e dei diritti fondamentali della persona, quali la sicurezza degli individui, la loro salute, la vita privata e la protezione dei dati personali, l'integrità, la dignità, l'autodeterminazione[13].

Si pensi alle conseguenze negative che possano provenire ad una persona, sul piano economico, reputazionale ed emotivo, dal trattamento algoritmico e dalla circolazione dei suoi dati personali[14], nonché ai possibili incidenti dovuti dalla loro perdita[15]; ai danni cagionati, nel settore sanitario, alla salute del paziente dall'uso di sistemi di supporto alla diagnosi medica che, a causa della scarsa rappresentatività o del mancato aggiornamento dei dati che siano stati loro forniti, segnalino, come urgente, un erroneo trattamento curativo o farmacologico ovvero erroneamente non ne indichino uno necessario[16].

Si consideri che un algoritmo incorporato in un prodotto può cagionare un pregiudizio alla salute di chi lo adoperi o di terzi: possono verificarsi incidenti causati da un veicolo *self-driving*, il cui programma sbagli, nel valutare gli *input* che provengano dall'ambiente circostante[17]; errori commessi dai *robot* chirurgici, a danno dei pazienti[18] oppure dai *robot* industriali, a danno dei lavoratori.

---

[9] Cfr. G. Mobilio, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, consultabile on line sul sito *www.federalismi.it*, 2020, n. 16, p. 285.

[10] Si veda la pronuncia del Cons. St., 8 aprile 2019, n. 2270, in *Foro it.*, 2019, 11, III, c. 606, riguardo agli esiti della procedura dell'assegnazione delle sedi al personale docente scolastico (l. 107/2015), compiuta sulla base di un algoritmo appositamente introdotto dal Miur.

[11] Cfr. G. Biferali, *Big data e valutazione del merito creditizio per l'accesso al peer to peer lending*, in *Dir.inf e informatica*, 2018, p. 487 ss.

[12] Cfr. D. Porrini, *Big data, personalizzazione delle polizze ed effetti nel mercato assicurativo*, in V. Falce, G. Ghidini, G. Olivieri (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2018, p. 319 ss.

[13] Sul punto cfr. M. Gambini, *Responsabilità civile e controlli del trattamento algoritmico*, in P. Perlingieri, S. Giova, I. Prisco (a cura di), *Il trattamento algoritmico, op.cit.*, p. 314.

[14] Cfr. M. Infantino, *La responsabilità per danni algoritmici: prospettive europeo-continentali*, in *Resp. civ. e prev.*, 2019, pp. 1762 ss., par. 2, consultabile *online*, sul sito http://dejure.it

[15] Cfr. V. Zeno-Zenkovich, *Liability for Data Loss*, in Mak-Tjin Tai Berlee (eds.), *Research Handbook*, in *Data Science and Law*, Cheltenham, 2018, pp. 39 ss.

[16] Cfr. G. Comandé, *Intelligenza artificiale e responsabilità tra liability e accountability: il carattere trasformativo dell'IA e il problema della responsabilità*, in *Anal.giur.econ.*, 2019, p. 182.

[17] Tra i contributi sul tema, cfr., *ex multis*, M. C. Gaeta, *Liability rules and self-driving cars. The evolution of tort law in the light of new technologies*, Napoli, 2019, *passim*; F.P. Patti, *The European Road to Autonomous Vehicles,* 43 Fordham Int'l L.J. 125 (2019), p. 125 ss.; L. Gatt, I. Caggiano, M.C. Gaeta, *Italian Tort Law and Self-Driving Cars: State of art and Open Issues,* in B.H. Oppermann, J. Stender-Vorwachs (a cura di), *Autonomes Fahren. Technische Grundlagen, Rechtsprobleme, Rechtsfolgen*, München, 2020, p. 239 ss.

[18] Per un'attenta disamina della tematica della responsabilità civile nel campo della robotica medica, cfr. C. Perlingieri, *Responsabilità civile e robotica medica*, in *Tecnologie e diritto*, 2020 p. 165 ss. Con precipuo riguardo alla chirurgia plastica, cfr. M. Migliardi, *La chirurgia plastica nell'era dell'intelligenza artificiale. Tutela della salute, privacy e consenso informato*, Padova, 2022, p. 125 ss.

L'impiego dell'algoritmo può produrre ingenti perdite agli investitori, ad esempio, per effetto di un *bug* oppure di un comportamento anomalo del programma che animi un *robo-advisor* finanziario[19].

Sorge allora il quesito di quale sia il modello di responsabilità civile più adeguato a tutelare i soggetti lesi dai sistemi digitali e a garantire loro la corretta ed equa riparazione dei danni subiti[20].

La questione assume particolare rilevanza, quando tali sistemi sono capaci di apprendimento e in grado di assumere decisioni autonome, giacché la complessità delle tecnologie incide negativamente sulla comprensione dei meccanismi, in base ai quali è stata presa una determinata risoluzione. I processi decisionali automatizzati, ideati per rispondere, oltre che a stimoli predeterminati, a nuovi impulsi, identificati autonomamente dagli algoritmi, finiscono con l'essere incontrollabili ed imprevedibili, *ex ante*, da parte di chi li progetta, li programma, li sviluppa e li utilizza; opachi *ex post*[21] e, pertanto, difficilmente spiegabili, imperscrutabili ed indecifrabili da parte dei loro destinatari, in quanto nascosti dentro una scatola nera (il c.d. effetto *black box*)[22], con conseguenti difficoltà di contestazione in sede giudiziaria[23].

Tali peculiarità rendono la soluzione non facile.

Primariamente, è difficile rispondere all'interrogativo di portata giuridica, oltre che etica, di chi e a quale titolo sia il soggetto responsabile delle condotte autonome dei sistemi tecnologici e dei danni dalle medesime provocati. Se coloro che progettano, programmano, sviluppano ed usano gli algoritmi non saranno in grado di prevederne le reazioni e, di riflesso, i pregiudizi conseguenti, in quale modo dovranno essere allocate le responsabilità[24]?

Si dovrà individuare il danneggiante, tra i soggetti che intervengono nel "ciclo di vita" dei sistemi di intelligenza artificiale, creandoli, eseguendone la manutenzione o controllandone i rischi associati[25], quali: l'ideatore-autore-progettista dell'algoritmo, veicolante l'apprendimento; l'"addestratore", figura identificabile in colui che "addestri" un'entità artificiale intelligente o comunque la esponga ad esperienze che siano congrue ad indirizzarlo ovvero ad istruirlo; colui che lo utilizzi o lo "produca" o lo incorpori in un prodotto oppure in una componente dello stesso; il programmatore del *software*; il fornitore di sistemi intelligenti ed, in alcuni casi, l'utilizzatore (*user*) o il "titolare" (a vario titolo) ovvero il "custode" della macchina[26].

Tra l'altro, tali figure possono coincidere, soprattutto nelle imprese di grandi dimensioni che, invece di affidarsi a terzi, scelgano l'internalizzazione della produzione delle componenti del prodotto digitale: si immagini un'impresa automobilistica che, nel costruire un'auto a guida autonoma, produca

---

[19] Sul tema, cfr. E. CORAPI, *Robo advice*, in G. ALPA (a cura di), *Diritto, op. cit.*, p. 401 ss.
[20] Cfr. M. GAMBINI, *op.cit.*, p. 330.
[21] Sul punto, cfr. U. SALANITRO, *op.loc.ult.cit.*
[22] Cfr. A. AMIDEI, *La responsabilità da intelligenza artificiale tra product liability e sicurezza del prodotto*, in U. RUFFOLO (a cura di), *XXVI Lezioni*, *op.cit.*, p. 150, il quale parla del «dilemma del "*black box*"».
[23] Cfr. E. TROISI, AI e *GDPR*: l'*Automated Decision Making*, *la protezione dei dati e il diritto alla 'intellegibilità' dell'algoritmo*, consultabile *online* in *EJPLT*, 2019, p. 47 ss.
[24] Cfr. M. GAMBINI, *op.cit.*, p. 330.
[25] Cfr. G. CAPILLI, *I criteri di interpretazione della responsabilità*, in G. ALPA, (a cura di), *Diritto, op.cit,* p. 477.
[26] Cfr. U. RUFFOLO, *Intelligenza Artificiale, machine learning e responsabilità da algoritmo,* in *Giur.it.*, 2019, p. 1698; G. CAPILLI, *op.cit.*, p. 477.

l'*hardware* e provveda all'ideazione, alla progettazione ed alla programmazione del *software* di guida intelligente.

1. I "nuovi" danni algoritmici: quali modelli di responsabilità civile?

Una volta identificati i soggetti potenzialmente responsabili, secondo le circostanze del caso concreto, è d'uopo definire il regime di imputazione e la natura della responsabilità[27].

Molte delle situazioni descritte possono involvere rapporti contrattuali, come quello di vendita di prodotti, di lavoro, di assicurazione, di banca, di intermediazione finanziaria, di opera professionale e i soggetti lesi sono legittimati ad azionare rimedi contrattuali, per ottenere la riparazione dei danni algoritmici[28].

L'Unione europea è intervenuta in sede di contratti di fornitura di contenuti o servizi digitali, con la direttiva 2019/770/UE, recepita in Italia dal d.lg. 4 novembre 2021, n. 173 (artt. 135 *octies* ss., c.cons.), riconoscendo innovativamente al consumatore la legittimazione ad azionare i rimedi contrattuali che gli spettino, in caso di difetto di conformità o di mancata fornitura del servizio o del contenuto digitale, anche laddove il trasferimento dei propri dati personali rappresenti il "corrispettivo contrattuale" della prestazione fornita dall'operatore economico. In coordinamento con tale provvedimento, la direttiva 2019/771/UE[29], recepita dal d.lg., 4 novembre 2021, n. 170 (artt. 135 *bis* ss., c.cons.), detta la disciplina della vendita dei beni di consumo, da un lato, escludendone l'applicazione ai contratti di fornitura di un contenuto o di un servizio digitale, dall'altro, disponendone l'attuazione ai contenuti digitali o ai i servizi incorporati o interconnessi con i beni e che siano forniti con gli stessi, ai sensi del contratto di vendita, indipendentemente dal fatto che detti contenuti o servizi digitali siano somministrati dal venditore o da terzi (art. 3, 3° co.) [30]. La normativa prevede la responsabilità del

[27] Cfr. I. GIUFFRIDA, *Liability for AI Decision-Making: Some Legal and Ethical Considerations*, in *Fordham Law Review*, 2019, 88, 2, p. 443.

[28] Cfr. M. INFANTINO, *op.cit.*, par. 3. Nel caso, ad esempio, di un malfunzionamento di un prodotto intelligente, come un veicolo a guida autonoma, o di un macchinario industriale, il venditore del bene sarà contrattualmente responsabile nei confronti del suo acquirente e il datore di lavoro verso il lavoratore danneggiato. Nelle ipotesi di errori provocati, nell'elaborazione dei dati personali, da parte della banca o della società assicurativa che ledano la posizione dei loro clienti, costoro potranno agire in giudizio, ai fini del conseguimento del risarcimento del danno, in forza del contratto bancario oppure assicurativo. Alla stessa stregua, il paziente potrà citare in giudizio il medico che sbagli la diagnosi o il trattamento medico o farmacologico, affidandosi all'utilizzo dell'intelligenza artificiale, facendo valere l'inadempimento dell'obbligazione di prestazione d'opera professionale. Sulla responsabilità contrattuale, connessa all'uso dell'intelligenza artificiale, cfr. M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di intelligenza artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 333 ss.; A. MASSOLO, *Responsabilità civile e IA*, *ivi*, p. 373 ss.

[29] La direttiva modifica il regolamento (UE) 2017/2394 e la direttiva 2009/22/CE e abroga la direttiva 1999/44/CE.

[30] Le due direttive, nell'ambito della strategia per il mercato unico digitale, mirano al bilanciamento tra l'esigenza di promozione della competitività delle imprese e la necessità di garantire un elevato livello di protezione dei consumatori. Per un'attenta analisi delle rilevanti novità introdotte, cfr., *ex multis*, A. DE FRANCESCHI, *La vendita di beni con elementi digitali,* Napoli, 2019, *passim*; R. TORINO, G. CAPILLI, *Codice del consumo: le novità per i contratti di vendita e fornitura di beni digitali,* Torino, 2022, *passim*. Per un commento al recepimento della direttiva 2019/771/UE in Spagna, cfr. M. CASTILLA BAREA, Prologuista García Vicente, José Ramón, *La nueva regulación europea de la venta de bienes muebles a consumidores. Studio de la Directiva*

professionista, per qualsiasi difetto di conformità, sussistente al momento della consegna del bene e che emerga entro due anni, stabilendo i requisiti soggettivi e oggettivi di conformità che il bene deve rispettare. Il difetto potrà concernere altresì gli elementi digitali contenuti nel bene e sussisterà, qualora gli aggiornamenti dovuti siano carenti, viziati o installati in modo imperfetto. Il venditore dovrà garantirli anche per la sicurezza dei terzi, al fine di assicurare che i beni digitali continuino ad essere conformi per il periodo previsto nel contratto oppure nell'arco temporale che il consumatore possa attendersi ragionevolmente. In ogni modo, la normativa ha una valenza distinta da quella della responsabilità del produttore che si attua al di fuori del rapporto tra le parti contrattuali; infatti, gli obblighi del venditore verso l'acquirente del bene, malgrado siano calibrati sulla sicurezza dei terzi, non si declinano in doveri verso gli altri consociati[31].

Inoltre, assume preminente interesse la questione della gamma dei rimedi applicabili, nelle ipotesi di disfunzioni degli *smart contracts*[32].

Sotto il profilo della responsabilità extracontrattuale, entrano in gioco la responsabilità per danni da prodotto difettoso ed altri modelli.

In tale contesto, assume rilevanza centrale la direttiva comunitaria 85/374/CEE sulla responsabilità per danno da prodotti difettosi, ormai confluita, in Italia, nel Codice del Consumo (negli artt. 114 ss.)[33].

(UE) 2019/771 y su transposición por el Real Decreto-ley 7/2021, de 27 de abril, Cizur Menor (Navarre), Spagna, 2021, *passim*.

[31] Per tali osservazioni, cfr. U. SALANITRO, *op.cit.*, p. 1258 s.

[32] Con tale locuzione, si fa, per lo più, riferimento a contratti in cui l'adozione della tecnologia determina procedimenti di formazione semplificati, grazie a "*software* intelligenti" ovvero protocolli informatici, per mezzo dei quali gli elementi di un rapporto contrattuale vengono formalizzati e tradotti in un codice crittografico. In sostanza, tali *software* sono in grado di eseguire autonomamente i termini dell'accordo contrattuale, codificati al loro interno, qualora siano soddisfatte le condizioni ivi definite *ex ante* (cfr. D. DI SABATO, *Diritto e new economy*, Napoli, 2020, p. 158). Il programma elettronico compie, cioè, in automatico, valutazioni relative alla sussistenza dei presupposti, delle circostanze ovvero delle condizioni per l'esecuzione del rapporto contrattuale, finendo, in tal guisa, con il sottrarre alle parti la scelta in ordine al 'se' ed al 'come' della stessa (cfr. F. DI GIOVANNI, *Attività contrattuale e intelligenza artificiale*, in *Giur.it.*, 2019, p.1697; D. DI SABATO, *op.cit.*, p. 158). Tali contratti sono ampiamente usati nel settore bancario, finanziario e assicurativo e rendono più agevole l'attuazione degli interessi delle parti contraenti, visto che costituiscono un regolamento contrattuale flessibile, idoneo ad incidere, in modo diretto, nelle vicende negoziali con programmi che, sostituendosi quasi del tutto ai contraenti umani, gestiscono la formazione, la fase esecutiva e le sopravvenienze del contratto. Cfr. D. DI SABATO, *op.cit.*, p. 156; I. MARTONE, Gli *smart contracts. Fenomenologia e funzioni*, Napoli, 2022, p. 27 ss. La letteratura sugli *smart contracts* è vastissima. *Ex multis*, cfr. M. MAUGERI, *Smart contracts e disciplina dei contratti*, Bologna 2021, *passim*. Per altro verso, tuttavia, la diffusione della contrattualizzazione algoritmica pone problematiche complesse, tra le quali, la sussistenza del rischio che l'algoritmo, nel tradurre in termini informatici la volontà delle parti che definiscono le regole del rapporto contrattuale, non ne operi una corretta trasposizione. In queste ipotesi, nasce il dubbio della conciliabilità di tale figura con i rimedi caducatori o conservativi tradizionali e ci si domanda sulla base di quali presupposti siano attivabili i rimedi restitutori e risarcitori. Cfr. I. MARTONE, *op.cit.*, p. 170 ss.

[33] La letteratura giuridica sulla disciplina della responsabilità per danno da prodotto difettoso è sconfinata. *Ex multis*, cfr. G. SALVI, *Responsabilità extracontrattuale*, in *Enc.dir.*, XXIX, Milano, 1988, p. 1229; A. GORASSINI, *Contributo per un sistema della responsabilità del produttore*, Milano, 1990, *passim*; G. ALPA, U. CARNEVALI, F. DI GIOVANNI, G. GHIDINI, U. RUFFOLO, C.M VERARDI (a cura di), *La responsabilità per danno da prodotti difettosi*, Milano, 1990, *passim*; G. PONZANELLI, *Responsabilità del produttore*, in *Riv.dir.civ.*, 1995, 2, p. 215 ss.; ID., *La responsabilità civile. Profili di diritto comparato*, Bologna, 1992, p. 112; G. ALPA, M. BIN, P. CENDON, *La responsabilità del produttore*, in *Trattato di diritto commerciale e di diritto pubblico dell'economia* (diretto da F. GALGANO), XIII, Padova, 1989, *passim*; C. CASTRONOVO, *Danno da prodotti (dir. it. e straniero*), in *Enc.giur.*, X, Roma, 1995, 11; M. FRANZONI, *Dieci anni di responsabilità del produttore*, in *Danno e resp.*, 1998, p. 823; P.G. MONATERI, *Illecito e responsabilità civile*, in *Trattato di diritto privato* (diretto da M. BESSONE), Torino, X, 2, 2002, p. 257; L. CABELLA PISU, *Ombre e luci nella responsabilità del produttore*, in *Contratto e impresa Europa*, 2008, p. 617 ss.; A. CORDIANO, commento sub art. 114, in E. CAPOBIANCO, G. PERLINGIERI (a cura di) *Codice del consumo*

Si inizi col dire che la direttiva si apre con il principio generale, secondo il quale il "produttore" europeo è responsabile del danno cagionato dal difetto del prodotto.

Il "prodotto" è definito, nel Codice del Consumo, in maniera ampia, dall'art. 3, 1 °co., lett. d), e), (la cui definizione è ripresa dall'art. 103 c.cons., in tema di sicurezza generale dei prodotti); oltre che dall'art. 115 c.cons., che si trova in rapporto di specialità rispetto alla definizione più ampia e prevede che è "prodotto" "ogni bene mobile, anche se incorporato in altro bene mobile o immobile".

La nozione di "produttore" è estesa e include il fabbricante della componente ed il fornitore della materia prima. L'art. 121 c.cons. statuisce la responsabilità solidale di tutti gli operatori della linea di produzione, salvo il diritto di rivalsa esperibile, nell'ambito dei coobbligati.

La direttiva ha introdotto un regime di responsabilità oggettiva, dato che prescinde dall'accertamento della colpa; il danneggiato deve provare il danno effettivamente subito, il difetto del prodotto e il nesso di causalità tra difetto e danno[34].

Il criterio di imputazione si fonda sul rischio di immissione del prodotto nel mercato e sulla nozione di difetto[35].

L'art. 6 della direttiva e l'art. 117, c.cons., definiscono la "difettosità" del prodotto, con una clausola aperta alla molteplicità dei modi in cui può estrinsecarsi, in termini di mancanza di sicurezza, consistente nella difformità tra le condizioni di sicurezza concretamente offerte dal prodotto e quelle che, dallo stesso, è legittimo attendersi «tenendo conto delle circostanze», tra le quali: il modo in cui sia stato messo in circolazione, la sua presentazione, le sue caratteristiche palesi, le istruzioni o le avvertenze fornite; l'uso per il quale può essere ragionevolmente destinato e i comportamenti che, in relazione ad esso, si possono ragionevolmente prevedere; il tempo in cui è stato messo in circolazione[36]. La nozione di difetto non coincide con un vizio intrinseco del bene; ma consiste in un "giudizio di valore" che ha ad oggetto la corrispondenza del rischio attinente al prodotto (in base alle circostanze menzionate) alle legittime aspettative di sicurezza degli utenti[37]. In sostanza, sussiste la regola

---

annotato con la dottrina e la giurisprudenza, Napoli, 2009, p. 645; M. FRANZONI, *L'illecito*, in *Trattato della responsabilità civile*, seconda edizione, I, Milano, 2010, p 661 ss.; A. THIENE, *commento sub art. 114 cod. cons.*, in *Commentario breve al Diritto dei consumatori* (diretto da G. De Cristofaro, A. Zaccaria), Padova, 2010, p. 767; R. PARDOLESI, G. PONZANELLI, *Speciale 2012, "I 25 anni di products liability"*, *Danno e resp.*, 2012, *passim*.

[34] La direttiva si applica ai danni causati dalla morte o dalle lesioni personali oppure a quelli provocati alla proprietà.

[35] Cfr. G. CAPILLI, *op.cit.*, p. 471. La normativa si inserisce nell'ambito di uno spazio europeo di riferimento, nel quale rientrano provvedimenti che sono espressione dell'attuazione del principio di precauzione, quale strumento per gestire l'incertezza, facendo sì che la responsabilità sia traslata ai soggetti produttori. Cfr. U. IZZO, *La precauzione nella responsabilità civile. Analisi di un concetto sul tema del danno da contagio per via trasfusionale,* Padova, 2004, p. 1.

[36] Sul tema, *ex multis*, cfr. U. CARNEVALI, *La responsabilità del produttore*, Milano, 1974, p. 150 ss.; F. CAFAGGI, *La nozione di difetto e il ruolo dell'informazione. Per l'adozione di un modello dinamico-relazionale di difetto in una prospettiva di riforma*, in *Riv. critica dir.priv.*, 1995, p. 450 ss.; M. FRANZONI, *Responsabilità per colpa e responsabilità oggettiva*, in S. PAGLIANTINI, E. QUADRI e D. SINESIO (a cura di), *Scritti in onore di Marco Comporti,* Milano, 2008, p. 1322 ss.

[37] Sul punto, cfr. G. STELLA, *Causa ignota del danno derivante dall'uso del prodotto e responsabilità del produttore per prodotto difettoso*, in *Resp. civ. e prev.*, 2017, p. 1444 ss.; G.F. SIMONINI, *L'approccio olistico nel danno da prodotto*, in *Danno e resp.*, 2018, p. 137 ss.; G. PONZANELLI, *Responsabilità del produttore*, *op.cit.*, p. 220 ss. Tradizionalmente si distinguono quattro tipologie di difetti: i difetti di fabbricazione o di costruzione;

che non può essere superato "il livello accettabile di rischio" che il prodotto diffonde tra il pubblico, da individuarsi in riferimento al momento della sua immissione in commercio[38].

Ci domanda se tale normativa sia idonea a governare i "nuovi" rischi, derivanti dall'uso di sofisticati prodotti delle tecnologie digitali, che presentano caratteristiche molto diverse dai beni per i quali la direttiva è stata concepita negli anni Ottanta. Sorgono, difatti, difficoltà a collegare i concetti di "prodotto", di "produttore", oltre che quello di "difetto", con le questioni relative al suo accertamento, ad alcuni *smart devices*[39].

Anzitutto, si rilevi[40] che i nuovi beni delle tecnologie digitali, alle volte, sono composti da un insieme non distinguibile di cose materiali (manufatti, sensori, *hardware*) e di elementi immateriali (*software*, applicazioni, algoritmi, dati personali e non), oltre che da servizi (quali, ad esempio, la raccolta, l'elaborazione, l'analisi di dati, servizi di connettività, etc.). Invero, la componente immateriale e quella logico-informatica, che impiega e produce dati, assumono il maggior peso sia sotto il profilo economico-tecnologico, sia quanto ai rischi che possono provocare. Tali prodotti possono, poi, subire modificazioni, nel corso del loro utilizzo, a causa dell'aggiunta di *software*, di applicazioni oppure per via di estensioni e di aggiornamenti della componente digitale. Tali modifiche sono progettate dallo stesso produttore come essenziali per il funzionamento del prodotto e sono fornite da quest'ultimo e, più di frequente, da terzi per conto del primo, dopo l'immissione del bene in circolazione nel mercato.

Ancora, vi sono i prodotti intelligenti in grado di prendere decisioni autonome, come i veicoli autonomi e i *robot* chirurgici, e talvolta anche capaci di apprendimento, con le descritte conseguenze che ne derivano.

Ebbene, la questione della qualificabilità di tali beni come "prodotti" non ha rilevanza pratica, quando il contenuto digitale sia incorporato in un bene *hardware* più complesso, visto che, in tal caso, il suo fabbricante sarà certamente chiamato a rispondere verso il consumatore danneggiato, sebbene risulti difettosa la mera componente "*software*"[41]. Quesiti più complessi sorgono per i casi in cui un contenuto digitale venga venduto non insieme ad un *hardware* più articolato che lo incorpori, ma in via separata. Precipuamente per l'intelligenza artificiale, la problematica è aggravata, ancora di più, dalla rilevanza che gli algoritmi di *machine learning* ricoprono nel funzionamento del *software* (rispetto ai quali i primi sono ancora più immateriali), soprattutto

---

i difetti di progettazione, consistenti nella difformità di *design* dagli *standard* che possono esigersi, in concreto, dal produttore; la mancanza o la carenza di informazioni circa il corretto funzionamento del prodotto; i difetti da sviluppo, ossia i danni che, allo stato attuale della scienza e della tecnica, risultano del tutto imprevedibili.

[38] Cfr. R. MONTINARO, *op.cit.*, p. 360.

[39] Cfr. ID., *op.cit.*, p. 350; L. COPPINI, *op.cit.*, p. 727 ss. Per un'attenta disamina della questione dell'idoneità della disciplina vigente a regolamentare i danni causati dai *robot* intelligenti, cfr. I. ZURITA MARTÍN, *op.cit.*, *passim*; A. BERTOLINI, *Artificial Intelligence and Civil Liability,* in *Study Requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies*, Bruxelles, 2020, p. 56; U. RUFFOLO, *Responsabilità da produzione*, *op.cit.,* pp. 131 ss.; G. CAPILLI, *op.cit.*, pp. 471 ss.; A. AMIDEI, *op.ult.cit.*, p. 152 ss.

[40] Per le osservazioni che seguono, cfr. R. MONTINARO, *op.cit.*, pp. 350, 354.

[41] Sul punto e per le riflessioni che seguono, cfr. A. AMIDEI, *op.ult.cit.*, p. 153.

tenendo conto del fatto che sovente i loro autori sono diversi, rispetto a quelli che realizzano le altre componenti del prodotto.

Potrebbe, in verità, risultare difficile qualificare l'algoritmo come "prodotto", ai sensi della Direttiva, qualora, considerando che lo stesso è destinato, per sua natura, ad essere incorporato nel "prodotto" intelligente, lo si intenda come un mero progetto, una mera idea o formula, ovvero un'entità non ancora adeguata a divenire una "componente" fisica di un prodotto o di parte di esso (quali il *software* di cui sia munito). Potrebbe succedere che l'"autore" dell'algoritmo sia un soggetto diverso dal produttore dello *smart product*[42] e, secondo tale ricostruzione, il primo si configurerebbe come un semplice "fornitore" di idee o progetti e sarebbe problematico immaginare una sua responsabilità autonoma[43].

Sotto un diverso angolo di visuale, che si condivide, l'algoritmo può essere inteso quale creazione intellettuale, consistente «nella mera descrizione di un procedimento, in un pugno di *bit* o in una semplice formula matematica» e, quindi, come "componente" immateriale, caratterizzante il sistema intelligente[44].

In quest'ottica, si possono contemplare, quali produttori di una "componente" dell'entità artificiale intelligente, non solo il produttore del complessivo *software* che lo incorpori, ma anche l'ideatore-autore dei codici di programmazione, quello dell'algoritmo d'autoapprendimento o quello di altri apporti che condizionino i comportamenti del prodotto [45]. L'inventore dell'algoritmo dovrebbe, di conseguenza, essere responsabilizzato sia sul piano negoziale verso il suo committente, sia, sul piano aquiliano, verso i terzi danneggiati dal sistema tecnologico, al quale abbia attribuito il potere di apprendere e di indirizzare conseguentemente il proprio comportamento. Allora, quando l'intelligenza artificiale *self-learning*, nata ''buona'', traligni, in seguito, in *malware* (*malicious software*), potrebbe rinvenirsi la causa della distorsione della macchina, rispetto a quello che dovrebbe essere il risultato atteso, nella mancata introduzione nell'algoritmo di "blocchi", in grado di impedire le future "deviazioni" dell'intelligenza artificiale o, ad ogni modo, del *device* che la incorpori. In tale ipotesi, la "componente" algoritmo di apprendimento sarà "difettosa" e la responsabilità per il danno determinato dal difetto sarà imputabile all'inventore dell'algoritmo e sarà autonoma e distinta da quella del produttore del dispositivo che lo incorpori. La responsabilità del primo concorrerà con quella di quest'ultimo, in linea con l'approccio della direttiva europea che prevede la responsabilità cumulativa e non alternativa dei soggetti facenti parte della catena produttiva, con l'obiettivo di offrire effettiva tutela ai consumatori[46].

---

[42] Cfr. A. AMIDEI, *op.ult.cit.*, p. 150, il quale definisce l'algoritmo quale «mera linea di codice».

[43] In posizione critica verso tale impostazione cfr. U. RUFFOLO, *Intelligenza Artificiale, machine learning e responsabilità da algoritmo*, in *Giur.it.*, 2019, p. 1691.

[44] Di fatto, l'algoritmo, pur non comparendo quale componente distinta del prodotto finale, attribuisce "l'anima" al *software* di un'intelligenza artificiale complessa, incarnata o meno in entità robotica. Cfr. U. RUFFOLO, *op.loc.ult.cit.* Conformemente R. MONTINARO, *op.cit.*, p. 359.

[45] Cfr. U. RUFFOLO, *La responsabilità da produzione*, *op.cit.*, p. 134.

[46] È questa la ricostruzione di U. RUFFOLO, *Intelligenza Artificiale*, *machine learning*, *op.cit.*, p. 1691, il quale sottolinea che un ulteriore aspetto da valutare è che i danni provenienti dai sistemi di intelligenza artificiale *self-learning* potrebbero derivare da *bias*, imputabili agli "insegnamenti" ricevuti direttamente o indirettamente dall'"addestratore". In tale ipotesi, si dovrebbe considerare la responsabilità di quest'ultimo

Secondariamente, la direttiva presenta l'ulteriore criticità di "cristallizzare" il "difetto", al momento della messa in circolazione del prodotto.

L'applicazione rigorosa della disciplina attualmente vigente implicherebbe, *in primis*, che il "produttore" risponda per i difetti del prodotto o delle sue componenti, unicamente quando sussistano al tempo della messa in circolazione del bene, ancorché si manifestino successivamente. Costui potrebbe, quindi, invocare l'esimente del "difetto sopravvenuto", quando il danno sia dovuto ad una condotta anomala ed imprevedibile del prodotto, conseguente al processo di *self learning*, argomentando che la deviazione dovrebbe essere collegabile ad un difetto "iniziale", quale, ad esempio, una propensione anomala del meccanismo di autoapprendimento a determinare quel tipo di comportamenti dannosi.

In secondo luogo, il produttore potrebbe far valere l'esimente del c.d. rischio da sviluppo, attualmente opzionale a livello europeo e vigente nel nostro ordinamento, escludendo la qualificazione di "difetto" per l'anomalia dello *smart device* non prevedibile, allo stato delle oggettive conoscenze tecnico-scientifiche del tempo in cui abbia messo in circolazione il prodotto[47].

In aggiunta, la direttiva non precisa chi sia il responsabile, quando un'impresa modifichi un prodotto che sia già immesso sul mercato o qualora sia importato dal consumatore da un Paese che non sia uno Stato membro dell'Unione europea. Tale circostanza non garantisce la protezione dei consumatori e rende complesso alle imprese misurare i rischi della commercializzazione di prodotti innovativi[48].

Vieppiù, la complessità, l'autonomia, l'opacità e l'imprevedibilità dell'intelligenza artificiale si riverbera negativamente sulla posizione del danneggiato, sotto il profilo dell'onere della prova del nesso di causalità tra l'operato del prodotto digitale e l'evento dannoso.

Ordunque, le Istituzioni europee, nella consapevolezza che la direttiva ha dimostrato, per quasi quarant'anni, di essere uno strumento normativo efficace, hanno avanzato la necessità della sua modernizzazione, per adeguarla al mondo digitale[49]. Per tali ragioni, è da salutare con favore l'iniziativa della Commissione europea che, il 28 settembre 2022, ha presentato la proposta per una direttiva del Parlamento europeo e del Consiglio sulla responsabilità per danni da prodotti difettosi[50], di revisione della disciplina attualmente vigente, che costituirà oggetto di analisi *infra*.

La proposta di revisione dovrà essere interpretata, in via sistematica, unitamente alle due proposte di regolamento, presentate, nel 2021, dalla

---

quantomeno concorrente con quella del produttore di un'entità artificiale intelligente e/o con quella dell'ideatore dell'algoritmo, se distinto da quest'ultimo. Cfr. U. RUFFOLO, *op.ult.cit.*, p. 1698 s.

[47] Per tali riflessioni, cfr. U. SALANITRO, *op.cit.*, p. 1261 s., il quale richiama le preoccupazioni della Commissione europea, esposte nella Relazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e responsabilità, 19 febbraio 2020, (COM (2020), 64 final), p. 17.

[48] Cfr. D. MAISTO, *Nuove norme europee sulla responsabilità per danno da prodotti difettosi anche derivanti da AI*, consultabile *online*, sul sito in https://quifinanza.it/innovazione/

[49] Cfr. il punto 8 della Risoluzione del Parlamento europeo del 20 ottobre 2020 «recante raccomandazioni alla Commissione sul regime di responsabilità civile per intelligenza artificiale» (2020/2014(INL))) e la Relazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e responsabilità, cit., pp. 15 ss.

[50] Bruxelles, 28.9.2022 COM(2022) 495 final 2022/0302 (COD).

Commissione europea, relative, l'una, alla sicurezza generale dei prodotti e l'altra alla sicurezza delle macchine. Si puntualizzi che la Direttiva 2001/95/CE sulla sicurezza generale dei prodotti si pone in termini complementari a quella sulla responsabilità per danno da prodotto difettoso, statuendo i requisiti da rispettare per la messa in commercio di beni**,** fissando la tipologia di informazioni da fornire ai consumatori e regolando l'apposizione del marchio CE. La Direttiva c.d. Macchine 2006/42/CE rappresenta la regolamentazione settoriale di riferimento, in merito alla produzione e alla messa in commercio di prodotti automatizzati, dato che definisce i requisiti essenziali, in ambito di sicurezza e di salute pubblica, ai quali devono rispondere le macchine, durante la fase di progettazione, fabbricazione e funzionamento, prima della loro immissione sul mercato. Entrambe le direttive sono state emanate in un momento in cui i nuovi prodotti tecnologici ed i dispositivi correlati erano rari e tecnicamente non avanzati, come allo stato attuale; per tale motivo, costituiscono oggetto di modernizzazione[51]. Il 21 aprile 2021 è stato pubblicato il testo della Proposta di Regolamento del Parlamento europeo e del Consiglio sui prodotti macchina che, nei prossimi mesi, una volta terminato l'*iter* di approvazione, andrà a sostituire la direttiva Macchine 2006/42/CE [52]. Il 30 giugno 2021 è stato pubblicato il testo della proposta di regolamento del Parlamento europeo e del Consiglio, relativo alla sicurezza generale dei prodotti che modifica il regolamento 1025/2012/UE e che abroga la direttiva 87/357/CEE e la direttiva 2001/95/CE[53].

Detto ciò, ci si interroga su quali siano i modelli di responsabilità civile, delineati dall'Unione Europea, per far fronte alle ipotesi in cui il paradigma della responsabilità da danno da prodotto difettoso non offra risposte esaurienti ai "nuovi danni" provocati dalle tecnologie digitali emergenti[54].

Si vaglieranno le soluzioni offerte dai provvedimenti europei *in fieri,* ponendo in evidenza che le Istituzioni europee hanno predisposto un «sistema multilivello» di responsabilità [55] che prevede sia *liability rules*, norme sulla responsabilità civile, sia "*permittance or prohibition" rules*, volte a guidare, *ex ante*, i comportamenti dei vari soggetti, coinvolti nella "catena di valore" delle entità artificiali intelligenti, in conformità al principio di *accountability*.

Si sottolineeranno i punti di forza e le criticità dell'approccio europeo.

[51] Sull'esigenza di modernizzazione della disciplina attualmente vigente sulla sicurezza dei prodotti, cfr. I. ZURITA MARTÍN, *Las propuestas de reforma legislativa del Libro Blanco europeo sobre inteligencia artificial en materia de seguridad y responsabilidad civil*, in *Actualidad Jurídica Iberoamericana*, 2021, n. 4, pp. 452 ss.
[52] Bruxelles, 21.4.2021. COM (2021) 202 final. 2021/0105(COD).
[53] Bruxelles, 30.6.2021COM (2021) 346 final, 2021/0170(COD).
[54] Come noto, la letteratura giuridica ha ricondotto i nuovi danni nell'alveo degli schemi della responsabilità civile vigenti nel nostro ordinamento giuridico. Per un'analisi delle più rilevanti ricostruzioni dottrinali, mi si consenta di rinviare a G. D'ALFONSO, *Il regime della responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"*, consultabile *online* in *EJPLT*, 2022, 1, pp. 101 ss.
[55] La locuzione è di G. COMANDÉ, *Multilayered (Accountable) Liability for Artificial Intelligence*, in S. LOHSS, R. SCHULZE, D. STAUDENMAYER (a cura di), *Liability for Artificial Intelligence and the Internet of Things*, Baden-Baden, 2019, p. 178 ss.

2.1. Le questioni affrontate dal legislatore europeo. L'individuazione del soggetto responsabile nell'ambito della "catena di valore" del sistema digitale.

In via preliminare, si precisi che, a partire dalla Risoluzione del Parlamento europeo del 16 febbraio 2017, «recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica», i provvedimenti di *soft* e di *hard law* sottolineano che l'Unione Europea si prefigge di coniugare la promozione dell'innovazione tecnologica con le esigenze di garantire la sicurezza e l'affidabilità dei prodotti e dei servizi digitali e di apprestare una tutela effettiva dei diritti e delle libertà fondamentali dei destinatari dei comportamenti e delle decisioni dei sistemi intelligenti[56].

Sin dai primi interventi, i provvedimenti adottati dalle Istituzioni Europee confluiscono nel dare attuazione alla linea giuspolitica, per la quale devono essere i diritti fondamentali ed i valori europei a guidare lo sviluppo del mercato e non viceversa[57].

Nell'apprestare un efficace complesso di tutele, si perseguono due obiettivi: evitare che l'utilizzo di tecnologie digitali possa implicare una diminuzione di sicurezza e di responsabilità rispetto a quella tradizionale (c.d. equivalenza funzionale); allocare i danni nel modo più idoneo, in capo al soggetto che sia meglio in grado di minimizzarli[58].

Ciò premesso, si indagherà sulla posizione assunta dalle Istituzioni Europee, in relazione a taluni profili critici.

Il primo aspetto da analizzare attiene all'individuazione del soggetto responsabile, nell'ambito della "catena di valore" dei sistemi intelligenti.

Si parta dalla considerazione che la presenza di tecniche sempre più sofisticate, alle quali collaborino molteplici attori (principalmente, il progettista, il programmatore, l'ideatore e l'addestratore dell'algoritmo; il produttore, il distributore; l'utilizzatore del sistema digitale), oltre che il sovrapporsi dei loro ruoli e delle loro competenze (nell'ideazione, nella progettazione, nello sviluppo, nella diffusione ed utilizzazione di tali sistemi e nell'impiego di algoritmi per l'autoapprendimento) possono rendere complesso stabilire la progressione della serie di nessi causali ed incerta l'identificazione dei soggetti danneggianti, come pure l'individuazione dei relativi criteri di imputazione della responsabilità[59].

---

[56] Cfr. A. PAJNO, M. BASSINI, G. DE GREGORIO, M. MACCHIA, F.P. PATTI, O. POLLICINO, S. QUATTROCOLO, D. SIMEOLI, P. SIRENA, *AI: profili giuridici. Intelligenza artificiale: criticità emergenti e sfide per il giurista*, consultabile *online* sul sito www.biodiritto.org, p. 2. Per un'articolata e puntuale rassegna degli atti di *soft* ed *hard law*, cfr. G.T. ELMI, S. MARCHIAFAVA, *Sviluppi recenti in tema di intelligenza artificiale e diritto: una rassegna di legislazione, giurisprudenza e dottrina*, in Riv.it. informatica e diritto, 2022, n. 2.

[57] Cfr. G. RESTA, *Cosa c'è di 'europeo' nella Proposta di Regolamento UE sull'intelligenza artificiale*?, *Dir.inf. e informatica*, 2022, par. 3, consultabile *online* sul sito http://dejure.it

[58] Cfr. Relazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e responsabilità, cit., pp. 19, 22.

[59] Cfr. M. GAMBINI, *op.cit.*, p. 333. La dottrina si interroga se la circostanza che l'algoritmo abbia appreso in maniera autonoma, in modo non prevedibile, interrompa il nesso di causalità tra l'istruzione iniziale, conferita alla macchina dall'operatore economico, ed il risultato finale dell'evento dannoso prodotto dalla condotta della stessa, al di fuori del controllo e dell'intervento umano. Come pure, in situazioni di incertezza probatoria, ci si domanda non solo chi sia il responsabile, tra i vari soggetti coinvolti nell'operatività

Addirittura, taluni attori, in maniera progressiva, potrebbero acquisire il carattere dell'anonimato, con la conseguenza che potrebbe ricorrere il pericolo dei c.dd. danni anonimi[60].

Per di più, il numero dei soggetti responsabili potrebbe risultare tanto elevato da rendere impossibile, se non eccessivamente oneroso, per il soggetto leso, agire in giudizio per ottenere il ristoro: i costi giudiziari potrebbero essere troppo ingenti, potrebbero porsi problemi di giurisdizione, di notifiche da compiere e le parti entrerebbero in conflitto, esercitando domande trasversali e di manleva, per fare in modo che la responsabilità gravi sugli altri[61].

A fronte di tali difficoltà, il legislatore ha il compito di garantire ai soggetti danneggiati la possibilità effettiva di «raggiungere» il responsabile, senza dover affrontare difficoltà insormontabili[62]. In particolar modo, quando il problema sussista nella circostanza che l'evento dannoso è stato causato dal concorso delle condotte di più operatori economici, seppur indipendenti tra loro, è essenziale un modello costruito su responsabilità concorrenti che spinga, a monte, i diversi attori dei processi algoritmici a minimizzarne i rischi e a prevenire i pericoli di pregiudizio e, a valle, garantisca un'equa distribuzione degli oneri economici del risarcimento del danno tra i soggetti coinvolti nell'illecito[63].

In tale contesto, la responsabilità non può che essere solidale e «multipla» e gravare in capo a coloro che siano coinvolti nella "catena di valore", ravvisandosi l'elemento unificante nella circostanza che tutti cooperino per il raggiungimento di un obiettivo comune, consistente nel progettare, programmare e produrre un'intelligenza artificiale e le sue componenti[64]. La solidarietà passiva rafforzerà la posizione del creditore, conferendogli la possibilità di scegliere il corresponsabile più solvibile, impedendo che il danno rimanga anonimo[65]; il *solvens*, a sua volta, avvierà l'azione di regresso verso gli altri corresponsabili, in misura proporzionale alla responsabilità di ciascuno di essi.

Il giudice dovrà interpretare, in concreto, la relazione sussistente tra l'ideatore o il programmatore dell'algoritmo, il produttore del bene o il prestatore del servizio che lo incorpori ed, eventualmente, i soggetti terzi, rispetto al processo di ideazione, programmazione e sviluppo delle applicazioni intelligenti (quali il proprietario o l'utilizzatore, il gestore di rete e i potenziali

---

dell'algoritmo, ma anche se siano responsabili coloro che, seppure non abbiamo determinato l'evento che abbia provocato il danno, avrebbero potuto impedirlo Cfr. M. INFANTINO, *op.cit.*, nota 44.

[60] Cfr. D. DI SABATO, *Sistemi riparatori e risarcitori*, in P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico*, *op.cit.*, p. 341. A titolo esplicativo, si pensi che la maggior parte degli algoritmi opera, grazie al contributo ed al coordinamento di più fattori. I codici sono redatti sovente da una pluralità di autori, quali imprese *high-tech*, sviluppatori *in house*, piccole *start-up* e contributori autonomi, che spesso lavorano senza coordinarsi, ciascuno scrivendo una parte del codice. Sul punto cfr. M. INFANTINO, *op.cit.*, par. 4.

[61] Cfr. G. CAPILLI, *op.cit.,* p. 477.

[62] Cfr. V. DI GREGORIO, *op.cit.*, p. 61.

[63] Cfr. M. GAMBINI, *op.cit.*, p. 332.

[64] Cfr. G. COMANDÉ, *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi Giuridica dell'Economia*, 2019, p. 174 che richiama la teoria dell'impresa comune, avanzata da D.C.VLADECK, *Machines without Principals: Liability Rules and Artificial Intelligence*, in *Wash.L.Prev.*, 89, 117, 2014, p. 149.

[65] Cfr. P. PERLINGIERI, *Presentazione*, in P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico, op.cit,* p. X.

aggressori esterni)[66]; per identificare, successivamente, l'effettivo ruolo da loro svolto sia singolarmente, sia in forma associata e porre sempre la dovuta attenzione «al *cui prodest*, secondo il broccardo *ibi commoda ubi incommoda*!»[67].

La scelta tra tali soggetti e l'eventuale configurabilità di una loro responsabilità cumulativa discenderà dalle diverse abilità delle applicazioni, dall'identificazione del compito svolto da ciascuno di essi, tanto più dalle circostanze del caso concreto[68]. In realtà, pur dovendosi riconoscere un ruolo centrale all'ideatore dell'algoritmo, la sua responsabilità deve essere cumulativa con quella del produttore del dispositivo che lo incorpori e con quella del suo utilizzatore/proprietario/custode. A sua volta, la responsabilità di quest'ultimo non potrà essere esclusa, sostenendo che potrebbe non avere le competenze per comprendere o correggere il funzionamento dell'algoritmo, considerato che, in ogni caso, se ne assume il rischio nel momento stesso in cui decide di acquistare ovvero adoperare il bene o il servizio in cui esso è incorporato. In caso contrario, ne deriverebbe una riduzione di tutela del soggetto leso, per il quale potrebbe essere complicato acquisire le informazioni essenziali, per agire in giudizio contro l'ideatore o il programmatore dell'algoritmo.

L'autorità giudiziaria dovrà sicuramente vagliare e graduare, di volta in volta, le responsabilità dei molteplici soggetti, compensando l'eventuale abbassamento del livello di responsabilità dei proprietari/utilizzatori/custodi del prodotto digitale con il rafforzamento della responsabilità del suo produttore e/o dell'ideatore dell'algoritmo[69].

In merito al profilo dei criteri di imputazione della responsabilità, è condivisibile l'orientamento dell'*Expert Group on Liability and New Technologies*[70]. Il Gruppo di esperti ha capovolto la posizione espressa dal Parlamento europeo[71] che, al fine di colmare i cc.dd. "vuoti di responsabilità", sollevati dal diffondersi delle tecnologie emergenti, aveva preferito l'elaborazione di nuove categorie e di nuove norme, proponendo, come possibili soluzioni normative, due modelli alternativi di attribuzione di responsabilità: quello della responsabilità oggettiva e quello della gestione dei rischi, da riferire, quest'ultimo, al soggetto che, tra i numerosi potenzialmente coinvolti nel verificarsi del danno, sia quello causalmente «più vicino al prodotto», a seconda del malfunzionamento che si verifichi in concreto e sia, pertanto, in grado di minimizzare i rischi e di affrontare l'impatto negativo. A differenza del Parlamento europeo, il Gruppo di esperti ha dichiarato che tali due approcci debbono essere complementari nell'attribuzione della responsabilità, soprattutto nei casi in cui l'utilizzo della tecnologia potrebbe determinare un aumento dei rischi di danno. Si è affermato che, in conformità

---

[66] Cfr. M. GAMBINI, *op.loc.ult.cit.*

[67] Cfr. P. PERLINGIERI, *Relazione conclusiva*, in. P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico, op.cit.*, p. 387.

[68] Per le notazioni che seguono cfr. M. GAMBINI, *op.cit.*, p. 332 s.

[69] Cfr. U. SALANITRO, *op.cit.*, p. 1266.

[70] Nel parere dal titolo "*Liability for Artificial intelligence and other emerging digital technologies. Report from the Expert Group on Liability and New Technologies – New Technologies Formation, European Union"*, pubblicato a maggio del 2019, punti 5-12, p. 25 ss.

[71] Nella Risoluzione del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica.

ai principi di giusta ed efficiente allocazione dei danni, si dovrà imputare la responsabilità oggettiva (a prescindere dall'accertamento della sussistenza di un comportamento colposo) al soggetto che gestisca e controlli il rischio che possa scaturire dall'immissione nel mercato del sistema intelligente e che benefici dell'operazione. Secondo tale punto di vista, la gestione del rischio rappresenta uno dei possibili criteri di imputazione della responsabilità oggettiva che sussisterà quand'anche l'impresa abbia adottato tutte le precauzioni obbligatorie, ma vi sia un rischio "residuo", connesso al tipo di attività svolta, che graverà sul soggetto che sia in condizione di sopportare i costi della collettività[72].

Si è altresì chiarito che l'imputazione della responsabilità per colpa può operare sulla base del presupposto che siano stabiliti i criteri normativi di riferimento, al fine di verificare se la condotta dei soggetti, coinvolti nella gestione delle entità artificiali intelligenti, sia stata diligente.

Si è, tanto più, sostenuta la possibile coesistenza di diverse forme di imputazione della responsabilità.

Il Gruppo di esperti è anche intervenuto sulla questione se l'imprevedibilità dei rischi connessi all'impiego delle tecnologie digitali debba condurre all'imposizione di una polizza assicurativa in capo agli operatori economici del settore. Si è esclusa l'opportunità di prescrivere l'assicurazione obbligatoria per tutti gli *smart devices*, valutando che debba essere adottata unicamente nei casi in cui l'evento dannoso sia prevedibile, calcolabile e quantificabile in somme che potrebbero condurre all'insolvenza del soggetto danneggiante, sia che debba rispondere per responsabilità oggettiva, sia per colpa. Contemporaneamente si è prospettata la possibile istituzione di fondi di compensazione, che troverebbero applicazione nei soli settori sprovvisti di assicurazione obbligatoria[73].

2.2. (segue) La probatio "diabolica" del nesso di causalità tra l'operato del sistema intelligente e l'evento dannoso.

Il secondo profilo riguarda le difficoltà che il ricorrente dovrà affrontare nel costituire la prova del nesso di causalità tra l'operato del sistema ad alta complessità tecnologica e l'evento dannoso.

La complessità e l'opacità tecnica che caratterizza i codici sottostanti agli algoritmi rende problematica l'identificazione della causa del pregiudizio: non è facile capire se derivi da un difetto del codice, dalla sua interazione con altri prodotti intelligenti, dalla qualità dei dati e delle istruzioni ricevute dall'algoritmo o dal modo in cui esso sia stato usato[74]. Gli ostacoli alla

[72] Cfr. V. DI GREGORIO, *op.cit*, p. 62.

[73] Sul punto, cfr. U. RICCIARDELLI, *Automazione self-learning e responsabilità civile: note a margine di una riflessione europea*, consultabile *online* sul sito https://rivista.camminodiritto.it/, 20 maggio 2022, p. 26 s. Sulla questione, cfr. U. SALANITRO, *op.cit.*, p. 1274, il quale ha tratteggiato la versione di un fondo di compensazione, il cui onere di finanziamento ricada non sugli utenti, bensì sui produttori ed eventualmente sui *provider*, secondo un criterio che non sia legato alla quota di mercato, quanto alla frequenza e alla gravità degli incidenti in cui il prodotto o la rete sia coinvolta. Il fondo di compensazione, così strutturato, avrebbe la funzione di coprire i danni anonimi, permettendo una parziale socializzazione dei rischi e avrebbe il vantaggio di consentire un risparmio dei costi amministrativi di gestione delle controversie.

[74] Cfr. M. INFANTINO, *op.cit.*, par. 4.

comprensione dei meccanismi inferenziali, sui quali si basano i processi decisionali automatizzati, rendono ardua la contestazione in sede giudiziaria[75].

Un argine determinante a tali implicazioni delle intelligenze artificiali è indubitabilmente rappresentato dal principio di trasparenza algoritmica[76], la cui rilevanza è emersa, in ambito europeo, già nel 2018, nella Comunicazione della Commissione al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni sull'Intelligenza artificiale per l'Europa, ove si è affermato che l'Unione Europea deve assicurare una cornice etica e giuridica che sia rispettosa dei diritti e delle libertà fondamentali dei cittadini, sul piano economico e sociale, oltre che dei principi di trasparenza e di responsabilità[77].

Si è autorevolmente affermato che codesto principio permette di accertare e correggere possibili errori del processo automatizzato, a tutela del singolo e della correttezza della procedura, sia in fase preventiva (con obblighi informativi sulla logica da seguire), sia in fase successiva, con il riconoscimento del diritto alla spiegazione delle decisioni o dei comportamenti assunti dal sistema tecnologico[78]. Nella medesima prospettiva, il principio è stato qualificato, «in prima approssimazione», come l'obbligo, posto in capo ai soggetti che adottino risoluzioni, adoperando sistemi automatizzati di trattamento dei dati personali, di fornire ai destinatari una spiegazione comprensibile delle procedure utilizzate e di motivare le risoluzioni assunte, sulla loro scorta[79].

A livello europeo, il principio è stato declinato in diverse modalità.

Nella c.d. Legge sui servizi digitali (*Digital Service Act*), entrata in vigore il 16 novembre 2022[80] (affiancata dalla c.d. legge sui mercati digitali, *Digital Markets Act*, entrata in vigore il primo novembre 2022[81]), il legislatore europeo ha accolto, per le grandi piattaforme *online*, una soluzione che si impernia su una serie di principi, tra i quali la trasparenza, l'accessibilità ai dati e agli algoritmi, l'informativa completa agli utenti, l'autonomia nella scelta del grado di profilazione[82].

Si presti ulteriormente attenzione alla proposta di Regolamento del Parlamento europeo e del Consiglio, del 21 aprile 2021 (c.d. legge

---

[75] Cfr. G. MOBILIO, *op.cit.*, p. 285; E. TROISI, *Automated Decision Making and right to explanation. The right of access as ex post information,* consultabile *online* in *EJPLT*, 2022, 1, p. 184.

[76] Cfr. P. STANZIONE, *GDPR e tutela della vita democratica*, *Relazione al convegno "Gli Stati Generali del diritto di internet*", consultabile *online* sul sito https://dirittodiinternet.it/atti-digitali-di-gli-stati-generali-del-diritto-di-internetluiss-161718-dicembre-2021-di-giuseppe-cassano-e-francesco-di-ciommo-direttori-scientifici-premessa-gli-atti-digitali-fanno, p. 6.

[77] Bruxelles, 25 aprile 2018, COM (2018) 237 final.

[78] Cfr. P. STANZIONE, *op.loc.ult.cit.* Prestigiosa dottrina sottolinea che l'algoritmo deve essere conoscibile e trasparente in tutti i suoi passaggi. È determinante garantire la completezza e la selezione dei dati e la loro adeguatezza, allo scopo della loro applicazione al caso concreto, considerato che ciò evita che la decisione possa essere neutra; come pure che i dati siano verificati, sia in via preventiva, sia successivamente al loro trattamento, al fine di impedire distorsioni. Dalla correttezza dell'algoritmo conseguirà l'idoneità della decisione automatizzata ad essere valutata giudizialmente. Per tali argomentazioni, cfr. P. PERLINGIERI, *Struttura algoritmica e interpretazione*, in *Tecnologie e diritto*, 2020, p. 487; ID. *Relazione conclusiva, op.cit.*, pp. 387, 390.

[79] Cfr. D. POLETTI, *Decisioni algoritmiche e diritto alla comprensione*, *Relazione al convegno "Gli Stati Generali del diritto di internet*", 2021, cit., p. 1.

[80] Regolamento 2022/2065/UE e che modifica la direttiva 2000/31/CE (c.d. regolamento sui servizi digitali).

[81] Regolamento 2022/1925/UE, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive 2019/1937/UE e 2020/1828/UE (c.d. regolamento sui mercati digitali).

[82] Cfr. D. POLETTI, *op.cit.*, p. 3.

sull'intelligenza artificiale)[83] che, nel dettare regole armonizzate, relative all'immissione nel mercato, alla messa a disposizione, alla messa in servizio e all'uso di sistemi intelligenti, ha scelto un modello basato sul rischio.

La proposta costituirà oggetto di attenta analisi *infra* (par. **4.1.1**.). In tale sede, preme sottolineare che ha disposto norme specifiche in materia di trasparenza algoritmica, per quanto concerne i sistemi "ad alto rischio" che, come vedremo, sono identificati sulla base della loro destinazione e del loro impatto. L'art. 12 ha stabilito che essi dovranno essere progettati e sviluppati, in maniera tale che il loro funzionamento sia tracciabile durante tutto il ciclo di vita, con la registrazione automatica degli eventi ("*log*")[84], e sia "sufficientemente" trasparente da consentire agli utenti di interpretare l'*output* e usarlo adeguatamente (art. 13). Tali sistemi dovranno essere accompagnati da istruzioni per l'uso, in un formato digitale o non digitale appropriato, con l'indicazione delle loro caratteristiche e dei loro limiti, in modo tale che il loro funzionamento sia trasparente e non opaco: a tal uopo, questi documenti dovranno contenere informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili agli utenti e a chiunque acquisti o adoperi sistemi digitali.

Invece, per i sistemi di intelligenza artificiale "a rischio basso o limitato", il legislatore europeo ha fissato solo i requisiti minimi di trasparenza. Tale scelta è stata oggetto della censura che la normativa, nello statuire obblighi di trasparenza «molto vaghi» (art. 52), sembra incidere «in maniera recessiva» su tale categoria, che, malgrado sia qualificata a "rischio limitato" include applicazioni che possono essere pericolose[85]. Precisamente, si dispone che, quando vengono usati sistemi intelligenti destinati a interagire con le persone fisiche, i "fornitori" dovranno semplicemente notificare ai consumatori/cittadini la circostanza che essi sono operativi in quell'ambito, a meno che non risulti evidente dalle circostanze e dal contesto di utilizzo. Quando si tratti di sistemi di riconoscimento delle emozioni o di categorizzazione biometrica, gli "utenti" dovranno informare le persone fisiche che vi siano esposte delle loro modalità di funzionamento. Per quanto riguarda i cc.dd. "*deep fake*", che sono sistemi che generano o manipolano immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri, gli "utenti" dovranno rendere noto che il contenuto è stato generato o manipolato artificialmente.

Il provvedimento *in fieri* è stato oggetto dell'ulteriore critica di essere intervenuto sul piano degli obblighi di trasparenza, senza riconoscere al destinatario delle risoluzioni del sistema tecnologico nessun diritto di accesso alle informazioni sul suo funzionamento; in ciò, distinguendosi dal Regolamento 2016/679/UE in materia di protezione dei dati personali (c.d. *GDPR*) che ha istituito il diritto del soggetto interessato al loro trattamento di

[83] Bruxelles, 21.4.2021 COM(2021) 206 final 2021/0106(COD)

[84] I *log* indicano il periodo di ogni impiego del sistema (data e ora di inizio e data e ora di fine) e identificano le persone fisiche coinvolte nella verifica dei risultati. Cfr. F.A. NANNI, *Analisi della Proposta di Regolamento sull'intelligenza artificiale pubblicata dalla Commissione europea il 21 aprile 2021*, in *Cyberlaws.it*, 2021.

[85] Cfr. D. POLETTI, *op.loc.ult.cit.*

accedere alle informazioni significative sia sulla logica impiegata, sia sull'importanza e sulle conseguenze previste dallo stesso[86].

A tal proposito, la letteratura giuridica si è posta il quesito se al principio di trasparenza algoritmica possa essere ricollegato un vero e proprio diritto dei destinatari di processi decisionali automatizzati di comprendere non solo la loro architettura e le loro caratteristiche, ma tanto più i criteri adottati e le ragioni delle singole risoluzioni cui siano sottoposti[87]: diritto qualificabile come diritto alla "spiegazione" o all'"interpretazione" o alla "comprensibilità" dell'algoritmo.

Goodman e Flexmann sono stati tra i primi studiosi a rinvenire, nella regolamentazione del *GDPR,* gli estremi di quello che hanno definito "il diritto all'interpretabilità umana dell'algoritmo", ricavandone un fondamento nel considerando 71, nel combinato disposto degli artt. 13 e 14 (obbligo di notifica), dell'art. 22 (divieto di essere sottoposto a una decisione completamente automatizzata), cui si affiancano il diritto di accesso (art. 15) ed il diritto di ottenere le informazioni riguardanti il trattamento dei dati personali (art. 12)[88]. Nella stessa direzione, il Art. 29 *Working Party*, alla luce del considerando 71 e dell'art. 22 *GDPR*, ha sostenuto che è nodale che i processi decisionali 'completamente' automatizzati siano controbilanciati dall'obbligo di fornire alla persona interessata le informazioni puntuali che la riguardino, dal diritto di ottenere un intervento umano ovvero di esprimere il suo punto di vista e dal diritto di conseguire una spiegazione sulla decisione presa, con la precisazione delle valutazioni che ne siano state alla base, oltre che dal diritto di poterla contestare[89].

Altra dottrina nega che l'art. 22 *GDPR* possa costituire l'appiglio normativo, per il riconoscimento del diritto alla spiegazione algoritmica, dichiarando che la norma non indica espressamente il diritto dell'interessato a essere informato sull'uso del procedimento automatizzato[90]. Taluni sottolineano che l'art. 22 è pieno di eccezioni che ne impedirebbero comunque un'applicazione piena[91]. Si è altresì osservato che il diritto alla spiegazione algoritmica non potrebbe trovare fondamento nel considerando 71, perché non si tratterebbe di una previsione giuridicamente vincolante[92].

---

[86] Cfr. G. SCHNEIDER, *Intelligenza artificiale e decisioni automatizzate: la responsabilità "regolatoria" d'impresa, oltre la compliance*, in *Riv.dir.impresa*, 2020, p. 50 s.

[87] Cfr. G. MOBILIO, *op.cit.*, pp. 284-293.

[88] Cfr. GOODMAN, S. FLEXMAN, *European Union Regulation on algorithmic decision-making and a "Right to explanation"*, in *AI MAGAZINE*, 2017, p. 51 ss. Sulla stessa linea, si riconosce che l'interpretazione sistematica di tali norme garantisca una "*legibility*" dei dati personali e degli algoritmi analitici, da intendersi come comprensibilità del funzionamento di questi ultimi. Cfr. G. MALGIERI, G. COMANDÉ, *Why a right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, p. 245 ss.

[89] Cfr. G. SIMEONE, *Machine learning e tutela della privacy alla luce del GDPR*, in G. ALPA (a cura di), *Diritto e intelligenza artificiale, op. cit.*, p. 285 che fa riferimento al *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation* 2016/679, adottate il 3 ottobre 2017 e riviste il 6 febbraio 2018 dall'art. 29 *Working Party.*

[90] Cfr., *ex multis*, tra i primi commentatori, S. WATCHER, B. MITTELSTADT, I. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does non Exist in the General Data Protection Regulation,* in *International Data Privacy Law*, 2017, 7(2), 76–99.

[91] Cfr. M. PALMIRANI, *Interpretabilità, conoscibilità, spiegabilità dei processi decisionali automatizzati*, in U. RUFFOLO (a cura di), *XXVI, Lezioni, op.cit.*, p. 73.

[92] Cfr. F. SARZANA DI S. IPPOLITO, M. NICOTRA (a cura di), *Diritto della Blockchain, Intelligenza artificiale e Iot, Padova*, 2018, p. 260. Tale argomentazione potrebbe essere confutata, rammentando che, ancorché i

In ogni modo, si rimarchi che, pur riconoscendo un fondamento normativo al diritto alla comprensibilità o alla spiegazione algoritmica, in fondo, non sarebbe neanche chiaro chi sia il soggetto obbligato ad assolvere l'obbligo di "spiegabilità" e verso chi sia rivolta la spiegazione. Si evidenzi che la spiegazione cambia, a seconda del destinatario in un rapporto dialogico e in considerazione del fatto che gli attori, coinvolti nel processo decisionale automatizzato, possono essere tanti e tutti spinti da esigenze di spiegazioni difformi[93].

Il dibattito sulla configurabilità di tale diritto non è sopito[94] e poche sono le pronunce giurisprudenziali sul tema. In ogni caso, quantunque sia auspicabile un intervento normativo che garantisca la trasparenza degli algoritmi in senso ampio, con riferimento a tutte le possibili applicazioni dell'intelligenza artificiale ed oltre i limiti, di cui all'art. 22 *GDPR*; da un altro punto di vista, il bisogno di ottenere la spiegazione del funzionamento degli algoritmi incontra i limiti correlati sia alle privative industriali ed alla segretezza commerciale, sia alle conoscenze tecniche altamente qualificate, necessarie per capirne il significato ed il funzionamento. In effetti, qualsivoglia sia il linguaggio di programmazione utilizzato, la scrittura e la lettura degli algoritmi esige competenze speciali e la comprensione del percorso che ha condotto l'algoritmo ad uno specifico risultato è tanto più complicata, quanto più autonomo ed intelligente sia lo stesso[95].

In conclusione, a dispetto di tali problematiche, la posizione probatoria del ricorrente può essere "alleggerita" dall'imposizione, in capo ai danneggianti convenuti, di obblighi di *disclosure* di informazioni sugli elementi di prova, necessari alla dimostrazione della sussistenza del nesso di causalità tra l'evento dannoso e il funzionamento dello *smart device*- quantomeno per quanto attiene alle applicazioni di intelligenza artificiale ritenute a rischio elevato e ad ambiti particolarmente "sensibili", quali quello sanitario ed automobilistico[96].

Questa opzione è stata accolta dalle Istituzioni europee, nelle due recenti proposte di direttive sulla responsabilità civile che saranno esaminate *infra.*

2.3. (segue) Principio di accountability e "sistema multilivello" di responsabilità.

Alla luce delle riflessioni svolte, appare chiaro che la complessità, l'autonomia, l'opacità dei sistemi di intelligenza artificiale e l'incertezza delle regole del loro funzionamento rendono i tradizionali paradigmi della

---

considerando non abbiano autonomo valore normativo, può, ad ogni modo, riconoscersi, come ribadito dalla Corte di Giustizia dell'Unione Europea, un loro ruolo ermeneutico supplementare, facendo luce sull'interpretazione da attribuire ad una norma di legge. Cfr. C. TABBARRINI, *Comprendere la "Big Mind": il GDPR sana il divario di intelligibilità uomo-macchina?*, in *Dir.inf. e informatica*, 2019, p. 555 ss., par. 2., consultabile *online* sul sito http://dejure.it

[93] Cfr. M. PALMIRANI, *op.cit.*, p. 72 s. che richiama S. WATCHER, B. MITTELSTADT, I. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does non Exist in the General Data Protection Regulation, op.loc.ult.cit.* e J.H.N. JANSSEN, *The right to explanation: means for "white boxing' the black-box?*, Tilburg, 2019, *passim.*

[94] Parte della dottrina identifica il diritto alla spiegazione del processo decisionale automatizzato nel diritto di accesso, di cui all'articolo 15 *GDPR*. Cfr. E. TROISI, *op.ult.cit.,* p. 197. *Contra* G. FINOCCHIARO, *Intelligenza e protezione dei dati personali*, in *Giur.it*, 2019, p.1675.

[95] Per tali osservazioni, cfr. M. INFANTINO, *op.cit.*, par. 4.

[96] Cfr. A. AMIDEI, *op.ult.cit.*, p. 159.

responsabilità civile inefficienti, per garantire una tutela effettiva dei diritti e delle libertà fondamentali dei destinatari delle loro risoluzioni.

Ne consegue che, in tale contesto, la responsabilità civile non può avere un ruolo prioritario[97] e che è compito del legislatore affrontare due ordini di questioni giuridiche: le «*issues of liability*», attinenti alle tematiche di natura prettamente civilistica e le «*issues of permittance*», concernenti le esigenze di regolamentazione pubblicistica del settore[98].

Sovviene, cioè, la necessità di sviluppare, accanto alla disciplina della responsabilità civile "algoritmica", norme amministrative che stabiliscano i parametri su cui orientare la programmazione, la produzione e la commercializzazione dei sistemi digitali e che fissino nuove procedure per la loro verifica e convalida, allo scopo di poter valutare e controllare la sicurezza, la trasparenza, la comprensibilità, la rendicontabilità e la responsabilità etica degli stessi[99].

Solo in tal modo, potrà realizzarsi un'intelligenza artificiale affidabile ed antropocentrica[100] e costruire un'architettura di entità artificiali intelligenti, idonea a garantire la loro conformità ai principi etici ed alle normative vigenti dell'Unione Europea[101].

Il modello legislativo più congruo a risolvere i problemi giuridici correlati all'innovazione tecnologica deve essere permeato dai principi di prevenzione e di precauzione ed elaborare un "sistema multilivello di responsabilità" che sia imperniato sul principio di *accountability,* analogamente a quanto previsto dal *GDPR*[102]. Si deve, cioè, puntare alla massima responsabilizzazione dei soggetti coinvolti nell'intero processo, a partire dall'ideazione e dalla programmazione

---

[97] Cfr. D. DI SABATO, *op.ult.cit.,* p. 343.

[98] Sul punto cfr. A. AMIDEI, *Intelligenza Artificiale e product liability: sviluppi del diritto dell'Unione Europea*, in *Giur.it.*, 2019, p. 1718.

[99] Cfr. il Parere del Comitato economico e sociale europeo su «L'intelligenza artificiale. Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società», Document 52016IE5369 (punto 3.16).

[100] Cfr. Commissione europea, Direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie, Orientamenti etici per un'IA affidabile, Ufficio delle pubblicazioni, 2019, punti 87 e ss.

[101] Cfr. M. GAMBINI, *op.cit.*, p. 326. In relazione ai profili etici dell'Intelligenza artificiale è molto importante la Risoluzione del Parlamento europeo del 20 ottobre 2020, «recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate» (2020/2012(INL)), ove si è previsto, in linea con la logica del *based risk*, il bisogno di regole che fissino un'impostazione etica predefinita, sin dalla progettazione dei sistemi intelligenti; la possibilità di un intervento umano, al fine di sopperire all'asimmetria tra coloro che impieghino le tecnologie digitali e coloro che vi siano assoggettati. Alla Risoluzione è allegata la proposta di Regolamento del Parlamento europeo e del Consiglio «sui principi etici per lo sviluppo, la diffusione e l'utilizzo dell'intelligenza artificiale, della robotica e delle tecnologie correlate» che intende «istituire un quadro normativo dell'Unione di principi etici e obblighi giuridici per lo sviluppo, la diffusione e l'utilizzo dell'intelligenza artificiale, della robotica e delle tecnologie correlate nell'Unione». Esso statuisce molteplici e specifici obblighi per le tecnologie ad "alto rischio". Per un approfondimento, cfr. M. CASTILLA BAREA, *op.loc.ult.cit.* Già prima dell'emanazione del provvedimento, la dottrina ha posto in evidenza che le Istituzioni Europee sono profondamente consapevoli della necessità di realizzare una cornice di regole per lo sviluppo di un'intelligenza artificiale antropocentrica «nel senso di tutelante e potenziante l'essere umano in quanto tale». Cfr. *Per un'intelligenza antropocentrica. Intervista a Lucilla Gatt*, consultabile *online* in *Diritto mercato tecnologia*, 21 febbraio 2020.

[102] Sul punto cfr. G. COMANDÉ, *Multilayered (Accountable) Liability for Artificial Intelligence*, in S. LOHSS, R. SCHULZE, D. STAUDENMAYER (a cura di), *Liability for Artificial Intelligence and the Internet of Things*, Baden-Baden, 2019, p. 178l; M. GAMBINI, *op.cit.*, p. 325, s. Il *GDPR* affida al titolare del trattamento la scelta delle soluzioni più idonee, per il raggiungimento dell'obiettivo della gestione del rischio, derivante dal trattamento dei dati personali, prevedendo che dovrà, di seguito, risponderne, qualora sorgano problemi. Cfr. R. CARLEO, *Il principio di accountability nel GDPR: dalla regola alla auto-regolazione*, in *Nuovo diritto civile*, 2021, p. 366. Sul punto si tornerà *infra*.

fino all'impiego delle applicazioni algoritmiche, facendo gravare su di loro l'obbligo di rendere conto delle decisioni assunte a coloro che ne subiscano gli effetti.

Sotto un altro punto di vista, le regole della responsabilità civile, quale che sia la norma applicabile scelta, devono essere "immerse" nel più ampio perimetro della responsabilizzazione dei ruoli di tutti i soggetti presenti nel ciclo di vita dei sistemi digitali. Da ciò discenderà una nozione di responsabilità civile che assumerà una connotazione diversa, più ampia e connessa al principio di *accountability*. In tale ottica, la responsabilità civile rappresenterà solo un «tassello del mosaico», dovendo essere integrata e potenziata da altri strumenti pubblicistici di tutela preventiva[103].

3.1.1. Scenari normativi. Le "permittance" rules e la proposta della c.d. legge sull'intelligenza artificiale.

La Commissione europea si sta muovendo in tale direzione.

Per un verso, ha elaborato norme volte a ridurre e gestire i rischi per la sicurezza e a tutelare i diritti fondamentali. Per altro verso, nella consapevolezza dell'impossibilità di eliminare tutti i potenziali rischi e nella persuasione che la sicurezza e la responsabilità sono due facce della stessa medaglia che si applicano in momenti diversi e si rafforzano a vicenda, la Commissione ha dettato norme in materia di responsabilità civile, da applicare allorché tali rischi dovessero concretizzarsi e cagionare danni[104].

Nel quadro normativo che si sta delineando, sul piano delle "*permittance" rules*, si pongono le due proposte di regolamento, *supra* menzionate, l'una relativa alla sicurezza generale di prodotti e l'altra relativa alla sicurezza delle macchine; nonché la proposta di regolamento, definita c.d. legge sull'intelligenza artificiale, che assume una portata di nodale importanza.

La proposta di regolamento si pone l'obiettivo di «delineare una cornice giuridica alta ed armonizzata» [105]: "armonizzata", dacché si impegna a fissare regole uniformi, da applicare a livello europeo; "alta", siccome ha l'ambizione di promuovere lo sviluppo dell'intelligenza artificiale, mirando, da un lato, a ridurre al minimo i rischi per la sicurezza e i diritti fondamentali, intervenendo prima dell'immissione dei sistemi intelligenti sul mercato dell'Unione europea, dall'altro lato, garantendo certezza giuridica.

Il provvedimento *in fieri* si inserisce nell'ambito del disegno strategico europeo di assicurare un mercato digitale comune e di consentire all'Unione Europea «di essere un *leader* mondiale nello sviluppo di un'intelligenza artificiale sicura, affidabile ed etica» e un «*leader* nella produzione

---

[103] Per tali argomentazioni, cfr. G. COMANDÉ, *Intelligenza artificiale e responsabilità tra liability e accountability*, *op.cit.*, pp. 180, 184.

[104] Cfr. Relazione della Commissione alla Proposta per una direttiva del Parlamento europeo e del Consiglio, relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale; c.d. direttiva sulla responsabilità da intelligenza artificiale/*AI Liability Directive*, Bruxelles 29 settembre 2022, (COM (2022) 496 final 2022/0303 (COD)), punto 1.

[105] Cfr. V. FALCE, *Regolamento IA tra innovazione, valori e concorrenza*, *Relazione al convegno*, dal titolo "*Gli Stati Generali del diritto di internet*", 2021, cit., p. 1.

normativa»[106]. Nel contesto geopolitico, si mira a far sì che il modello europeo divenga un riferimento globale nel mercato delle tecnologie, che possa essere usato nelle altre regioni del mondo [107], riproducendo il c.d. «effetto Bruxelles»[108].

Non sorprende, perciò, che la proposta di regolamento- in modo analogo a quanto previsto dal *GDPR*, in relazione al trattamento transfrontaliero dei dati personali, al *Digital Service Act* e al *Digital Market Act*- individui un ambito di applicazione territoriale che travalica i confini del mercato interno [109]. La normativa e l'apparato sanzionatorio si applicheranno, effettivamente, non soltanto ai "fornitori" e agli "utenti" dei sistemi digitali immessi o utilizzati nel territorio dell'Unione Europea, ma anche ai "fornitori" e agli "utenti" che siano situati al di fuori di tale area, quando l'*output,* prodotto dal sistema sia impiegato in ambito europeo.

La proposta di regolamento definisce in maniera generica e descrittiva (tutti) i sistemi di intelligenza artificiale, all'art. 3, n. 1, adoperando un criterio orizzontale omnicomprensivo. Prevede, infatti**,** regole generali, per profilare uno spazio complessivo, nel quale operino tutti i sistemi digitali (a titolo esplicativo, sia il medico, sia il finanziario), oltre che quelli ancora non ideati.

Tale opzione è stata oggetto della critica che presenterebbe il limite intrinseco di trattare tutte le applicazioni di intelligenza artificiale in modo sostanzialmente omogeneo, quando, viceversa, sono diversissime tra loro e possono assumere distinte caratteristiche, a seconda dell'ambito in cui vengano usate[110].

La nuova disciplina adotta un modello di gestione, basato su una «piramide» ascendente dei rischi, connaturati nell'impiego di dispositivi intelligenti, che va dal rischio "medio o basso", al rischio "alto", fino al rischio "inaccettabile"[111], per compiere una graduazione di regole che fissino divieti, obblighi e misure di *enforcement*, modulandole in funzione del diverso livello di rischio connesso a determinate tipologie di attività. Il «rischio tipico» non è definito in corrispondenza dei valori di mercato, quanto, piuttosto, avendo precipuo riguardo alla cornice dei valori e dei diritti fondamentali riconosciuti dall'Unione Europea[112]. In sostanza, l'obiettivo primario che la proposta persegue è la tutela dei diritti fondamentali e la salvaguardia del processo democratico[113].

---

[106] La relazione introduttiva della proposta di regolamento dichiara lo scopo di «tutelare la sovranità digitale dell'Unione e di sfruttare gli strumenti e i poteri di regolamentazione di quest'ultima per plasmare regole e norme di portata globale» p. 7.

[107] Cfr. G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale*, in *Riv.trim.dir.pubbl.*, 2022, pp. 1085 ss. par. 2, consultabile *online* sul sito http://dejure.it; G. RESTA, *op.cit.*, par. 2, il quale offre spunti di comparazione della *policy* europea con la cinese e la statunitense.

[108] Per l'elaborazione di tale tesi, cfr. A. BRADFORD, '*The Brussels Effect'*, 107 Northwestern U.L. Rev. (2013), p. 1.

[109] Cfr. G. RESTA, *op.cit.*, par. 4. L'autore (*ivi*, par. 2) evidenzia come l'adozione di una clausola ampia e strutturalmente indeterminata, come quella dell'art. 2, par. 1, lett. c), tracci una «via molto scivolosa per il legislatore europeo».

[110] Cfr. G. FINOCCHIARO, *op.ult.cit.*, par. 3.

[111] Cfr. Dossier 57, 12 novembre 2021, di commento alla proposta della c.d. Legge sull'intelligenza artificiale della Camera dei Deputati, Ufficio Rapporti con l'Unione europea, XVIII legislatura, p.1.

[112] Cfr. G. RESTA, *op.cit.*, par. 6.

[113] Di fatto, il legislatore tratteggia un modello regolatorio rispondente al «paradigma dei diritti fondamentali». Cfr. G. RESTA, *op.cit.*, par. 3.

Si pone, perciò, un divieto, con eccezioni e deroghe, e si impedisce l'ingresso nel mercato interno ai sistemi intelligenti che creino un rischio "inaccettabile", relativamente alle violazioni delle libertà fondamentali e dei diritti, riconosciuti e garantiti a livello europeo. In concordanza al principio di prevenzione, si vieta, la messa in servizio sia di sistemi che adoperino tecniche subliminali che agiscano senza che una persona ne sia consapevole, sia di quelli che sfruttino la vulnerabilità di uno specifico gruppo di persone, dovuta all'età o alla disabilità fisica o mentale, quando tali sistemi siano volti a distorcere materialmente il comportamento di tali soggetti, in un modo che provochi o possa cagionare a tale persona o a un'altra un danno fisico o psicologico[114]. È vietata l'immissione nel mercato e la messa in servizio di sistemi di *social scoring* (punteggio sociale, adottato in Cina), lesivi della dignità umana e di quelli di identificazione biometrica remota «in tempo reale», in spazi accessibili al pubblico, come quelli di riconoscimento facciale.

Per i sistemi a rischio "basso o limitato", si sono stabiliti (unicamente) obblighi di trasparenza e si incoraggia l'elaborazione di codici di condotta[115].

La normativa si incentra prevalentemente sui sistemi "ad alto rischio", classificati in quelli destinati ad essere usati come componenti di sicurezza di prodotti soggetti a valutazione della conformità *ex ante* da parte di terzi; in altri sistemi intelligenti indipendenti che presentano implicazioni, principalmente in relazione ai diritti fondamentali, esplicitamente elencati nell'allegato III[116].

In linea generale, sono dettate una serie di previsioni volte a far sì che tali sistemi siano affidabili durante la loro progettazione, il loro sviluppo e la loro esecuzione. A tale scopo, li si assoggetta ad una procedura di valutazione di conformità *ex ante* che si concluda con la marcatura CE.

Sono fissati dettagliatamente gli obblighi e i requisiti che i sistemi "ad alto rischio" dovranno rispettare (artt. 8 ss.)[117]. A norma dell'art. 8, al fine di garantire la conformità ad essi, bisognerà tenere conto sia della finalità prevista dall'entità artificiale intelligente, sia del sistema di gestione dei rischi, disposto dall'art. 9.

Prima di tutto, ai sensi dell'art. 9, paragrafi 1 e 2, si dovrà istituire, attuare, documentare e mantenere un modello di gestione dei rischi, vale a dire un processo iterativo continuo, eseguito nel corso dell'intero ciclo di vita di un sistema "ad alto rischio", che richiederà un aggiornamento costante e sistematico. Esso comprenderà le fasi successive di identificazione ed analisi dei rischi noti e prevedibili associati al sistema; la stima e la valutazione dei rischi che potranno emergere, quando il sistema sia utilizzato conformemente alla sua finalità prevista e in condizioni di uso improprio ragionevolmente prevedibile; la valutazione di altri eventuali rischi derivanti dall'analisi dei dati,

---

[114] Cfr. G. FINOCCHIARO, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir.inf. e informatica*, 2022, par. 3, consultabile *online* sul sito http://dejure.it. L'Autrice puntualizza che la criticità sussiste nelle eccezioni previste dal legislatore.

[115] La dottrina individua, in una prospettiva sistematica, un quarto livello di rischio che si potrebbe definire "minimo" o nullo, nel quale far rientrare tutti gli altri sistemi di intelligenza artificiale che potranno essere sviluppati e impiegati, senza necessità di adeguamento alla normativa suddetta. Cfr. E. BATTELLI, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona*, in D. BUZZELLI, M. PALAZZO (a cura di), *Intelligenza artificiale e diritti della persona, op.cit.*, p. 101, p. 107.

[116] Cfr. Relazione della Commissione europea che accompagna la proposta, punto 5.2.3.

[117] Per le considerazioni che seguono, cfr. G. FINOCCHIARO, *op.ult.cit.*, par. 3.

raccolti dal monitoraggio successivo all'immissione sul mercato; oltre che l'adozione di adeguate misure di gestione dei rischi.

Nell'ottica del principio di *accountability*, i risultati elaborati dai sistemi "ad alto rischio" dovranno essere verificati e tracciati, lungo il loro intero ciclo di vita[118]. La documentazione tecnica che li riguarderà dovrà essere redatta, prima della loro immissione sul mercato o della loro messa in servizio e in modo tale da dimostrare che il sistema digitale è conforme ai requisiti statuiti dal Regolamento; dovrà essere sottoposta ad aggiornamento continuo; fornirà alle autorità nazionali competenti e agli organismi notificati tutte le informazioni necessarie per valutare codesta conformità. Sono statuiti obblighi di conservazione delle registrazioni automatiche degli eventi (*file di log*) (art. 12).

I sistemi "ad alto rischio" devono essere progettati e sviluppati, in modo tale da garantire la trasparenza; con strumenti che ne consentano la supervisione umana, mirante a prevenire e ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali (art. 14); in modo tale da ottenere, in conformità alla loro finalità, un adeguato livello di accuratezza, robustezza e cibersicurezza che duri per l'intero ciclo di vita (art. 15).

Sono poi individuati alcuni criteri di qualità per i *set* di dati adoperati per l'addestramento, la convalida e la prova. Tali *set* devono essere sottoposti ad adeguate pratiche di *governance* e di gestione dei dati, di cui all'art. 10, par. 2, e devono essere pertinenti, rappresentativi, esenti da errori e completi e statisticamente appropriati.

Ulteriori obblighi e requisiti derivano, per tali sistemi, dalle norme che fissano specifici adempimenti proporzionati, in capo ai soggetti coinvolti nella filiera della loro creazione e del loro utilizzo: il "fornitore" (*ex* art. 3, par. 1, n. 2); l'"utente" (*ex* art. 3, par. 1, n. 4); l'"importatore" (*ex* art. 3, par. 1, n. 6) ed il "distributore" (*ex* art. 3, par. 1, n. 7).

In più, si prevede l'individuazione o l'istituzione, da parte degli Stati membri, di un'autorità di vigilanza e controllo dell'applicazione del Regolamento. Si istituisce il Comitato europeo per l'intelligenza artificiale, costituito dai rappresentanti degli Stati membri e della Commissione (art. 58), con il compito di raccogliere e condividere le migliori pratiche, di vigilare sull'attuazione della disciplina, oltre che di facilitare l'attuazione del provvedimento *in fieri* e di contribuire ad un'efficace cooperazione con le autorità nazionali di vigilanza e con la Commissione.

Si stabiliscono strumenti di *enforcement*, attribuendo all'autorità di sorveglianza nazionale poteri e misure, per assicurare il rispetto dei requisiti e degli obblighi menzionati. Specificamente l'autorità, se dovesse avere motivi sufficienti per ritenere che un sistema intelligente presenti un rischio per la salute o la sicurezza o per la tutela dei diritti fondamentali delle persone (ai sensi dell'art. 65, par. 1), effettuerà una sua valutazione, relativamente alla sua conformità ai requisiti e agli obblighi suddetti.

A loro volta, i fornitori saranno tenuti, in conformità al principio di *accountability*, a dimostrare all'autorità la "conformità" del sistema "ad alto rischio".

[118] Cfr. F.A. NANNI, *op.loc.ult.cit.*

In ogni caso se, nel corso di tale valutazione, l'autorità rileverà talune difformità, potrà imporre all'operatore pertinente l'adozione di misure appropriate per far cessare la violazione; ritirare il sistema dal mercato o richiamarlo per un tempo ragionevole, commisurato alla natura del rischio (art. 65, par. 2). Di tali azioni dovrà essere data comunicazione sia alla Commissione europea, sia agli altri Stati membri, per l'eventuale attivazione di corrispondenti misure di salvaguardia.

Infine, il regolamento statuisce che dovranno essere approntate, da parte degli Stati membri, le sanzioni amministrative pecuniarie, applicabili in caso di sua violazione e che le stesse dovranno essere effettive, dissuasive e proporzionate, dovendo, in particolar modo, tenere conto degli interessi dei "fornitori" di piccole o medie dimensioni e delle *start-up* e della loro sostenibilità economica.

3.1.2. (segue) Punti di forza e profili critici della disciplina.

Tratteggiati i capisaldi della disciplina, può elencarsi, tra i punti di forza, la scelta dello strumento normativo del regolamento, il cui impiego ha il pregio di assicurare l'uniformità in ambito europeo, nell'ottica di fornire la certezza del diritto necessaria sia agli operatori economici, per agevolare gli investimenti, l'innovazione e la concorrenza in tale settore; sia agli utilizzatori, per facilitare la circolazione delle tecnologie emergenti nel mercato e dare loro fiducia sul conseguimento di un elevato livello di tutela dei propri diritti.

La proposta di regolamento presenta una serie di criticità, tra le quali, in primo luogo, la rigidità delle definizioni dei sistemi digitali[119], siccome non solo non si tiene conto delle difformità tra le diverse applicazioni di intelligenza artificiale, ma neppure delle innovazioni, dal momento che qualunque sviluppo tecnologico dovrà essere inserito nella "griglia" definita dal legislatore. Sebbene la classificazione dei sistemi digitali sarà soggetta a revisione, come previsto nel regolamento, sicuramente la rapidità del progresso tecnologico determina il pericolo che le applicazioni future di intelligenza artificiale saranno regolamentate nella prospettiva attuale. Il metodo prescelto non è, pertanto, sufficientemente dinamico, per seguire gli sviluppi futuri[120].

In realtà, l'inadeguatezza della proposta di regolamento, sotto questo punto di vista, discende dalla circostanza che, nel redigerla, si è prediletto un approccio *top-down*. È, difatti, il legislatore ad identificare le tecnologie dell'intelligenza artificiale, a determinare le pratiche proibite e rischiose e ad individuare, *ex ante*, il diverso livello di rischio, dal quale far discendere le regole applicabili, lasciando poco spazio alla valutazione dei destinatari delle stesse. Questo metodo implica il pericolo di elaborare delle categorie normative astratte che non rappresentino in modo congruo le caratteristiche ed i rischi delle tecnologie digitali emergenti [121].

[119] Per le riflessioni che seguono, cfr. G. FINOCCHIARO, *op.ult.cit*, par. 4.
[120] Per tale critica, cfr. G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale, op.cit.*, par. 4.
[121] Sul punto, cfr. G. RESTA, *op.cit.*, par. 6.

Sarebbe, diversamente, più congruo un approccio *bottom-up*[122], come quello impiegato nel *GDPR*, ove l'apprezzamento del rischio è conferito, in prima battuta, ad una valutazione decentralizzata. Il provvedimento si contraddistingue per l'impianto normativo fondato sul principio di *accountability*, ossia sulla responsabilizzazione del titolare del trattamento che è tenuto a mettere in atto misure tecniche ed organizzative "idonee" a garantire un livello di sicurezza confacente al rischio, come pure a dare attuazione ai principi ed alle norme del regolamento. Tali misure dovranno essere scelte, in conformità alle caratteristiche peculiari del trattamento, più precisamente, ai sensi dell'art. 32, «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche». La decisione sull'appropriatezza delle risoluzioni da adottare sarà rimessa alla "discrezionalità" del titolare del trattamento che non sarà, però, illimitata, poiché dovrà essere necessariamente parametrata alle condizioni descritte. Il titolare del trattamento, oltre a valutare e scegliere le misure di sicurezza idonee, dovrà compiere un'attività di continuo monitoraggio, anche attraverso l'elaborazione di modelli organizzativi specifici. Inoltre, costui dovrà essere in grado di dimostrare tutto, provando la congruità delle scelte di regolamentazione compiute in modo autonomo[123].

Quest'impostazione consente un adattamento costante del modello di gestione del rischio da parte del titolare del trattamento dei dati personali e si basa evidentemente sul convincimento che costui sia il soggetto nella posizione migliore per gestire e valutare il rischio[124].

Tale risultato è stato raggiunto dal legislatore della *privacy*, cambiando la tecnica legislativa (originariamente adoperata nel recepimento Direttiva 95/46/CE), passando da un approccio che si basava su regole molto dettagliate a quello (diverso) del *GDPR*, che si fonda su principi generali e sulla responsabilizzazione del titolare del trattamento[125]. Si sono previste norme c.dd. "in bianco", per 'delegare' i privati ad individuare le regole più idonee, rendendoli responsabili e gravandoli dell'onere di fornire la prova della conformità alle stesse.

Si è, in tal modo, incentivato il ricorso all'autodisciplina, mediante codici di condotta, inquadrabili in linea con il principio di sussidiarietà orizzontale *ex* art. 118 Cost., la cui redazione è stata affidata ai destinatari delle norme, più vicini agli interessi generali che devono essere regolati; oltre che per mezzo

---

[122] Cfr. G. CONTISSA, F. GALLI, F. GODANO, GA. SARTOR, *Il Regolamento europeo sull'intelligenza artificiale. Analisi informatico-giuridica*, consultabile *online* in *i-lex. Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale*, 23 dicembre, 2021, p. 1 ss.

[123] Per tali notazioni, cfr. R. CARLEO, *op.cit.*, p. 356 ss. Si è affermato (G. FINOCCHIARO, *Intelligenza e protezione dei dati personali*, *op.cit.*, p. 1676) che l'*accountability* può tradursi come «responsabilità e, insieme, prova della responsabilità» ed è un meccanismo a due livelli, l'uno di attuazione di misure, l'altro di conservazione delle prove.

[124] Cfr. G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale, op.cit.* par. 4, secondo la quale, mentre il sistema di gestione del rischio è accompagnato dal principio di *accountability* nel *GDPR*, ciò non accadrebbe nella proposta della c.d. legge sull'intelligenza artificiale, dove la valutazione e la gestione del rischio dei sistemi intelligenti non è rimessa alle scelte degli operatori economici, ma al legislatore che detta regole tecniche, senza lasciare spazio a questi ultimi.

[125] Cfr. R. CATERINA, *Novità e continuità nel Regolamento generale sulla protezione dei dati*, in *Giur.it.*, 2019, p. 2777.

dell'elaborazione di *standard* "tecnici" di comportamento, non determinati dal legislatore, ma delegati ad organi non legislativi[126].

Si rilevi che i codici di condotta e l'elaborazione di *standard* "tecnici" comportamentali assumono rilevanza altresì nella disciplina della proposta della c.d. legge sull'intelligenza artificiale.

Anzitutto, l'art. 8 dispone che la "conformità" del sistema intelligente dovrà essere valutata alla stregua di determinati "*standard*". Essi saranno elaborati dalle *standard-setting organizations* europee[127]. È essenziale sottolineare che, se, per un verso, i produttori ed i fornitori di sistemi intelligenti potranno, in linea di principio, prescindere dalle norme tecniche armonizzate, elaborate da tali organizzazioni e provvedere autonomamente a riempire di contenuto la previsione legislativa; per altro verso, la presunzione di conformità, ai sensi dell'art. 40, potrà ritenersi sussistente unicamente quando vi sarà un adeguamento agli *standard,* elaborati da tali organizzazioni. Da ciò discende che «il vero ruolo nomotetico» finirà per l'essere svolto dalle *standard-setting organizations*. Tale circostanza presenta la problematicità che le organizzazioni suddette sono private; conseguentemente, le stesse 'vendono' *standard* (a loro volta protetti dal diritto d'autore) ed il loro operato provocherà una gamma di seri problemi, in termini di trasparenza e rappresentatività, rispetto a delle scelte che si riverbereranno sui diritti e sulle libertà fondamentali dei destinatari delle risoluzioni dei sistemi digitali e sullo stesso processo democratico.

Per quanto concerne i codici di condotta, la proposta di regolamento, al titolo IX, istituisce una cornice per la loro creazione che mira a incoraggiare i fornitori di sistemi intelligenti "non ad alto rischio" ad applicare volontariamente i requisiti obbligatori, previsti per quelli "ad alto rischio", concernenti i dati, la documentazione e la tracciabilità, la fornitura di informazioni e la trasparenza, la sorveglianza umana, la robustezza e la precisione. Le imprese che dovessero introdurre i codici di condotta per i sistemi "non ad alto rischio" lo faranno su base volontaria e potranno attuarli autonomamente[128].

Si aggiunga che recentemente la Commissione europea ha inaugurato un *sandbox*, da intendersi come uno "spazio di sperimentazione normativa", in cui le aziende potranno testare i loro prodotti e servizi, interagendo con le autorità di regolamentazione pertinenti. Il fine di tale iniziativa è di garantire certezza giuridica, nell'ambito delle soluzioni tecnologiche decentralizzate, individuando gli ostacoli normativi all'introduzione delle scelte degli operatori economici e fornendo consulenza giuridica, sulla base delle *best practices* e dell'evoluzione normativa, in un contesto dedicato, riservato e sicuro. Lo spazio

[126] Per tali argomentazioni, cfr. R. CARLEO, *op.cit.*, p. 363 s.

[127] Per le osservazioni sul tema G. RESTA, *op.cit.*, par. 6, che menziona il *CEN*, *European Commitee for Standardization* e il *CENELEC, European Committee for Electrotechnical Standardization*.

[128] Tali codici potranno altresì comprendere impegni volontari relativi, ad esempio, alla sostenibilità ambientale, all'accessibilità da parte delle persone con disabilità, alla partecipazione dei portatori di interessi alla progettazione e allo sviluppo dei sistemi di intelligenza artificiale, come pure alla diversità dei gruppi che si occupano dello sviluppo. Cfr. Relazione alla proposta di regolamento. Punto 5.2.7.

di sperimentazione è finanziato, per gli anni 2023-2026, dal *Digital Europe Programme*[129].

Alla luce di tali considerazioni, può affermarsi che, a fronte dei limiti della tecnica normativa prescelta, nella proposta di regolamento, cionondimeno sia i codici di condotta, seppure limitatamente a coloro che decidano di adottarli, sia i *sandboxes* avranno, senza dubbio, un ruolo fondamentale nell'adeguamento di suddetta disciplina alla realtà complessa ed in continua evoluzione delle intelligenze artificiali[130].

Un ulteriore aspetto critico della proposta di regolamento è individuabile nella circostanza che il *risk-based approach* implica che i rilevanti oneri amministrativi di redazione e di aggiornamento della documentazione, di certificazione, di notifiche, di marcatura incomberanno sulle imprese, indipendentemente dalle loro dimensioni e dalla tipologia di applicazione dell'intelligenza artificiale. Come ovvio, il peso di tali oneri e costi graverà in misura minore sulle grandi imprese ed in misura maggiore sulle piccole e medie imprese e sulle *start up*. L'opzione di dettare la medesima regolamentazione, senza differenziare tra i soggetti e i distinti ambiti di operatività delle nuove tecnologie, è stata confutata, argomentando che le applicazioni di intelligenza artificiale possono essere molto diverse tra loro ed essere declinate in maniera difforme[131]. Pur condividendo tale obiezione, occorre porre in evidenza che il legislatore europeo ha conferito agli Stati membri la funzione di prevedere misure di sostegno per le piccole e medie imprese e che il Consiglio europeo, nel c.d. orientamento generale del 6 dicembre 2022 (*infra*), ha previsto innovativamente talune misure a loro supporto.

Ulteriormente, alla domanda se la proposta di regolamento tuteli idoneamente i diritti ed i valori europei costantemente richiamati, si risponde che esso lascia completamente scoperto il profilo dei diritti e dei rimedi individuali[132]. Il provvedimento *in fieri*, pur proclamando di voler difendere i valori ed i diritti fondamentali dell'Unione europea dai rischi dell'intelligenza artificiale, si focalizza sugli obblighi e sulle prerogative del "fornitore", dell'"utente", dell'"importatore" e del "distributore", definendo una cornice amministrativa per l'immissione dei sistemi digitali nel mercato. Non riconosce, tuttavia, ai destinatari dei processi decisionali automatizzati diritti, quali il diritto ad ottenere una spiegazione del meccanismo di funzionamento dell'entità artificiale intelligente e dell'algoritmo e il diritto a non essere soggetti a decisioni discriminatorie. Né si configurano, distintamente dal *GDPR*, nuovi strumenti di tutela che la persona, individualmente o collettivamente, possa attivare, per rendere la tutela effettiva, più rapida ed efficace[133].

Ebbene, si segnali che, il 6 dicembre 2022, il Consiglio ha adottato la sua posizione comune (c.d. orientamento generale) sulla proposta di regolamento,

---

[129] Cfr. https://www.corrierecomunicazioni.it/digital-economy/blockchain-leuropa-lancia-la-prima-sandbox-normativa/

[130] Cfr. C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'UE in materia di intelligenza artificiale*, in *BioLaw Jorunal*, 2021/2, p. 29, consultabile online sul sito https://www.biodiritto.org

[131] Per le considerazioni di tale critica, cfr. G. FINOCCHIARO, *op.ult.cit.*, par. 4.

[132] Per il commento su tale questione, cfr. G. RESTA, *op.cit.,* par. 6; G. FINOCCHIARO, *op.ult.cit.*, par. 4.

[133] Saranno certamente applicabili i principi sostanziali previsti dal *GDPR* a tutela dei dati personali.

apportando delle modifiche al testo originario e intervenendo su taluni aspetti problematici evidenziati[134].

Primariamente, si circoscrive la definizione di intelligenza artificiale ai sistemi sviluppati mediante l'apprendimento automatico e a quelli basati sulla logica e sulla conoscenza, al fine di semplificare la distinzione tra sistemi *software* più semplici e le tecnologie di intelligenza artificiale. Nella classificazione di queste ultime, si impone di prendere in considerazione altresì la rilevanza dell'*output* del sistema tecnologico, rispetto all'azione pertinente oppure alla decisione da assumere. Si aggiunge, in tal modo, un livello orizzontale alla catalogazione, per evitare l'inclusione, tra le intelligenze artificiali "ad alto rischio", di quelle che non presentino il pericolo di causare gravi violazioni dei diritti fondamentali o altri rischi significativi.

Ancora, dal momento che i sistemi intelligenti sono sviluppati e distribuiti attraverso "catene di valore" complesse, sono stati chiariti ed adeguati i requisiti per i sistemi ad "alto rischio", allo scopo di renderli tecnicamente più realizzabili e meno onerosi per i portatori di interessi. A tal fine, il testo contiene chiarimenti sull'assegnazione di ruoli e di responsabilità ai vari soggetti coinvolti nelle catene di sviluppo e di distribuzione delle tecnologie emergenti, in modo specifico, i "fornitori" e gli "utenti"; oltre che precisazioni sui rapporti tra la responsabilità, ai sensi del Regolamento sull'intelligenza artificiale, e gli altri regimi previsti dalle diverse normative preesistenti, quali quella sulla protezione dei dati personali e la normativa settoriale, come quella riguardante l'ambito dei servizi finanziari.

In linea con il principio di proporzionalità, in forza del quale è indispensabile diversificare la posizione delle piccole-medie imprese e di quelle di grandi dimensioni, vi sono novità concernenti la qualità dei dati e la documentazione tecnica che le piccole e medie imprese dovranno redigere, per provare la conformità dei loro sistemi "ad alto rischio" ai requisiti previsti. Nella stessa direzione, si differenziano i massimali delle sanzioni amministrative, per renderli più proporzionati, in caso di violazioni da parte delle piccole e medie imprese e delle *start-up*.

Si pongano in evidenza le puntualizzazioni sulle procedure di valutazione della conformità e sulla vigilanza del mercato e l'introduzione di disposizioni, per conferire maggiore autonomia e rafforzare il ruolo del comitato per l'intelligenza artificiale e per garantire il coinvolgimento dei portatori di interessi.

La posizione definitiva del Parlamento europeo sulla proposta di Regolamento dovrebbe volgere al termine, a fine marzo 2023. In seguito, avrà inizio il trilogo tra il Consiglio, il Parlamento e la Commissione e il testo verrà adottato[135].

---

[134] Sul punto e per l'analisi di altre modifiche innovative, cfr. il Comunicato stampa del Consiglio europeo, 6 dicembre 2022, consultabile *online* sul sito https://www.consilium.europa.eu/it/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/; M. MARTORANA, R. SAVELLA *Intelligenza artificiale: orientamento del Consiglio europeo e ultimi sviluppi nella definizione del Regolamento*, consultabile *online* sul sito https://www.altalex.com/documents/news/2023/02/15/intelligenza-artificiale-orientamento-consiglio-europeo-ultimi-sviluppi-definizione-regolamento.

[135] Il Regolamento, una volta recepite le indicazioni dei pareri, si applicherà dopo che siano trascorsi due anni dalla sua effettiva entrata in vigore, per consentire a tutti gli operatori di predisporre gli adempimenti

Conclusivamente, alla luce delle notazioni critiche riportate, può dichiararsi che il modello di gestione del rischio, approntato dalla proposta di regolamento, si presenta rigido e statico, difformemente dal modello flessibile e dinamico, costruito dai principi ispiratori e dalla tecnica normativa del *GDPR*. Sarebbe, quindi, auspicabile un cambio di rotta delle Istituzioni europee che, nel revisionare la disciplina della proposta sulla c.d. "intelligenza artificiale", si ponga nel solco del modello virtuoso offerto dal *GDPR* e si focalizzi sull'esigenza di: considerare 'realmente' la rapidità dello sviluppo tecnologico; conferire agli operatori economici una maggiore discrezionalità, seppur parametrata su requisiti prefissati, affinché possa effettuare le scelte più adatte al settore in cui agisca e alle peculiarità del sistema intelligente; garantire strumenti di tutela effettivi ai soggetti danneggiati dalle risoluzioni dei sistemi intelligenti.

3.2.1. (segue) Le "liability" rules. La Risoluzione del Parlamento europeo «recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale».

Sul fronte delle *"liability" rules*, si incentri l'attenzione anzitutto sulla Risoluzione del Parlamento europeo, del 20 ottobre 2020, che ha chiesto alla Commissione di presentare, sulla base dell'articolo 225 TFUE, una proposta di regolamento sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale, seguendo le raccomandazioni dettagliate, figuranti nell'allegato alla risoluzione stessa.

Il Parlamento ha prospettato l'applicazione del regolamento nel territorio dell'Unione Europea, dove un'attività, un dispositivo o un processo virtuale o fisico, guidato da un sistema digitale, arrechi un danno o un pregiudizio alla vita, alla salute, all'integrità fisica di un individuo, al patrimonio di una persona fisica o giuridica ovvero un danno non patrimoniale rilevante, risultante in una perdita economica verificabile (art. 2, par. 1).

Il Parlamento europeo ha abbandonato la posizione, inizialmente assunta (nella Risoluzione del 2017, recante norme di diritto civile sulla robotica, cit.), del riconoscimento della "personalità elettronica" ai sistemi intelligenti [136], proponendo la soluzione innovativa di configurare, come responsabile, il c.d. *deployer*, l'operatore degli stessi. Tale opzione è stata ispirata dalla circostanza che costui beneficia dell'andamento dell'automa ed esercita il controllo sul rischio che vi è associato, in modo analogo al proprietario di un'automobile; inoltre, considerata la complessità delle entità artificiali intelligenti, l'operatore, in molti casi, sarà il primo punto di contatto visibile per il soggetto leso (punto 10 risoluzione).

La proposta di regolamento, nel sancire la responsabilità degli "operatori", li ha classificati sulla base del grado di supervisione che adoperino sul loro

necessari dal punto di vista organizzativo, tecnico e commerciale, al fine di poter essere *compliant* ai sistemi intelligenti, come strutturati dalla Proposta.

[136] Il Parlamento europeo si è basato sulla posizione negativa espressa dal Comitato economico e sociale europeo che ha esposto perplessità di carattere giuridico ed etico. Cfr. il Parere del Comitato economico e sociale europeo, 526a sessione plenaria del CESE del 31 maggio e primo giugno 2017 su "L'intelligenza artificiale. Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società", (2017/C 288/01), punto 3.33.

funzionamento. Si è differenziato tra l'"operatore *front-end*" e l'"operatore *back-end*", definendo il primo come la persona fisica o giuridica che effettua un certo grado di sorveglianza su un rischio connesso all'operatività del sistema intelligente e che ne beneficia (quale, ad esempio, il proprietario o il custode dell'autovettura o del dispositivo automatizzato); il secondo come la persona fisica o giuridica che, su base continuativa, stabilisce le caratteristiche della tecnologia, fornisce i dati e il servizio di supporto di *back-end* essenziale ed è in grado di esplicare un elevato grado di verifica sul pericolo, connesso all'operatività o al funzionamento del sistema tecnologico (per esempio, il gestore di una autostrada attrezzata per la guida automatizzata)[137].

Seguendo un metodo basato sul rischio, la proposta di regolamento ha delineato un duplice statuto giuridico, misurato sul grado di automazione del sistema digitale[138].

Per gli operatori di sistemi "ad alto rischio" (quali, ad esempio, gli aeromobili senza equipaggio, i veicoli con livello di automazione elevato, i sistemi autonomi di gestione del traffico, i dispositivi autonomi di pulizia di luoghi pubblici)[139], si è disposto un regime di responsabilità oggettiva, stabilendo che costoro non possano eludere la propria responsabilità, sostenendo di avere agito con la dovuta diligenza o che il pregiudizio sia stato cagionato da un'attività, da un dispositivo o da un processo autonomo, guidato dal loro sistema di intelligenza artificiale; e individuando l'unica esimente nella causa di forza maggiore. Le attività "ad alto rischio" sono state qualificate (art. 3, lett. c)), in base alla probabilità e alla gravità dei potenziali danni, al grado di autonomia e alle modalità o all'ambito di utilizzo dello strumento digitale.

L'individuazione delle attività "ad alto rischio" è stata deputata alla Commissione europea con un apposito allegato, statuendo che debba essere sottoposto al suo vaglio ed aggiornamento, almeno a scadenza semestrale.

Il legislatore europeo ha imposto a tale categoria di operatori la stipula di una polizza assicurativa, a copertura della propria attività, distinguendo la tipologia di assicurazione (art. 4, par. 4), a seconda che si tratti di operatore *front end* oppure *back en*d. D'altra parte, il Parlamento europeo ha ritenuto che la copertura della responsabilità civile rappresenti uno dei fattori determinanti per il successo delle nuove tecnologie e che spinga il pubblico ad avere fiducia, nonostante la possibilità di subire pregiudizi o di dover affrontare azioni legali (par. 23 della risoluzione cui è allegata la proposta di regolamento).

Si è, poi, sottoposto l'operatore di un sistema digitale non configurabile "ad alto rischio" (e non inserito nell'elenco allegato al regolamento in ragione della circostanza che l'automazione non è tanto elevata) ad un regime di responsabilità per colpa "aggravata" da un complesso di presunzioni[140]. Si è, cioè, esclusa la responsabilità dell'operatore che riesca a dimostrare che la lesione cagionata non sia imputabile a sua colpa, per uno dei seguenti motivi: il sistema si è attivato, senza che ne fosse a conoscenza e siano state adottate

[137] Cfr. U. SALANITRO, *op.cit.*, p. 1275.
[138] Cfr. C. LAENZA, *Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel terzo millennio*, in *Resp. civ. e prev.*, 2021, p. 1013.
[139] Per un'attenta analisi della categoria dei sistemi di intelligenza artificiale "ad alto rischio", introdotta, per la prima volta, nella proposta di regolamento, cfr. R. LOBIANCO, *Veicoli a guida autonoma e responsabilità civile: regime attuale e prospettive di riforma - I e II Parte*, in *Resp. civ. e prev.*, 2020, p. 724 ss., p. 1080 ss.
[140] Cfr. C. LAENZA, *op.cit.*, p. 1011 ss.

tutte le misure ragionevoli e necessarie, per impedire tale attivazione oppure costui ha svolto diligentemente le operazioni appropriate all'uso dell'intelligenza artificiale (selezionando un meccanismo idoneo al compito e alle competenze, mettendolo debitamente in funzione, monitorando le attività e mantenendo l'affidabilità operativa, mediante periodici aggiornamenti).

Si è dettata la regola della responsabilità solidale, sia quando vi dovesse essere un concorso di colpa di più operatori, sia nel caso in cui più operatori dovessero essere coinvolti in un danno causato da un'attività "ad alto rischio". Si è prevista l'esperibilità, da parte del *solvens*, di un'azione di regresso verso gli altri operatori, in misura proporzionale alla sua responsabilità.

Il provvedimento ha predisposto la riduzione del grado di responsabilità dell'operatore o la sua esclusione, rispettivamente quando il pregiudizio dovesse essere prodotto dal concorso di colpa del soggetto danneggiato oppure possa essergli esclusivamente imputabile.

In aggiunta, il Parlamento europeo ha ritenuto che la disciplina della responsabilità civile per colpa, vigente negli Stati membri, offra, il più delle volte, un livello sufficiente di tutela alle persone che subiscano danni, in seguito all'interferenza di un terzo, quale un *hacker*, dato che, in tal caso, il soggetto leso avvierà un'azione basata sulla colpa[141]. Si è comunque profilata la necessità di ulteriori norme, per integrare il diritto nazionale in materia di responsabilità civile, in ipotesi specifiche, incluse quelle in cui il terzo sia irrintracciabile oppure insolvibile.

La proposta di regolamento redatta dal Parlamento europeo, ai fini di una redazione da parte della Commissione, in linea con le indicazioni fornite, è stata oggetto di svariate critiche.

Prima di tutto, in relazione all'ambito oggettivo di applicazione, si è contestata la scelta di unificare la regolamentazione dei danni determinati dai sistemi intelligenti, usando un criterio orizzontale omnicomprensivo, invece di diversificare le applicazioni dell'intelligenza artificiale ed i relativi contesti di riferimento, quali, a titolo esplicativo, quello domestico, il medico, il finanziario oppure l'industriale[142].

In merito all'ambito soggettivo di applicazione, si è espresso scetticismo verso la distinzione tra operatore *back-end* e *front-end*, dichiarando che sarebbe stato preferibile, per il danneggiato, identificare, a monte, un "*entry point*", al quale rivolgersi in caso di danni, per rimettere, di seguito, a rivalse ed altri meccanismi la distribuzione della responsabilità tra i vari soggetti coinvolti, nella catena del sistema digitale[143].

Dal punto di vista processuale, si è rilevato che il «regime flessibile» di responsabilità prescelto[144] avvantaggerebbe la posizione processuale di coloro che abbiano subito un pregiudizio dagli operatori di un sistema "ad alto rischio", per i quali è stato statuito un regime di responsabilità oggettiva, con l'esimente della causa di forza maggiore. Vieppiù, la proposta di regolamento non ha

---

[141] Cfr. Risoluzione del 20 ottobre 2020, recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, cit. (punto 9).

[142] Cfr. A. BERTOLINI, F. EPISCOPO, *The Expert Group's Report on Liability for Artificial Intelligence and Other Emerging Digital Technologies: a critical assessmen*t, in *European Journal of Risk Regulation*, 2021, 12, 3, pp. 648 ss.

[143] Cfr. ID., *op.cit.* p. 656.

[144] Secondo la locuzione elaborata da U. SALANITRO, *op.cit.*, p. 1276.

previsto nulla riguardo alla *probatio* "diabolica" del nesso di causalità tra l'operato del sistema digitale e l'evento dannoso.

Infine, si evidenzi che la proposta di regolamento ha spostato l'attenzione dal produttore all'operatore, chiarendo, tuttavia, la coesistenza con la disciplina della responsabilità per danno da prodotto difettoso e la necessità di uno stretto coordinamento ed allineamento tra le due normative, a livello europeo e nazionale (obiettivo 6, allegato alla risoluzione)[145]. In particolare, l'art. 11, nel regolamentare la responsabilità in solido, ha fissato i criteri di prevalenza dell'una sull'altra, quando l'operatore sia anche il produttore di un sistema tecnologico. Precipuamente la norma ha sancito che, se un operatore di *front-end* dovesse essere altresì il produttore del sistema di intelligenza artificiale, le disposizioni del presente regolamento dovrebbero prevalere su quelle della direttiva sulla responsabilità per danno da prodotti difettosi; se l'operatore di *back-end* fosse anche il produttore, ai sensi dell'articolo 3 della direttiva suddetta, sarebbe opportuna la sua applicabilità a tale soggetto; se vi fosse un solo operatore che fosse anche il produttore del sistema, le previsioni del presente regolamento dovrebbero prevalere su quelle della direttiva.

Per di più, l'art. 12, par. 3, ha disposto che, qualora l'operatore di un sistema tecnologico difettoso dovesse "indennizzare" interamente la persona interessata per danni o pregiudizi, sia che dovesse rispondere a titolo di responsabilità oggettiva, sia che dovesse rispondere a titolo di colpa presunta, potrebbe esperire un'azione di regresso nei confronti del produttore dello *smart device* difettoso, conformemente alla disciplina europea ed alle norme nazionali che regolamentano la responsabilità per danno da prodotto difettoso.

Si osservi, infine, che il legislatore aveva optato per lo strumento normativo del regolamento, ritenendo insufficiente la direttiva, in ragione della rilevanza strategica del settore[146], nella consapevolezza che, se lo si fosse approvato, avrebbe comunque imposto esigenze di coordinamento con la disciplina nazionale ed un intervento di adeguamento a quella europea.

Concludendo, occorre rimarcare che tale iniziativa legislativa non ha avuto seguito, giacché la Commissione europea ha avanzato una differente proposta di regolamentazione della responsabilità civile extracontrattuale per l'intelligenza artificiale, per le ipotesi che non siano riconducibili al paradigma della responsabilità per danno da prodotto difettoso.

3.2.2. (segue) La proposta di revisione della direttiva sulla responsabilità per danni da prodotto difettoso.

Invero, il 28 settembre 2022, la Commissione europea ha presentato due proposte di direttive che dovranno essere approvate dal Parlamento europeo e dal Consiglio, in un pacchetto finalizzato ad adeguare le norme sulla responsabilità civile all'economia circolare, all'era digitale e all'impatto delle catene globali del valore, garantendo l'allineamento dovuto tra questi due strumenti giuridici necessari.

---

[145] Sulla coesistenza di tali regole, cfr. V. DI GREGORIO, *op.cit.* p. 55 ss.
[146] Cfr. U. SALANITRO, *op.cit*, p. 1274, s.

La prima propone la revisione della direttiva sulla responsabilità per danno da prodotto difettoso. Obiettivo della sua modernizzazione è di garantire la certezza giuridica sia alle imprese che devono potere innovare nel settore delle tecnologie digitali emergenti, oltre che assumere i nuovi modelli di economia circolare, modificando, in maniera sostanziale i prodotti, nella consapevolezza delle responsabilità che possano incombere su di loro e calcolando i rischi da dover sopportare; sia ai potenziali danneggiati dai sistemi digitali che devono poter accedere a un panorama normativo semplificato, rispetto a quello attualmente vigente. Si avverte, in effetti, la necessità di apprestare strumenti di tutela effettiva, rispetto ai nuovi danni e ai nuovi difetti, e di fornire la garanzia di trovare sempre un responsabile in Europa, quand'anche il prodotto provenga da uno Stato al di fuori dell'Unione Europea[147].

La seconda è la c.d. *AI Liability Directive* che introduce un regime di responsabilità differenziato per il settore dell'intelligenza artificiale, da applicare ai soli giudizi civili, aventi ad oggetto la richiesta di risarcimento di danni, promossi davanti ai giudici nazionali, in caso di colpa extracontrattuale. La disciplina non include i rischi derivanti dalla produzione e dall'impiego di prodotti digitali, ad eccezione delle ipotesi di violazione di normative di sicurezza, ponendosi in rapporto di complementarità alla proposta di direttiva sulla responsabilità oggettiva del produttore.

Entrambe le proposte di direttive sono, a loro volta, complementari alla proposta della c.d. legge sull'intelligenza artificiale [148].

Orbene, si rimarchi, prima di tutto, che, nella redazione della disciplina di revisione della direttiva della responsabilità per danno da prodotto difettoso, la Commissione ha optato per lo strumento normativo della direttiva, anche se il Parlamento le aveva proposto di valutare se la direttiva attualmente vigente dovesse essere trasformata, in fase di revisione, in regolamento[149]. L'art. 3 ha stabilito il livello di armonizzazione massima.

La proposta di revisione, pur mantenendo l'impianto della responsabilità oggettiva dei produttori per il risarcimento dei danni causati da prodotti non sicuri, ha previsto una serie di disposizioni innovative, per uniformare il regime della responsabilità del produttore alle nuove sfide del settore digitale.

Primariamente si amplia l'ambito oggettivo di applicazione, intervenendo sulla disciplina del danno, sulla definizione del "prodotto" e di quella di "difetto".

Si riconosce il diritto al risarcimento del danno a "qualunque persona fisica" che subisca un pregiudizio da un prodotto difettoso, nella sfera patrimoniale e in quella personale. Oltre ai danni a, o la distruzione della proprietà[150], alla morte o alle lesioni personali, si ricomprendono, in maniera innovativa, tra i

[147] Progetto di parere, CESE, 16 gennaio 2023, Proposta di direttiva del Parlamento europeo e del Consiglio sulla responsabilità per danno da prodotti difettosi. INT/1002, Revisione della direttiva sulla responsabilità per danno da prodotti difettosi, punti 1.3., 2.1.

[148] Sul punto, cfr. "*Consistency with other Union policies*" della proposta della Commissione della direttiva, consultabile *online* sul sito https://ec.europa.eu/info/sites/default/files/1_1_197605_prop_dir_ai_en.pdf, p. 5 s.

[149] Risoluzione del Parlamento europeo del 20 ottobre 2020, recante raccomandazioni alla Commissione sul regime di responsabilità civile per l'intelligenza artificiale intelligenza artificiale, cit., (punto 8).

[150] Le persone potranno chiedere il risarcimento del danno sia quando la proprietà danneggiata sia impiegata per scopi professionali, sia quando lo sia per scopi personali.

danni, quelli alla salute psicologica scientificamente riconosciuti e la perdita o la corruzione di dati personali, non usati esclusivamente a fini professionali[151].

La Commissione, dopo aver precisato, nella relazione alla proposta, che i sistemi tecnologici ed i beni che si basino sull'intelligenza artificiale sono considerati "prodotti", amplia notevolmente tale nozione, comprendendo, nell'ambito di applicazione della normativa, le componente digitali, quali le applicazioni ed altri *software* "integrati" in un prodotto o "interconnessi"- che rientrano nelle definizioni di "componente" (articolo 4, paragrafo 3), di "servizio correlato" (articolo 4, paragrafo 4) e di "fabbricante" (articolo 4, paragrafo 11)[152].

Un'altra importante novità concerne il concetto di "difetto", disciplinato dall'art. 6. Si statuisce un nuovo "*test* di difettosità" del prodotto, rispetto alla sicurezza «che il grande pubblico può legittimamente attendersi tenuto conto di tutte le circostanze». Questo *test*, coincidente, in sostanza, con quello previsto dalla direttiva attualmente vigente, è adeguato ai nuovi prodotti, con l'imposizione di considerare criteri riferiti, in modo specifico, agli *smart devices*, quali: i requisiti di *cyber-security*; i potenziali effetti negativi sul prodotto causati dalla sua capacità di apprendere successivamente al rilascio sul mercato [153] e «gli effetti sul prodotto di altri prodotti che ci si può ragionevolmente attendere siano utilizzati» insieme allo stesso, prendendo in considerazione la connettività tra i sistemi[154].

In tale ottica, vengono in rilievo i danni provocati dalla circostanza che prodotti, come i robot, i droni o i sistemi domestici intelligenti, siano resi insicuri da aggiornamenti *software*, dall'intelligenza artificiale oppure da servizi digitali necessari per il funzionamento del prodotto; nonché quelli che siano cagionati dalla condotta dei produttori che non gestiscano la vulnerabilità dei sistemi informatici[155].

Ad ogni modo, la proposta chiarisce che tutti i parametri di sicurezza obbligatori, sia quelli stabiliti dall'Unione Europea, sia quelli previsti in ambito nazionale, debbono essere presi in considerazione in sede giudiziale, quando si valuti la difettosità di un prodotto.

L'art. 7, nel regolamentare la responsabilità degli "operatori economici", definisce "la gerarchia delle responsabilità" tra i soggetti coinvolti nella catena di approvvigionamento del prodotto difettoso, in misura proporzionata al ruolo di ciascuno di essi. È, in tal modo, garantita la ricerca dell'operatore responsabile, ai fini del risarcimento del danno[156]. Tra i soggetti responsabili in prima linea, si pone il fabbricante del prodotto e quello della componente che

---

[151] Le nuove regole non permetteranno, nondimeno, il risarcimento per la violazione dei diritti fondamentali, come quando l'impiego discriminatorio di un *software* di reclutamento impedisca l'esito positivo di un colloquio di lavoro. Cfr. *Presse release*, 28 september 2022, Bruxelles, "*New liability rules on products and AI to protect consumers and foster innovation*", consultabile *online* sul sito https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5807".

[152] Progetto di parere, CESE, cit., punto 4.5.

[153] Cfr. S. Neri, R. Almanza, *Percorsi di riforma: la responsabilità da prodotto difettoso alla prova dell'AI*, consultabile *online* sul sito hhtps://www.wfw.come/articles, 9 febbraio 2023.

[154] Cfr. G. Proietti, *Responsabilità per danno da prodotti difettosi alla luce degli ultimi sviluppi tecnologici*, consultabile *online* sul sito www.dirittobancario.it, 27 ottobre 2022, par. 3.

[155] Cfr. *Presse release*, 28 september 2022, Bruxelles, "*New liability rules on products and AI to protect consumers and foster innovation*", cit.

[156] Sul punto cfr. Progetto di parere, CESE, punti 3.3., 4.1.

sia la causa del difetto cagionato. Potranno essere responsabili, oltre ai fabbricanti di *hardware*, anche i fornitori di *software* e di servizi digitali che incidano sul funzionamento del prodotto[157]. Qualora si tratti di un fabbricante stabilito al di fuori dell'Unione Europea, può essere ritenuto responsabile l'importatore o, in sua mancanza, il rappresentante autorizzato dal fabbricante. Vengono anche indicati, come responsabili, il fornitore di servizi di logistica, il distributore o il fornitore di una piattaforma *on line*.

L'art. 11 dispone che, qualora vi siano due o più operatori economici responsabili dello stesso danno, ai sensi della direttiva, gli Stati membri devono assicurare che rispondano solidalmente.

In più, la proposta di direttiva introduce due importanti nuove misure, nella prospettiva della mitigazione dell'onere probatorio del soggetto danneggiato: una sulla divulgazione degli elementi di prova, già disciplinata dalla maggior parte degli Stati membri; l'altra sulla presunzione del carattere difettoso del prodotto o del nesso di causalità tra difetto e danno, già oggetto di "codificazione" negli indirizzi giurisprudenziali, considerati favorevoli all'attore[158].

L'art. 8 stabilisce che gli Stati membri devono attivarsi, affinché il danneggiato, quando ricorrano fatti e prove sufficienti a sostenere la plausibilità della domanda risarcitoria, possa ottenere dal Tribunale un ordine, nei confronti del convenuto, di "divulgare" gli elementi di prova a sua disposizione che siano pertinenti, a condizione che costui si sia rifiutato di esibirli spontaneamente. Tale divulgazione è da intendersi, nel nostro ordinamento, come un ordine di esibizione che dovrà rispondere al principio di proporzionalità, considerando i legittimi interessi di tutte le parti e al principio di necessità, ovverosia nei limiti della richiesta risarcitoria[159].

Si osservi che la fissazione di regole sulla divulgazione di prove rilevanti da parte di coloro che ne dispongano, ai fini dell'accertamento della responsabilità, è importantissimo per i danneggiati, per i quali l'accesso alle informazioni suddette avrà un ruolo determinante nella decisione di agire in giudizio; come pure, in quanto rappresenterà un incentivo per gli operatori economici a rispettare gli obblighi di documentazione delle informazioni pertinenti, stabiliti dalla proposta della c.d. legge sull'intelligenza artificiale[160].

La proposta di direttiva, dopo aver ribadito la necessaria dimostrazione, da parte del danneggiato, del danno, del difetto e del nesso di causalità tra difetto e danno, interviene con l'intento di alleggerire l'onere della prova a carico di quest'ultimo. A tale scopo, l'art. 9, par. 2, prevede una presunzione di difettosità del prodotto, quando il convenuto non abbia adempiuto all'obbligo di divulgazione, di cui all'art. 8; nelle ipotesi in cui il ricorrente provi che il prodotto non è conforme ai requisiti di sicurezza obbligatori, finalizzati alla protezione dalla medesima tipologia di rischio, di cui al danno verificatosi ovvero dimostri che il danno è stato provocato da un evidente malfunzionamento del prodotto, durante il normale utilizzo o in circostanze ordinarie.

---

[157] Cfr. G. PROIETTI, *op.cit*, par. 2.
[158] Progetto di parere, CESE, cit., punto 4.8.
[159] Cfr. G. PROIETTI, *op.cit.*, par. 3.
[160] Cfr. considerando 16 della c.d. *AI Liability Directive*.

L'art. 9, par. 3, prevede una presunzione relativa del nesso di causalità tra il difetto del prodotto e l'evento dannoso, quando è stato accertato che il prodotto è difettoso e che il danno causato è di natura tipicamente coerente con il difetto in questione.

L'art. 9, par. 4, interviene sulla delicata questione delle imponenti difficoltà probatorie (sollevate, in particolar modo, dalla capacità di autoapprendimento dei sistemi di intelligenza artificiale), disponendo che, quando il giudice nazionale ritenga che il ricorrente abbia difficoltà eccessive, nei casi caratterizzati dalla particolare complessità tecnica o scientifica sulla prova del difetto o sul nesso di causalità o su entrambi, sussisterà una loro presunzione. Ciò succede se il danneggiato dimostri, sulla base di prove sufficientemente rilevanti, che il prodotto abbia contribuito a cagionare il danno e che sia probabile che lo stesso fosse difettoso o che il suo carattere difettoso sia una possibile causa del danno o entrambi gli aspetti. Il convenuto avrà, comunque, il diritto di contestare l'esistenza delle difficoltà eccessive o delle probabilità suddette (art. 9, par. 5).

Inoltre, la proposta della Commissione regolamenta le ipotesi, in cui i pregiudizi si verifichino, anni dopo l'acquisto o la messa in circolazione del prodotto nel mercato.

L'art. 10, par. 1, lett. c), include, tra i casi di esonero dalla responsabilità, quello in cui sia probabile che il difetto che abbia prodotto il danno non sussistesse, al momento della immissione del prodotto sul mercato, oppure, nel caso di un distributore, al tempo della sua messa a disposizione ovvero che tale difetto sia sopravvenuto dopo tale momento. In deroga a tale previsione, l'esimente non troverà applicazione, quando la difettosità del prodotto, in costanza di controllo da parte del fabbricante, sia dovuta a una delle seguenti cause: un servizio correlato; il *software*, compresi gli aggiornamenti o i suoi potenziamenti; la mancanza delle migliorie o degli aggiornamenti del *software*, necessari per mantenere la sicurezza (art. 10, par. 2)[161].

Nella proposta di revisione, permane l'esonero da responsabilità per il c.d. rischio da sviluppo (art. 10, par. 1, lett. e)), il quale, contrariamente alla disciplina oggi vigente, non potrà essere oggetto di deroga da parte degli Stati membri.

Pare chiaro che, con tale previsione, la Commissione europea si è posta l'obiettivo di realizzare la piena armonizzazione della disciplina europea del

[161] Al riguardo, particolarmente interessanti sono le riflessioni dottrinali, effettuate già prima della proposta di revisione della direttiva, oggetto di analisi, in relazione all'inapplicabilità ai prodotti digitali dell'esimente del "difetto sopravvenuto". L'Autrice parte dalla precisazione che i beni digitali sono connotati da *openness by design*, ossia sono concepiti per non essere completi di tutto ciò che occorre, al momento della loro messa in circolazione, e per essere soggetti a successive integrazioni ed aggiornamenti delle componenti immateriali e/o per richiedere accesso a dati, sistemi e reti, etc. Di qui, si sostiene che è richiesto un nuovo punto di vista, nel senso che l'*an* ed il *quomodo* delle modificazioni, cui il prodotto è soggetto, vengono in rilievo a partire dal suo stesso *design*, anche allo scopo dell'individuazione di un difetto di progettazione. In aggiunta, il fabbricante mantiene una stretta relazione con il prodotto e con il suo utente, anche a seguito della sua messa in circolazione, nell'ambito di rapporto che può definirsi "di durata", ed è pertanto in grado di acquisire conoscenza dei rischi insiti nello stesso e di gestirli. In questa prospettiva, qualora il danno sia cagionato dagli elementi aggiunti dopo l'immissione in commercio (ad esempio, dal malfunzionamento dell'app scaricata da internet, etc.), ma concepiti come elementi di un unitario prodotto, il produttore non potrà avvalersi dell'esimente del difetto sopravvenuto. Alla stessa stregua, neanche l'imprevedibilità delle azioni della macchina, riscontrabile nei prodotti di *machine learning*, varrebbe ad escludere la responsabilità del produttore, affermando che il difetto sia sopravvenuto. Cfr. R. MONTINARO, *op.cit.*, p. 359 ss.

rischio da sviluppo, superando il dettato della direttiva 85/374/CEE che aveva rimesso agli Stati membri la libertà di scegliere se farlo gravare in capo al consumatore oppure al produttore.

Sicché, in futuro, a seguito del recepimento della direttiva di revisione di quella attualmente vigente, tutte le discipline nazionali europee allocheranno il rischio da sviluppo tecnologico scientifico in capo all'utilizzatore del prodotto, esonerando l'impresa dalla responsabilità, ogni qualvolta il difetto sarà già esistente ed oggettivamente imputabile al produttore, al momento della messa in circolazione del prodotto nel mercato, ma la scienza e le conoscenze tecniche non consentiranno di identificarlo.

Siffatta causa di esclusione della responsabilità del produttore ha un'indiscutibile valenza politica, dal momento che favorisce la circolazione sul mercato di prodotti nuovi e la competitività delle imprese[162].

Da un altro punto di vista, a tali finalità, sottese all'indirizzo legislativo, si contrappone l'esigenza di garantire la sicurezza dei prodotti e di proteggere i consumatori danneggiati.

Si è, a tal proposito, sostenuto che l'eccezione del rischio da sviluppo contrasterebbe con il principio giuridico europeo di precauzione[163], finalizzato ad offrire una tutela anticipata, allorquando non vi sia certezza scientifica sul grado di offensività di una determinata attività d'impresa o di determinati beni o servizi, ma sussista il semplice sospetto che siano potenzialmente pericolosi e che possano provocare un rischio ad interessi "sensibili", quali l'ambiente, la salute umana, la sicurezza degli utenti o dei consumatori [164].

In Italia, ove il legislatore si è allineato all'opzione, accolta da taluni Stati membri, di introdurre l'esimente del rischio da sviluppo[165], si è consolidato l'orientamento giurisprudenziale che ha fatto ricorso al regime di responsabilità contemplato dall'art. 2050 c.c., quale alternativa rispetto alla disciplina della responsabilità del produttore, proprio al fine di assicurare un'adeguata tutela a coloro che subiscano danni, cagionati da rischi che non era possibile prendere in considerazione, al momento in cui la sicurezza del prodotto è stata valutata dal produttore[166].

---

[162] Cfr. D. Caruso, R. Pardolesi, *Per una storia della Direttiva 1985/374/CEE*, in *Danno resp.*, 2012, p. 9 ss.

[163] Cfr. G. Comandé, *La responsabilità civile per danno da prodotto difettoso…assunta con precauzione*, in *Danno e resp.*, 2013, p. 107; F. Santonostaso *Principio di «precauzione» e responsabilità d'impresa: rischio tecnologico e attività pericolosa «per sua natura». Prime riflessioni su un tema di ricerca*, in *Contratto e impresa Europa*, 2005, p. 78. Sul tema, *ex multis*, cfr. D. Cerini, *Responsabilità del produttore e rischio da sviluppo oltre la lettera della Direttiva 85/374/CEE*, in *Dir.econ.ass.,* 1996, p. 29; U. Rizzo, *op.cit.,* p. 380 ss.; G. Visintini, *L'esimente del rischio da sviluppo come criterio della responsabilità del produttore (l'esperienza italiana e tedesca e la direttiva comunitaria*), in *Resp.civ.prev.*, 2004, p. 1267.

[164] Cfr. F. Stella, *Il rischio da ignoto tecnologico e il mito delle discipline,* in Aa.Vv., *Il rischio da ignoto tecnologico*, Milano, 2002, p. 10 ss.; V. F. De Leonardis, *Il principio di precauzione nell'amministrazione del rischio*, Milano, 2005, p. 20; G. Comandé, *L'assicurazione e la responsabilità civile come strumenti e veicoli dell'analisi economica del diritto*, in ID. (a cura di), *Gli strumenti della precauzione: nuovi rischi, assicurazione e responsabilità*, Milano, 2006, p. 23 ss., p. 45 ss

[165] Il legislatore italiano è stato spinto da ragioni di politica del diritto di non creare uno svantaggio competitivo alle imprese italiane e di non scoraggiare le imprese straniere ad investire in Italia. Cfr. V. Buonocore, *L'impresa*, Torino, 2002, p. 302.

[166] Cfr. E. Al Mureden, *La conformità dei prodotti agli standard tecnici tra tutela del consumatore e limiti alla responsabilità del fabbricante*, in *Actualidad Juridica Iberoamericana*, n. 17, 2022, p. 894 s., p. 902 s. Cfr. L. Cabella Pisu, *op.cit.*, p. 645 che parla di una vera e propria casistica parallela. Si è parlato di una «fuga dalla disciplina del danno da prodotto difettoso», con il consolidarsi dell'orientamento che ha fatto ricorso ad altre forme di responsabilità, principalmente alla responsabilità per l'esercizio di attività pericolose, per

Si è parlato, al riguardo, di un "aggiramento" della tenuta tecnica dell'eccezione del rischio da sviluppo, operato dalla giurisprudenza, attraverso una lettura 'precauzionale' delle regole generali di imputazione della responsabilità civile, in modo puntuale della responsabilità per attività pericolose[167].

Per comprendere la portata di tale indirizzo giurisprudenziale, si precisi che l'art. 2050 c.c. viene prevalentemente interpretato ed applicato, "nel diritto vivente" come un'ipotesi di responsabilità oggettiva "per rischio di impresa"[168]. Ciò fa sì che, allorché l'attività venga classificata come pericolosa, la giurisprudenza maggioritaria tenda a non considerare mai raggiunta la prova liberatoria, posta in capo all'esercente l'attività, che esula dalla dimostrazione dell'assenza di colpa e consiste nella dimostrazione di aver adottato tutte le misure idonee a prevenire il danno[169]. Tale prova è, difatti, divenuta talmente rigorosa da essere equiparata al caso fortuito[170].

La regola, di cui all'art. 2050 c.c., è stata ampliamente applicata dalla giurisprudenza, allo scopo di garantire al soggetto danneggiato una posizione di favore, anche allorquando l'attività svolta dal danneggiante risulti poco rappresentativa sul piano del pericolo: le corti hanno invocato la sussistenza dell'elemento della pericolosità anche in casi relativi ad attività non pericolose in sé, ma che divengono tali, in riferimento ai soggetti che siano destinatari delle stesse[171].

---

offrire una risposta alle problematiche correlate ai danni cagionati dalla produzione di massa. Cfr. R. MONTINARO, *op.cit.*, p. 352; ID. *Dubbio scientifico e responsabilità civile*, Milano, 2012, p. 155 ss. Numerosissimi i contributi sul tema. *Ex multis*, cfr. G. COMANDÉ, *L'assicurazione e la responsabilità civile come strumenti e veicoli dell'analisi economica del diritto*, *op.cit.*, p. 23 ss.; F. DEGL'INNOCENTI, *Rischio di impresa e responsabilità civile. La tutela dell'ambiente tra prevenzione e riparazione dei danni*, Firenze University Press, 2013, p. 48 ss.

[167] Cfr. G. COMANDÉ, *La responsabilità civile per danno da prodotto difettoso*, *op.cit.*, p. 109. Per una lettura restrittiva del principio di precauzione, in rapporto all'applicabilità dell'art. 2050 c.c., C. CASTRONOVO, *Sentieri di responsabilità civile europea*, in *Europa dir. priv.*, 2008, p. 787.

[168] Influente dottrina ha sviluppato questa tesi, alla luce di un'interpretazione sistematica delle fattispecie di responsabilità speciali di cui agli artt. 2050-2054 c.c., strettamente correlata al *rischio* di impresa ed alle ripercussioni sul mercato assicurativo, fattori significativi che incidono sulla ripartizione dei danni e dei relativi costi dei consociati. L'Autore ha puntualizzato che la funzione della responsabilità oggettiva non è di punire, bensì di imputare a chiunque il «rischio oggettivamente creato» dalla propria attività, nella misura in cui esso sia esprimibile in costo ed amministrabile dal punto di vista economico, con le conoscenze e con i mezzi di previdenza che un buon amministratore abbia a propria disposizione. Cfr. P. TRIMARCHI, *Rischio e responsabilità oggettiva*, Milano, 1961, pp. 193 ss. La dottrina e la giurisprudenza prevalente e più recente si sono discostate dall'indirizzo più risalente che qualificava la responsabilità per l'esercizio delle attività pericolose come responsabilità per colpa, pur se "aggravata", con semplificazione dell'onere probatorio a favore del danneggiato; per configurarla, differentemente, come responsabilità oggettiva. Tra le voci più autorevoli che hanno configurato il regime di cui all'art. 2050 c.c. come responsabilità per colpa « aggravata », si v. A. DE CUPIS, *Il danno. Teoria generale della responsabilità civile*, Milano, 1979, p. 88 ss.; P. FORCHIELLI, *La colpa lievissima*, in *Riv.dir.civ.*, 1963, I, p. 202; E. PARAGLIA, *Appunti in tema di responsabilità da esercizio di attività pericolose*, in *Diritto e pratica nell'assicurazione*, 1975, p. 645. Fautori della ricostruzione della responsabilità oggettiva sono M. FRANZONI, *Responsabilità per l'esercizio di attività pericolose*, in G. ALPA, M. Bessone (diretta da), *La responsabilità civile. Una rassegna di dottrina e giurisprudenza*, Torino, 1987, p. 459 ss.; P.G. MONATERI, *La responsabilità civile*, in R. SACCO (diretto da), *Trattato di diritto civile*, Torino, 1998, p. 674 ss.

[169] Cfr. E. AL MUREDEN, *I danni da uso del cellulare tra tutela previdenziale e limiti della responsabilità del produttore*, in *Resp.civ.prev.*, 2010, p. 1392 ss., par. 4 (consultabile *online* sul sito dejure.it), il quale richiama C. CASTRONOVO, *La nuova responsabilità civile*, III es., Milano, 2006, p. 302, il quale afferma che la giurisprudenza «non si accontenta mai».

[170] Cfr. M. FRANZONI, *Responsabilità per l'esercizio di attività pericolose*, op.cit., p. 459.

[171] Come nel caso di attività di maneggio di cavalli, ove si individua il pericolo nella circostanza che i soggetti siano inesperti; Cass., 19 giugno 2008, n. 16637, in *Foro it.*, rep. 2009. Sul punto, cfr. A. FUSARO, *Attività pericolose e dintorni*, in *Riv.dir.civ.* 2013, p. 1339. A livello legislativo, la portata applicativa della norma è stata

Durevole è, poi, il ricorso al regime della responsabilità per attività pericolose, al fine di assicurare una protezione idonea a coloro che subiscano danni da prodotti qualificabili come 'conformi', alla luce della disciplina sulla sicurezza dei prodotti e delle norme tecniche armonizzate, ma la cui pericolosità sia conosciuta, al momento dell'ideazione dello *standard* legislativo e sia deliberatamente inclusa nell'ambito dei rischi correlati, in modo ragionevole, all'uso normale del prodotto. L'applicazione dell'art. 2050 c.c. impedisce al produttore di escludere la propria responsabilità, affermando il carattere non difettoso del prodotto, dedotto dalla conformità dello stesso agli *standard* previsti per la sua immissione nel mercato. L'impiego del regime della responsabilità per attività pericolosa ha, perciò, limitato il rigore dell'impostazione, secondo la quale, una volta approvata la conformità del prodotto agli *standard* legislativi che ne governano la sicurezza, non resterebbe spazio per configurare la responsabilità del fabbricante per i danni da questo cagionati[172]. In tale prospettiva, sono stati considerati pericolosi prodotti quali le bombole del gas [173], i derivati del tabacco [174], i fuochi di artificio e principalmente i farmaci [175] ed è stata loro applicata la disciplina dettata dall'art. 2050 c.c.

L'interpretazione della norma in tali termini ha permesso di attribuire rilevanza anche ai profili di dannosità e di pericolosità 'potenziale' dei prodotti che potrebbero rientrare nei rischi che il produttore non avrebbe potuto prendere in considerazione, al momento in cui la sicurezza del prodotto è stata valutata (c.d. rischio da sviluppo)[176]. Segnatamente l'applicazione dell'art. 2050 c.c. impedisce al produttore di liberarsi dalla propria responsabilità, richiamando l'esimente del rischio da sviluppo[177], dando, così, attuazione al principio di precauzione.

Ordunque, alla luce delle osservazioni svolte, ci si è domandati se il consumatore danneggiato possa scegliere tra la tutela extracontrattuale generale e la tutela extracontrattuale speciale ed invocare il regime della responsabilità per l'esercizio delle attività pericolose, in quanto più favorevole, per lo stesso, dal punto di vista processuale (e più gravoso, viceversa, per il produttore danneggiante), rispetto alla disciplina della responsabilità per danno da prodotto difettoso[178].

---

ampliata, in particolare, dall'art. 15, d.lg. 30 giugno 2003, n. 196 (Codice in materia di trattamento dei dati personali), secondo cui "chiunque cagioni danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile".

[172] Sul punto, cfr. E. AL MUREDEN, *La conformità dei prodotti agli standard tecnici tra tutela del consumatore e limiti alla responsabilità del fabbricante*, *op.cit.*, p. 902.

[173] Cfr. Cass., 26 luglio 2012, n. 13214, in *Giustizia civile. Massimario annotato della Cassazione*, 2012, p. 967.

[174] Tra le numerose pronunce, cfr. Cass., 11 ottobre 2018, n. 25161*, Giur.it.*, 2019, p. 1319; Cass., 21 gennaio 2020, n. 1165, dejure.it.

[175] Per il caso di danni causati da un farmaco antiobesità, cfr. Trib. Roma, 20 aprile 2002, in *Resp.civ.*, 2002, 1107. Sul tema, cfr. A. QUERCI, *Biotecnologie e scienze della vita nelle recenti normative di origine comunitaria: le nuove frontiere della responsabilità civile*, ivi, 2010, 219 s., 231.

[176] Cfr. E. AL MUREDEN, *La conformità dei prodotti agli standard tecnici tra tutela del consumatore e limiti alla responsabilità del fabbricante*, op.cit., p. 902, s.; ID., *I danni da uso del cellulare tra tutela previdenziale e limiti della responsabilità del produttore, op.cit.*, par. 4.

[177] Cfr. E. AL MUREDEN, *op.loc.ult.cit.*; F. CAFAGGI, *La responsabilità dell'impresa per i prodotti difettosi*, in N. LIPARI (a cura di), *Trattato di diritto privato europeo*, Padova, 2003, p. 562 ss.

[178] Sul punto e per le considerazioni che seguono, cfr. R. MONTINARO, *Responsabilità del produttore di farmaci, art. 2050 c.c. e gestione precauzionale del rischio*, in *Resp.civ.*, 2019, p. 1587 ss., par. 2, consultabile online sul sito *dejure.it*

La giurisprudenza ha ammesso la scelta tra tali due regimi, quand'anche ricorrano i presupposti per applicare la disciplina di derivazione europea, ponendo, a fondamento del ragionamento, la circostanza che l'art. 127 c. cons., nel trasporre l'art. 13 della direttiva 85/374/CEE, statuisce che le disposizioni sulla responsabilità da prodotto difettoso «non escludono né limitano i diritti che siano attribuiti al danneggiato da altre leggi»[179].

La letteratura giuridica ha affermato che tale ricostruzione, di fatto, vanifica le finalità armonizzatrici della direttiva sulla responsabilità del produttore e che l'art. 13 deve essere interpretato nel senso che non può ammettersi il cumulo della tutela extracontrattuale, predisposta dalla direttiva e di quella prevista dall'art. 2050 c.c., poiché hanno, in sostanza, la medesima natura extracontrattuale e lo stesso fondamento oggettivo. Si può, per contro, consentire il cumulo tra azione extra-contrattuale, ai sensi del codice del consumo, e l'azione contrattuale, quale quella della garanzia per vizi, nei casi in cui tra produttore e danneggiato esista anche un rapporto contrattuale, per esempio la compravendita[180].

L'indirizzo ermeneutico descritto è stato altresì criticato dalla Corte di Giustizia dell'Unione europea che, in una pronuncia non recente, ha assunto una posizione restrittiva riguardo al rapporto tra la disciplina nazionale di recepimento della direttiva e le normative nazionali di fonte diversa, stabilendo che i diritti riconosciuti al danneggiato, in virtù di una regolamentazione di carattere generale che abbiano lo stesso fondamento della direttiva, possono essere limitati oppure esclusi in ragione dell'applicazione di quest'ultima, frutto di un delicato contemperamento degli interessi del produttore e del consumatore[181].

La Corte di Giustizia ha costantemente condannato ogni «disallineamento», realizzato da parte della giurisprudenza nazionale, ponendo in evidenza che esso finisce col rappresentare «un *vulnus* al valore dell'armonizzazione»[182].

Concludendo, la disciplina di derivazione europea non potrà essere disapplicata, al solo fine di realizzare una tutela rafforzata del soggetto danneggiato, invocando il regime della responsabilità per attività pericolosa che non prevede l'esimente del rischio da sviluppo che, come visto, favorisce la posizione del produttore[183].

Ciò detto, si puntualizzi che la Corte di Giustizia dell'Unione Europea ha interpretato in modo restrittivo il rischio da sviluppo, precisando che, nel determinare l'ambito di estensione delle conoscenze scientifiche e tecniche previste dalla direttiva, si dovrà escludere la responsabilità del produttore

---

[179] Tra le numerose pronunce, cfr. Cass. civ., 27 luglio 1991, n. 8395, in *Giur. it.*, 1992, I, 1331, con nota di A. BARENGHI, *In tema di farmaci difettosi*; Cass. civ., 20 luglio 1993, n. 8069, in *Resp.civ.*, 1994, p. 61, con nota di A. BUSATO, *I danni da emoderivati: le diverse forme di tutela*, in *Foro it.*, 1994, I, 455; Cass. civ., 1° febbraio 1995, n. 1138, *ivi*, 1996, 144, con nota di S. BASTIANON, *La Cassazione, il « Trilergan » e la responsabilità per danni da emoderivati infetti.*

[180] Cfr. L. CABELLA PISU, *op.cit.*, p. 621.

[181] Cfr. Corte giust. CE, 25 aprile 2002, causa C-183/00, in *Foro it.,* 2002, IV, 294, con nota di A. PALMIERI, R. PARDOLESI, *Difetti del prodotto e del diritto privato europeo*. Sul punto cfr. G. PONZANELLI*, Armonizzazione del diritto v. protezione del consumatore: il caso della responsabilità del produttore,* in *Danno e resp.*, 2002, 728 s. Sul punto e per le riflessioni che seguono, cfr. R. MONTINARO, *op.ult.cit.*, par. 2.

[182] Cfr. E. AL MUREDEN, *La conformità dei prodotti agli standard tecnici tra tutela del consumatore e limiti alla responsabilità del fabbricante*, *op.cit*, p. 903.

[183] Cfr. L. CABELLA PISU, *op.cit*, p. 631.

soltanto quando, al momento della messa in circolazione del prodotto, il livello 'più alto' delle conoscenze della scienza e della tecnica, "accessibili" in qualsiasi settore produttivo, non consentiva di scoprire l'esistenza del difetto del prodotto[184].

In tale prospettiva, la previsione del rischio da sviluppo deve essere interpretata nel senso che, da un lato, al produttore devono essere imputati tutti i rischi di danno che siano messi in luce dalle più avanzate conoscenze tecnico-scientifiche, sempre che siano accessibili; dall'altro lato, sul danneggiato devono gravare unicamente quei rischi che ricadono al di fuori dello scibile umano[185].

Avendo precipuo riguardo ai prodotti digitali, la nozione di conoscenza oggettiva, disponibile al tempo della messa in circolazione nel mercato degli stessi, assume rilievo, nella misura in cui, di certo, essa influisce sulla valutazione del comportamento del produttore e/o dell'ideatore dell'algoritmo, in riferimento alle applicazioni di intelligenza artificiale. Si terrà conto della circostanza che tali soggetti non hanno saputo né individuare, né prevedere gli elementi di conoscenza scientifica e tecnica che avrebbero permesso loro di valutare il prodotto come non sicuro, dato che propriamente si sarebbe evoluto in una determinata direzione, e che, di conseguenza, li avrebbero spinti ad adottare tutte le misure di precauzione occorrenti per impedire, o quantomeno, limitare il danno[186].

3.2.3.(segue) La proposta c.d. AI Liability Directive.

La proposta c.d. *AI Liability Directive* statuisce l'applicabilità della disciplina alle azioni civili di responsabilità extracontrattuale intentate, nell'ambito di regimi di responsabilità per colpa, da parte di coloro che abbiano subito un danno da un sistema digitale, determinato da un'azione o un'omissione intenzionalmente lesiva o colposa di determinati soggetti coinvolti nella "catena di valore" del sistema.

La proposta rientra, come gli altri provvedimenti *in fieri* esaminati, nella strategia europea di promuovere la diffusione di un'intelligenza artificiale affidabile. Si prefigge, a tal uopo, di ridurre l'incertezza giuridica per le imprese che la sviluppano o la utilizzano, in relazione alla possibile esposizione alla responsabilità, e di garantire efficaci strumenti di tutela ai soggetti danneggiati.

La Commissione europea parte, anzitutto, dalla considerazione che le norme nazionali, vigenti in materia di responsabilità, in particolare per colpa, non sono idonee a gestire le azioni per i danni cagionati da prodotti e servizi basati sull'intelligenza artificiale, considerato che la complessità, l'autonomia e

---

[184] Cfr. Corte CE, 29 maggio 1997, C-300/95, in *Foro it.*, 1997, IV, c. 387, con nota di G. PONZANELLI, *Regno Unito, Corte di Giustizia ed eccezione dello «state of art»*.

[185] Cfr. R. MONTINARO, *Responsabilità da prodotto difettoso, op.cit.,* p. 354. Si sostiene che l'indubbia valenza politica del rischio da sviluppo ha condotto a ricomprendere nel suo ambito unicamente i rischi assolutamente imprevedibili sconosciuti e non i difetti, la cui potenziale presenza sia conosciuta o conoscibile, alla luce dalle più avanzate conoscenze tecnico-scientifiche, ma non siano eliminabili nel corso dei processi produttivi attuali. Cfr. F. SANTONOSTASO, *op.cit.*, p. 99, il quale richiama U. CARNEVALI, *Responsabilità del produttore*, in *Enc.dir., Aggiornamento*, II, 1998, p. 946; V. BUONOCORE, *OP.CIT.* p. 303; A. STOPPA, *Responsabilità del produttore*, in *Dig.disc.priv., sez.civ.*, XVIII, Torino, 1998, p. 135.

[186] Sul punto, cfr. G. CAPILLI, *op.cit.*, p. 481.

l'opacità che li caratterizza possono rendere difficile o eccessivamente costoso, da parte del ricorrente, identificare la persona responsabile e dimostrare che sussistono i presupposti ai fini dell'esito positivo di un'azione di responsabilità.

La Commissione valuta altresì che le strategie nazionali, relative al contesto digitale, rivelano che numerosi Stati membri stanno valutando di predisporre un'azione legislativa in materia di responsabilità civile per l'intelligenza artificiale o che la stanno pianificando concretamente. Si prevede che, qualora non vi fosse un intervento da parte dell'Unione Europea, gli Stati membri adegueranno le norme interne in materia di responsabilità civile alle nuove sfide poste dall'intelligenza artificiale. La c.d. *AI Liability Directive* è, dunque, finalizzata a prevenire la frammentazione che potrebbe provenire da adeguamenti specifici all'intelligenza artificiale, da parte delle norme nazionali in materia di responsabilità civile.

A tale scopo**,** la Commissione ha valutato che la direttiva è lo strumento normativo più idoneo per la proposta in esame, dato che garantisce l'effetto di armonizzazione e la certezza del diritto auspicati, prevedendo, al contempo, la flessibilità per consentire agli Stati membri, nel recepimento nazionale, di integrare le misure armonizzate[187].

In linea con il livello di armonizzazione minima prescelto, i legislatori nazionali potranno adottare o mantenere le normative interne più favorevoli, rispetto alla disciplina dettata dalla proposta di direttiva, purché siano compatibili con il diritto dell'Unione europea (art. 1, n. 4).

La proposta della direttiva presenta la peculiarità di dar luogo ad un'armonizzazione *mirata* delle norme degli Stati membri, in materia di responsabilità civile extracontrattuale per colpa, statuendo disposizioni solamente in materia dell'onere della prova. Non interviene sugli aspetti generali della responsabilità civile, quali la definizione di colpa, di causalità, i diversi tipi di danno che determinano le richieste di risarcimento, la distribuzione della responsabilità sugli autori del medesimo illecito, il concorso di colpa, la quantificazione dei danni e i termini di prescrizione[188].

La Commissione europea, in considerazione della circostanza che i soggetti danneggiati potrebbero dover sostenere costi iniziali molto elevati e affrontare procedimenti giudiziari molto più lunghi rispetto a quanto succede nei casi che non riguardino l'intelligenza artificiale, con la conseguenza che costoro sarebbero dissuasi dall'agire in giudizio, introduce dei meccanismi di alleggerimento probatorio, al fine gestire tali difficoltà, nonché per completare il quadro giuridico delineato con la proposta della c.d. legge sull'intelligenza artificiale[189].

Precisamente la proposta di direttiva prevede due strumenti giuridici di facilitazione dell'onere della prova degli attori, nelle azioni che possono essere basate sul diritto nazionale o sulle altre normative europee.

In primis, è riconosciuto il diritto del soggetto danneggiato di accedere a quegli elementi che possano costituire una prova, nei casi in cui si tratti di un

---

[187] Relazione della Commissione alla proposta, punto 2.

[188] Cfr. G.T. ELMI, S. MARCHIAFAVA, *op.loc.ult.cit.*

[189] Cfr. A NERI, *Verso un nuovo regime della responsabilità da intelligenza artificiale: presunzioni e diritto di accesso alle prove in favore dei soggetti danneggiati*, consultabile *online* sul sito www.wfw.com/articles, 22 dicembre 2022

sistema di intelligenza artificiale "ad alto rischio", come definiti dalla proposta della c.d. legge sull'intelligenza artificiale[190]. L'art. 3 dispone che gli Stati membri debbano predisporre un meccanismo procedurale, per mezzo del quale l'autorità giudiziaria possa ordinare ad un "fornitore", come pure ad un soggetto che soggiaccia agli stessi obblighi di quest'ultimo, o ad un "utente" di esibire quelle prove pertinenti che siano a sua disposizione, relative allo specifico sistema "ad alto rischio". Specularmente a quanto stabilito dalla proposta di direttiva sulla responsabilità per danno da prodotto difettoso, il ricorrente, al fine di ottenere tale ordine, deve presentare, a sostegno della richiesta, fatti e prove sufficienti a sostenere l'ammissibilità della domanda di risarcimento del danno; in più, l'ordine dell'autorità sarà subordinato alla circostanze che uno dei soggetti menzionati si sia rifiutato di esibire gli elementi di prova spontaneamente e che si reputi che il sistema intelligente abbia causato un danno.

L'ordine di esibizione dovrà rispondere ai principi di necessità e di proporzionalità. Quanto a quest'ultimo, l'art. 3, par. 4, nell'imporre ai giudici nazionali di tenere in considerazione gli interessi legittimi di tutte le parti, si riferisce alla tutela dei segreti commerciali, ai sensi della direttiva UE 2016/943 (direttiva c.d. "*trade secret*") ed alla normativa nazionale di recepimento. Si lascia, a tal punto, alle corti di merito l'arduo compito di bilanciare l'interesse sotteso alla richiesta della divulgazione/conservazione degli elementi di prova e l'esigenza di tutela del segreto commerciale[191].

Gli Stati membri dovranno introdurre idonei sistemi di impugnazione delle decisioni relative alle richieste di divulgazione.

Qualora il convenuto non rispetti l'ordine del giudice nazionale di esibire e conservare le prove, secondo quanto previsto dall'art. 3, paragrafi 1 e 2, vi sarà una presunzione di inosservanza di un obbligo di diligenza.

In secondo luogo, la proposta di direttiva elabora presunzioni confutabili, relative all'onere della prova del nesso di causalità[192].

L'art. 4 stabilisce che gli organi giurisdizionali presumono l'esistenza del nesso di causalità tra la colpa del convenuto e l'*output* prodotto da un sistema intelligente o la mancata generazione di un *output* da parte del sistema che abbia cagionato il danno, quando ricorrano le condizioni elencate dalle lett. a), b) e c): la dimostrazione, da parte del ricorrente, dell'inosservanza colposa, da parte del convenuto o di una persona della cui condotta costui è responsabile, degli obblighi di diligenza, previsti dalla disciplina nazionale o europea (quale anche la proposta della c.d. legge sull'intelligenza artificiale), posti a prevenire il danno verificatosi (lett. a)); la ragionevole probabilità, sulla base delle

---

[190] Per il commento all'art. 3 della proposta di direttiva, cfr. G. PROIETTI, *Sistemi di intelligenza artificiale e responsabilità: la proposta di AI liability Directive*, consultabile *online* sul sito www.dirittobancario.it , 6 ottobre 2022, p. 3.

[191] Cfr. G. LUSARDI, *Danni causati dall'intelligenza artificiale, chi paga? Cosa prevede la proposta di direttiva UE,* par. 4, consultabile *online* sul sito www.agendadigitale, 9 dicembre 2022,

[192] Per l'analisi dell'art. 4, cfr. il commento all'art. 4, contenuto nella proposta di direttiva, "*Presumption of causal link in the case of fault* (art. 4)", consultabile *online* sul sito https://ec.europa.eu/info/sites/default/files/1_1_197605_prop_dir_ai_en.pdf, pp.13 s.; G. LUSARDI, *op.cit.,* par. 3; G. PROIETTI, *op.ult.cit.*, p. 4, s.

circostanze del caso concreto, che tale condotta colposa abbia influito sull'*output* creato dal sistema o sulla sua incapacità di produrlo; la prova, fornita dal ricorrente, che l'*output* compiuto dal sistema digitale o la sua incapacità di elaborarlo abbia provocato il danno.

Per i sistemi intelligenti "ad alto rischio", l'art. 4 statuisce un regime differenziato, nel senso che, nell'ambito delle azioni promosse contro i "fornitori" o gli "utenti", la presunzione di causalità è limitata al caso del mancato rispetto degli obblighi previsti dalla proposta di regolamento, rispettivamente richiamati, per i primi, dall'art. 4, par. 2 e, per i secondi, dall'art. 4, par. 3.

Per tale categoria di sistemi intelligenti, sussiste un'eccezione alla presunzione di causalità, laddove il convenuto dimostri che all'attore siano ragionevolmente accessibili le prove e che abbia le competenze idonee a provare il nesso causale.

Quando la richiesta risarcitoria riguardi un sistema "non ad alto rischio" (che non è soggetto ai requisiti obbligatori della proposta della c.d. legge sull'intelligenza artificiale), la presunzione di causalità si applicherà, solo quando la prova del nesso di causalità sia ritenuta eccessivamente complessa per l'attore.

Per i casi in cui il convenuto usi il sistema intelligente nell'ambito di un'attività personale non professionale, la presunzione di causalità si applicherà unicamente quando costui abbia interferito materialmente con le sue condizioni di funzionamento oppure quando fosse tenuto ed in grado di determinarle ed abbia omesso di farlo. Tale previsione esprime il bisogno di contemperare gli interessi delle persone lese e quelli degli utenti non professionali, escludendo l'applicazione della presunzione di causalità, nelle ipotesi in cui tali soggetti non aggiungano rischi con il loro comportamento.

L'articolo 4, par. 7, dispone che il convenuto abbia il diritto di confutare la presunzione di causalità, di cui all'articolo 4, par. 1.

Un riesame dell'applicazione della direttiva, da parte della Commissione europea, è previsto nel termine di cinque anni, allo scopo di presentare una relazione al Parlamento europeo e al Consiglio, nonché al Comitato economico e sociale europeo (art. 5).

Conclusioni.

In chiusura, può osservarsi che il contesto normativo che disciplinerà i sistemi di intelligenza artificiale si sta muovendo nella direzione della prevenzione dei rischi, prevalentemente in riferimento ai sistemi "ad alto rischio", accostando, alla regolamentazione della sicurezza, la normativa sulla responsabilità civile improntata ad un *favor* delle vittime dei danni cagionati da 'tutti' i sistemi digitali[193].

Di fatto, da un lato, la mancata adozione, da parte delle categorie degli operatori economici obbligati, delle misure tecniche ed organizzative di sicurezza, previste dalla proposta della c.d. legge dell'intelligenza artificiale,

[193] Cfr. ID. *op.loc.ult.cit.*

condurrà all'irrogazione di sanzioni amministrative; dall'altro lato, la violazione degli obblighi di conformità ai parametri di sicurezza suddetti determinerà una presunzione di difettosità del *digital device* (ai sensi della proposta di revisione della direttiva sulla responsabilità per danno da prodotto difettoso), oltre che la responsabilità aggravata per colpa presunta del "fornitore" o dell'"utente" e, di conseguenza, l'obbligo di risarcimento del danno (ai sensi della proposta c.d. *AI Liability Directive*)[194].

In realtà, però, la violazione di *standard* di sicurezza prefissati non comporterà automaticamente la "difettosità" del sistema intelligente[195]; così come, l'adesione agli stessi non implicherà necessariamente l'esonero dalla responsabilità in caso di danni, perché il sistema conforme potrebbe essere "difettoso"[196]. In altri termini, il rispetto di certi *standard* denoterà unicamente la conformità ad un astratto modello regolamentare, fissato sulla base di criteri statici e non dinamici, ma ciò non escluderà che il sistema digitale provochi danni a terzi, in sede di utilizzo da parte del fruitore finale[197].

Ad ogni modo, senza dubbio, la predisposizione, accanto alla normativa civilistica della responsabilità civile, della regolamentazione pubblicistica ha il merito di disegnare un panorama normativo, in cui gli strumenti di tutela successiva convergono con quelli di tutela preventiva, fondati sulla valutazione dei rischi e sulla loro limitazione, attraverso l'uso di una serie di misure tecniche predeterminate ed oggetto di costante monitoraggio e aggiornamento, in conformità al principio di precauzione[198].

Deve, tuttavia, muoversi una critica alle Istituzioni europee per il cambio di rotta, nella disciplina della responsabilità civile extracontrattuale, al di fuori del regime della responsabilità per danno da prodotto difettoso.

La c.d. *AI Liability Directive* non si pone nel solco della regolamentazione dettata dalla proposta di regolamento, il cui contenuto è stato raccomandato alla Commissione dal Parlamento europeo, nella Risoluzione sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale.

In primis, a differenza della Commissione che ha optato, nella proposta di direttiva, per l'approccio dell'armonizzazione minima, diversamente il Parlamento europeo aveva prescelto lo strumento normativo del regolamento che avrebbe garantito uniformità, attraverso l'introduzione di regimi di responsabilità pienamente armonizzati.

---

[194] Analogamente a quanto previsto dal GDPR (artt. 83 e 84 *GDPR*), secondo il quale alla mancata adozione, da parte del titolare del trattamento, delle misure impostegli, conseguono ingenti sanzioni amministrative e la violazione degli obblighi determina la responsabilità aggravata per colpa presunta del titolare (e del responsabile) del trattamento e, di conseguenza, l'obbligo di risarcimento del danno, *ex* art. 82. Sul punto, cfr. M. GAMBINI, *op.cit.,* p. 322.

[195] Cfr. U. RUFFOLO, *La responsabilità da artificial intelligence, algoritmo e smart product: per i fondamenti di un diritto dell'intelligenza artificiale self-learning*, in ID. (a cura di) *Intelligenza artificiale. Il diritto, i diritti, l'etica*, op.cit., p. 144.

[196] Cfr. U. RUFFOLO, E. AL MUREDEN, *Authonomous vehicles e responsabilità nel nostro sistema e in quello statunitense*, in *Giur.it.*, 2019, pp. 1709; Cfr. A. FUSARO, *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso europeo*, in *Nuov.giur.comm.*, 2020, pp. 1353,1348.

[197] Cfr. A. AMIDEI, *Intelligenza artificiale e product liability*, *op.cit.*, p. 1722

[198] Cfr. R. CARLEO, *op.cit.*, p. 361. La dottrina sottolinea che tra le cc.dd. "*issues of permittance*" e le "*issues of liability*", sussiste un rapporto di complementarietà e non di reciproca alternatività. Cfr. M. BUTTEN, A. DE STREEL, M. PEITZ, *Eu liability rules for the age of artificial intelligence*, in *Centre of regulation in Europe*, 2021, p. 45.

In secondo luogo, la proposta di regolamento prevedeva un regime di responsabilità oggettiva per gli operatori di sistemi intelligenti "ad alto rischio", regime che, come ampiamente argomentato dall'*Expert Group on liability and new technologies*, risulta essere il più idoneo a garantire la gestione del rischio e ad assicurare un'allocazione dei danni giusta ed efficiente.

Ancora, la proposta di direttiva, incentrandosi esclusivamente sulle difficoltà probatorie, con l'obiettivo di predisporre un assetto unitario in ambito europeo, presenta talune criticità, tra le quali: la difficoltà di identificare, nella catena della produzione e dell'utilizzo di un sistema intelligente, il soggetto responsabile; il richiamo a nozioni di carattere nazionale, come quello della colpa; le differenze che possono sussistere, negli Stati membri, in relazione alla nozione di danno risarcibile e, non da ultimo, il ruolo degli organi giurisdizionali nazionali, che potrebbero creare disomogeneità nel mercato unitario[199].

Alla luce di quanto detto, è auspicabile che l'Unione Europea formuli un nuovo e generale modello di responsabilità civile per i danni cagionati dalle applicazioni di intelligenza artificiale, che vada oltre l'impostazione dell'armonizzazione minima della proposta di direttiva e superi i limiti della proposta di regolamento, raccomandata dal Parlamento europeo[200]; offrendo, per di più, una risposta operativa all'opportunità di introdurre azioni collettive, soprattutto quando gli incidenti algoritmici provochino danni di valore ridotto ad una pluralità di soggetti, e al problema di come finanziare le controversie e alla questione del luogo in cui radicare la causa, quando vi siano conflitti transfrontalieri[201].

Solo così, si potranno realmente proteggere i diritti fondamentali ed i valori europei.

Infine, voglia riflettersi sulla tecnica legislativa adottata dalle Istituzioni europee.

Si premetta che, negli ultimi anni, si è assistito ad un profluvio di iniziative legislative in materia di intelligenza artificiale. Tale circostanza ha indotto la dottrina ad obiettare che il continuo interventismo, volto a "plasmare il futuro digitale europeo", starebbe, effettivamente, manifestando «un eccesso di protagonismo normativo», in materia di regolazione del mercato digitale[202].

In aggiunta, tale settore, «stretto in una morsa giuridica», rischierebbe di essere compresso e di non riuscire ad esprimere le proprie potenzialità[203]. Ci si dovrebbe avvalere dei vantaggi e delle opportunità offerte dalle intelligenze artificiali che rappresentano un "volano" per lo sviluppo economico, scientifico e sociale globale, benché provvedendo a minimizzare i rischi e le criticità che le stesse presentano[204].

La dottrina si è posta il quesito se sia davvero conveniente adottare regole puntuali e specifiche, che rischino di essere superate, in breve tempo, dal

---

[199] Cfr. A NERI, *op.loc.ult.cit.*

[200] Per tali riflessioni, cfr. G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale, op.cit.*, par.4.

[201] Cfr. M. INFANTINO, *op.cit.*, par. 6.

[202] Cfr. autorevolmente T.E. FROSINI, *Dma, Dsa e intelligenza artificiale. L'Europa non stritoli l'innovazione,* consultabile *online* sul sito https://formiche.net/2021/10/dma-dsa-intelligenza-artificiale-frosini/

[203] Cfr. ID., *La privacy nell'era dell'intelligenza artificiale*, consultabile *online* sul sito *DPCE Online,* 2022, 1, vol. 5, p. 281.

[204] Cfr. ID., *L'orizzonte giuridico dell'intelligenza artificiale*, in *BioLaw Journal, Rivista del Biodiritto*, 1/2022, p. 160, consultabile online sul sito https://www.biodiritto.org

progresso tecnologico talmente veloce e mutevole da farle divenire facilmente obsolete[205].

La regolamentazione della materia si dovrebbe improntare sul principio della neutralità tecnologica, ormai affermato in ambito internazionale, in forza del quale il diritto dovrebbe rimanere neutro, rispetto alla tecnologia: la norma giuridica non si dovrebbe riferire ad un livello di sicurezza predeterminato oppure ad una tecnologia peculiare; all'opposto, si dovrebbe limitare a prevedere l'obiettivo da raggiungere, senza individuare le modalità tecniche per la sua realizzazione[206].

In tale direzione, risultano sempre più necessarie «una tavola di principi valoriali» ed una diffusa consapevolezza culturale ed "etica" che possano trovare attuazione sia nella prassi, sia nelle pronunce giudiziali. A fronte dell'imprevedibilità dello sviluppo tecnologico, apparirebbe irragionevole pretendere «un diritto calcolabile» e "perdente" ogni atteggiamento formalistico che escluda il ricorso ai principi e ai valori sui quali la civiltà giuridica si è venuta man mano formandosi[207].

Di qui, l'esigenza di comprendere come, nel contesto tecnologico in continua evoluzione, sia nodale l'impiego di una tecnica legislativa che si serva, più che di "norme ipertrofiche" di dettaglio[208]che impongono dei veri e propri «fardelli burocratici»[209], distintamente di principi, che permettano l'interpretazione che sia idonea alla risoluzione del caso concreto, tenendo conto dell'ambito di riferimento[210].

---

[205] Cfr. T.E. FROSINI, *Dma, Dsa, op.loc.ult.cit.;* P. PERLINGIERI, *Relazione conclusiva*, in *Il trattamento algoritmico, op.cit.,* p. 388 ss.

[206] Cfr. G. FINOCCHIARO, *La proposta di regolamento*, *op.cit.*, par. 1, nota 11, la quale precisa che tale principio si è affermato nell'elaborazione dell'*UNCITRAL*, già nel *Model Law or Electronic Commerce* del 1996.

[207] Per tale ricostruzione, cfr. P. PERLINGIERI, *Relazione conclusiva*, in *Il trattamento algoritmico dei dati tra etica, diritto ed economia, op.cit.,* p. 388 ss.

[208] La locuzione è di T.E. FROSINI, *L'orizzonte giuridico*, *op.cit.,* p. 161.

[209] L'espressione è di G. FINOCCHIARO, *La proposta di regolamento*, *op.loc.ult.cit.*

[210] Cfr. autorevolmente P. PERLINGIERI, *Note sul «potenziamento cognitivo»*, in *Tecnologie e diritto*, 2021, p. 214, il quale rimarca che spetterebbe un ruolo determinante alle autorità indipendenti nazionali e sovranazionali.