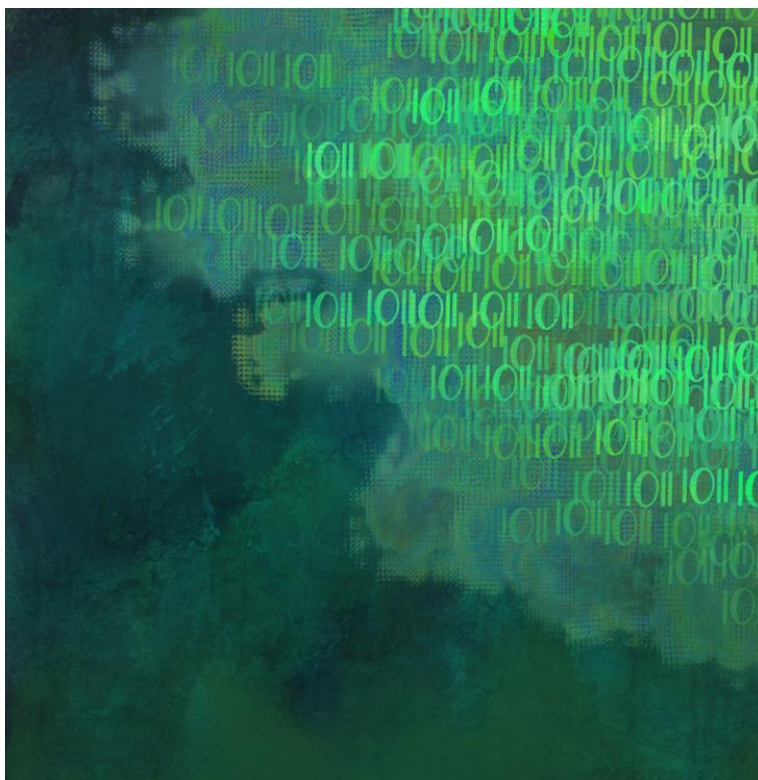


La sostenibilità dell'innovazione digitale

a cura di

Ilaria Garaci e Roberta Montinaro



UniorPress



UNIVERSITÀ DI NAPOLI L'ORIENTALE
DIPARTIMENTO DI SCIENZE UMANI E SOCIALI

La sostenibilità dell'innovazione digitale

a cura di
Ilaria Garaci e Roberta Montinaro



UniorPress
Napoli 2023

In copertina: 0110, Indigo Picciano, 2023.

La sostenibilità della innovazione digitale
a cura di Ilaria Garaci e Roberta Montinaro
UniorPress, Napoli 2023. ISBN 978-88-6719-276-2



With the support of the
Erasmus+ Programme
of the European Union

Edizione digitale con licenza
Creative Commons Attribution 4.0 International



UniorPress - Via Nuova Marina 59, 80133 - Napoli
www.uniorpress.unior.it

INDICE

ROBERTA MONTINARO	
<i>La sostenibilità dell'innovazione digitale. Un'introduzione</i>	7
ENRICO CATERINI	
<i>Artificial intelligence, persona e soggetto</i>	23
MARCO FASCIGLIONE	
<i>I diritti umani nell'era degli algoritmi e dell'intelligenza artificiale</i>	89
ILARIA GARACI	
<i>La valutazione d'impatto sui diritti fondamentali dei minori di età nell'ambiente digitale. Riflessioni a margine della proposta di direttiva relativa alla due diligence delle imprese ai fini della sostenibilità e del Digital Services Act</i>	113
FRANCESCO MEZZANOTTE	
<i>Rischio e responsabilità nei sistemi dell'Internet of Things</i>	137
ANTONINA ASTONE	
<i>Consensus ed intelligenza artificiale: limiti e prospettive</i>	187
ANTONELLA CORRENTI	
<i>Piattaforme tecnologiche: protezione ed educazione dell'utente all'utilizzo delle infrastrutture informatiche nei mercati a concorrenza imperfetta</i>	217
ROSARIO PETRUSO E GUIDO SMORTO	
<i>Trasformazione della filiera distributiva e responsabilità delle piattaforme del commercio elettronico nella proposta di direttiva "sulla responsabilità per danno da prodotti difettosi"</i>	245
ENRICO AL MUREDEN	
<i>Tutela della persona e limitazione dell'errore umano tra Advanced Driver Assistance Systems e guida automatizzata di livello 3</i>	299

MARCO CARLIZZI	
<i>Sostenibilità e innovazione nell'attività bancaria: il conto di base come soluzione per chi abbia ridotte capacità cognitive</i>	323
ETTORE BATTELLI	
<i>Gli smart-contract nel mercato delle assicurazioni: limiti e opportunità</i>	361
GIOVANNI BERTI DE MARINIS	
<i>L'algo-governance nelle imprese di assicurazione e l'integrazione dei fattori ESG</i>	405
SARA LANDINI	
<i>Sostenibilità e diritto dei privati. Il caso dei contratti sostenibili nel settore turistico</i>	431
INDICE DEGLI AUTORI IN ORDINE ALFABETICO	459

La sostenibilità dell'innovazione digitale. Un'introduzione

ROBERTA MONTINARO

SOMMARIO: 1. Innovazione digitale e sostenibilità: un chiarimento concettuale. – 2. Politiche ed iniziative legislative recenti nel panorama del diritto europeo. - 3. Il ruolo del diritto. - 4. l'IA per la sostenibilità e la sostenibilità dell'IA.

1. Innovazione digitale e sostenibilità: un chiarimento concettuale

La sostenibilità, riferita allo sviluppo in generale ed a quello tecnologico in particolare, costituisce un concetto elaborato nel campo delle discipline economiche e da qualche tempo in qua transitato nell'ambito dell'etica, della politica e del diritto¹. Il giurista ha quale punto di riferimento il concetto di sostenibilità desumibile dall'Agenda ONU 2030 ove essa è declinata prestando attenzione alle tre dimensioni, economica, sociale ed ambientale, tra loro interconnesse².

La transizione verso una economia e società digitali può creare i presupposti essenziali per le trasformazioni necessarie al fine di perseguire la sostenibilità in questa triplice dimensione, ma è anche in grado di mettere in pericolo il raggiungimento dei relativi obiettivi³.

Le tecnologie digitali sono dotate della capacità di conformare i rapporti sociali ad ogni livello (dai rapporti tra privati a quelli tra privati e sfera pubblica)⁴. Non a caso gli studiosi di teoria della regolazione le qualificano come 'emergenti' nel significato di idonee a mettere in crisi le categorie concettuali con cui le diverse discipline sono solite interpretare e decifrare il proprio oggetto. Basti pensare – per limitarci a pochi esempi attinenti al campo del diritto ed in particolare del diritto privato – alle categorie di persona e soggetto⁵, identità dell'individuo⁶, bene, proprietà e responsabilità⁷, etc.

L'evoluzione incontrollata delle tecnologie digitali, tra le altre conseguenze, ha determinato il raggiungimento, da parte di pochi attori privati di grandi dimensioni, della c.d. sovranità dei dati (che si è tradotta in sovranità sulla conoscenza estraibile da quei dati), la quale non solo contraddice l'obiettivo della riduzione delle disuguaglianze, ma anzi crea un sempre più marcato divario tra le imprese dell'economia digitale e le autorità pubbliche. Inoltre, sul piano economico, essa determina squilibri tra attori economici di grandi dimensioni e piccole e medie imprese, con tutte le ricadute pregiudizievoli che un simile squilibrio determina⁸, nonché tra imprese e consumatori⁹. Attraverso il controllo delle informazioni¹⁰ ed il monitoraggio degli individui, poi, le piattaforme digitali tendono ad influenzare le relazioni di mercato ma anche l'autodeterminazione dei singoli¹¹ e l'esercizio delle libertà democratiche¹². Infine, lo sviluppo delle tecnologie digitali va adeguatamente gestito per evitare che si traduca nella creazione di nuove barriere nel mercato del lavoro e nell'accesso ai sistemi educativi.

Da qui l'importanza di un'adeguata *governance* al fine di impedire un'estensione incontrollata del potere delle grandi imprese di *information and communication technology*¹³, in considerazione della incidenza su economia e società, dispiegata dalle scelte degli operatori online concernenti l'impiego dei dati e la costruzione dei sistemi intelligenti¹⁴.

2. Politiche ed iniziative recenti nel panorama del diritto europeo

La sostenibilità dell'innovazione digitale, nelle tre accezioni considerate, è al centro di politiche e iniziative legislative recenti dell'UE.

In ordine alle prime, le istituzioni europee hanno acquisito consapevolezza che la transizione verso un'Europa maggiormente sostenibile dal punto di vista economico, ambientale e sociale deve andare di pari passo con la digitalizzazione¹⁵. La Risoluzione del Parlamento Europeo del 25 novembre 2020 "Verso

un mercato unico più sostenibile per le imprese e i consumatori”, individua come necessaria la regolamentazione delle informazioni e della pubblicità online, attraverso il controllo delle pratiche di raccolta dei dati personali e dei modelli di business, adottati dagli intermediari online.

Quanto alle iniziative legislative, il pensiero corre innanzitutto al c.d. *EU Digital Package*¹⁶, ma anche al c.d. *European Democracy Action Plan*¹⁷ della Commissione Europea. È invero indubbio che il *Digital Markets Act* (Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), d’ora in poi ‘DMA’) persegue obiettivi di sostenibilità economica (in chiave di ridimensionamento e controllo dell’operato delle piattaforme che abbiano il ruolo di *gatekeepers*). Parimenti, il *Digital Services Act* (Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), d’ora in poi ‘DSA’)¹⁸ reca in premessa un riferimento esplicito alla sostenibilità, laddove precisa che la dipendenza delle nostre economie e società dai servizi digitali ha reso ancor più evidente la natura bifronte di questi ultimi, in quanto strumenti in grado, allo stesso tempo, di promuovere e di ostacolare il raggiungimento degli obiettivi dello sviluppo sostenibile¹⁹.

Il DSA ha di mira la sostenibilità sociale, ad esempio, quando enuncia tra i propri obiettivi la creazione di un quadro giuridico di riferimento in grado di salvaguardare i diritti ed i legittimi interessi di tutte le parti coinvolte. Il regolamento non trascura del tutto nemmeno la sostenibilità ambientale della digitalizzazione, laddove sottolinea la necessità di promuovere la crescita sostenibile e la sostenibilità dell’e-commerce, mettendo in luce il ruolo che possono svolgere gli intermediari online nella transizione

verso una produzione ed un consumo sostenibili (astenedosi dal ricorrere a pratiche di disinformazione ed a falsi *green claims*; o fornendo ai consumatori informazioni circa l'incidenza sull'ambiente dei prodotti e dei servizi resi loro disponibili).

Il già ricordato *European Democracy Action Plan*, invece, incita ad andare oltre la considerazione della mera dimensione economica delle politiche europee, preoccupate esclusivamente di costruire un efficiente Mercato Unico Digitale, nella consapevolezza che il monopolio delle informazioni da parte dei Giganti della Rete e l'opacità della 'decisione algoritmica'²⁰ trascende oramai la regolamentazione del mercato per toccare il tema della sovranità.

La regolazione della circolazione dei dati (personali e non) riveste invero un ruolo primario. La 'data governance' europea, come disegnata dalla European Data Strategy²¹ e dalle relative misure di attuazione, già adottate (Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati), d'ora in poi 'DGA') e in studio (Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati), COM/2022/68 final, d'ora in poi 'Data Act'), appare – almeno nelle intenzioni dichiarate – muoversi nella direzione²² di promuovere la tutela degli interessati favorendo al tempo stesso la creazione di un'economia dei dati e lo sviluppo delle tecnologie digitali e dell'Intelligenza artificiale, in vista del benessere e dell'inclusione sociale. In tale contesto un'ambiziosa frontiera è rappresentata dall'uso – e ancora prima dall'accesso ai dati (concepiti come '*commons*') – per il bene pubblico²³, nonché dal superamento degli ostacoli che si frappongono al ricorso alla digitalizzazione come mezzo per assicurare la realizzazione degli obiettivi di sviluppo sostenibile, i c.d. SDG, primo fra

tutti quello rappresentato dalla corrente posizione di controllo (eminentemente privato) delle infrastrutture necessarie a tal fine²⁴.

Viceversa, la sostenibilità ambientale appare essere stata del tutto obliterata nella enucleazione delle policy relative alla *data governance*²⁵.

3. Il ruolo del diritto

Compito del diritto è imprimere una direzione allo sviluppo tecnologico, tale da rendere quest'ultimo sostenibile dal punto di vista sociale ed economico, prima ancora che ambientale.

Scendendo dal piano delle emunzioni di principio a quello della regolazione, si nota che produzione legislativa (ad ogni livello) ed interpretazione giuridica sono entrambe cruciali a questo fine. Entrambe debbono essere orientate, innanzitutto, a conformare l'architettura dei poteri privati, ad esempio, ponendo fine o prevenendo la formazione di posizioni dominanti nei mercati di riferimento. Occorre poi promuovere la responsabilizzazione di tutti gli attori, pubblici e privati; a tale ultimo fine, appare essenziale, sia stimolare l'acquisizione di consapevolezza da parte delle istituzioni, comunità ed individui, sia e soprattutto creare i necessari incentivi affinché la stessa concezione delle tecnologie avvenga tenendo conto dei rischi di danno per i diritti di singoli e gruppi, nonché delle conseguenze sociali svantaggiose.

La sostenibilità dell'ambiente digitale non può essere affidata esclusivamente alla prospettiva, che è stata sino ad ora imperante, della privatizzazione dei relativi rapporti, la quale si è rivelata inadeguata a fronteggiare da sola le sfide della rivoluzione digitale. A questo riguardo, uno Studio del Consiglio d'Europa (DGI (2020)¹⁶ "*Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe's standards on human rights, democracy and the rule of*

law”) sottolinea come gli strumenti di *soft law* - seppur utili per preparare il terreno alla futura legislazione grazie alla partecipazione dei diversi attori economici ed istituzionali - possono essere viziati da conflitti di interesse ed animati dal fine di impedire l'adozione di regolamentazioni vincolanti.

Di recente, il legislatore europeo ha dato mostra di voler sposare - e rendere imperativi - i modelli di *corporate social responsibility*, con i connessi doveri di *due diligence* e *risk assessment*²⁶, elaborati da strumenti di *soft law*²⁷. Nel DSA, si impone invero a taluni operatori dell'economia digitale, piattaforme e motori di ricerca molto grandi, di compiere una valutazione dei rischi sistemici da includere nelle procedure di gestione dei rischi²⁸. Le scelte degli operatori online relative all'adozione di certi modelli economici, specie di quelli che coinvolgono dati degli utenti e comportano l'impiego di sistemi intelligenti²⁹, debbono tenere conto degli esiti di una simile valutazione.

La ricordata disciplina non reca alcuna menzione dei fattori di sostenibilità introdotti dall'Agenda ONU; e, tuttavia, molti dei rischi sistemici, elencati in modo non esaustivo dall'art. 34, 2 (a), si pongono in diretto rapporto con tali fattori, tanto è vero che si auspica una applicazione del DSA che sia in linea di continuità con i principi di sostenibilità sociale, di cui alla *European Commission Corporate Governance Initiative*³⁰, alla luce altresì del principio di precauzione³¹.

Non meno importante è però garantire l'accesso a tutele effettive, non solo attraverso l'introduzione di nuove regole, laddove necessario, ma anche per mezzo di un'accorta attività di adeguamento, se del caso in via di interpretazione, delle discipline già esistenti. Effettività delle tutele vuol dire elevata capacità deterrente, nonché coerenza nel loro *enforcement*, giacché è questo il campo su cui si gioca la partita del nuovo ordine che l'Europa ambisce a fornire alla società digitale.

In merito, il quadro legislativo appare però disomogeneo e frammentato.

Al principio di *accountability*, la legislazione europea in materia di dati personali attribuisce un ruolo centrale³². Tale principio – insieme alla tutela *by design* di diritti ed interessi e all'onere di dimostrare la *compliance* gravante sull'impresa, che di esso costituiscono diretti corollari – esprime la consapevolezza che la *governance* delle tecnologie non può essere affidata interamente a rimedi ex post, quali il risarcimento (cfr. *infra*). Esso, tuttavia, attualmente vige, come detto, oltre che nel contesto della *data protection*, solamente nel campo dei servizi digitali rientranti nell'ambito di applicazione del DSA, dove serve ad assicurare la sostenibilità delle tecnologie digitali, ed è altresì contemplato dalla Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzare sull'Intelligenza Artificiale (legge sull'Intelligenza Artificiale, d'ora in poi 'AI Act'), ma limitatamente ai sistemi di IA ad alto rischio, secondo la definizione ivi recata.

La pertinente letteratura giuridica suggerisce di estendere il principio in questione al di fuori del limitato campo di applicazione delle discipline normative in cui è espressamente codificato. L'adozione di quella particolare prospettiva di tutela preventiva costituita dal c.d. *by design* e in particolare della *human rights by design* può considerarsi un corollario della già richiamata *corporate social responsibility*. Il principio di *accountability* si va facendo strada anche nella disciplina dei rapporti tra professionisti e consumatori, nello specifico, nella regolamentazione delle pratiche commerciali sleali ed alla luce della diligenza professionale cui i professionisti debbono attenersi³³.

In ordine ai rimedi, si registra una coesistenza di diversi registri concettuali e, per conseguenza, di ordini disomogenei di tutele.

Da un lato, un ruolo centrale è affidato dal legislatore europeo al c.d. *public enforcement*, la cui efficacia deterrente è stata rafforzata (così è in caso di violazione delle discipline in materia di pratiche commerciali scorrette, secondo la direttiva UE 2161/2019 del Parlamento europeo e del Consiglio ('direttiva

omnibus'), ma anche di non osservanza delle prescrizioni contenute nel DSA e DMA)³⁴. Un ruolo complementare è, altresì, riservato al c.d. *private enforcement*.

Troviamo così nel DSA disposizioni relative all'accesso alle tutele di natura privatistica offerte dal diritto nazionale e UE (più esattamente, al risarcimento del danno; cfr. art. 54). In ragione del carattere contrattuale della trama di relazioni stabilite dalle imprese protagoniste della c.d. economia delle piattaforme³⁵, le salvaguardie previste dal diritto dei contratti possono contribuire ad ovviare, sia allo squilibrio di potere contrattuale connotante i rapporti tra prestatori del servizio di intermediazione e destinatari dello stesso, sia ai limiti di consapevolezza e liceità del consenso prestato dall'interessato in merito al trattamento dei propri dati personali³⁶.

Si discute, tuttavia, se i rimedi di carattere privatistico esistenti possano considerarsi appropriati, nella misura in cui si tratta di tutele incentrate su posizioni giuridiche individuali, quali i diritti della personalità, sulle tradizionali figure dei vizi del consenso e sul concetto di danno³⁷. In merito a quest'ultimo, troviamo infatti pregiudizi la cui incidenza su soggetti determinati non può essere accertata (ad es., su un membro del pubblico sottoposto a pratiche di sorveglianza di massa o su un appartenente ad una categoria discriminata) o che non si verificano in una singola unità di tempo, ma si sedimentano nel tempo (ad es., i rischi per i minori legati a sistemi di IA che sfruttino la vulnerabilità di specifici gruppi³⁸).

Il DSA ha poi introdotto il concetto di rischio sistemico, il quale esprime la minaccia di effetti svantaggiosi per l'economia e società, rischio che può essere fatto valere nell'ambito delle tutele collettive inibitorie secondo la direttiva (UE) 2020/1828 del Parlamento e del Consiglio del 25 novembre 2020 relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori (ivi inclusi gli interessi 'generali', secondo la definizione di cui all'art. 3 (3) in essa rinvenibile)³⁹.

4. l'IA per la sostenibilità e la sostenibilità dell'IA

La crescita rapidissima delle tecnologie ed applicazioni di Intelligenza Artificiale e Machine learning (d'ora in poi, unitariamente, 'IA'), resa possibile da quantità sempre crescenti di dati e dall'accresciuta potenza di calcolo dei dispositivi informatici, ha dato origine ad una nuova disciplina, l'etica dell'IA, consistente nello studio delle questioni etiche e sociali che devono affrontare sviluppatori, produttori, consumatori, cittadini, politici e organizzazioni della società civile. Questo campo di studi, dopo essersi nel tempo concentrato su ciò che l'IA è in grado di fare e sui rischi connessi alle tecniche di apprendimento automatico (la lesione della privacy, l'opacità dell'algoritmo *black box*, gli esiti discriminatori delle decisioni algoritmiche dovute a distorsioni nei dati di addestramento e nei modelli di apprendimento, etc.), intende mettere al centro lo sviluppo sostenibile, al fine di dirigere l'uso dell'IA verso usi 'buoni'⁴⁰, con attenzione all'intero ciclo di vita dell'IA (progettazione, formazione, sviluppo e uso). Una definizione di sostenibilità riferita all'IA ci è resa disponibile dall'Organismo USA di standardizzazione, il quale mira a promuovere uno sviluppo ed uso responsabile dell'IA, declinabile in una triplice direzione, di "human centricity, social responsibility, and sustainability". La sostenibilità dell'IA, secondo uno specifico standard ivi inserito, consiste in uno "state of the global system, including environmental, social, and economic aspects, in which the needs of the present are met without compromising the ability of future generations to meet their own needs"⁴¹.

In questo campo è emersa una distinzione cruciale, quella tra una prospettiva che considera l'IA per la sostenibilità, rappresentata da movimenti quali quello appena ricordato, ed un'altra che, invece, prende in esame la sostenibilità dell'IA⁴², del *design*, sviluppo ed impiego dell'IA e delle relative applicazioni, con particolare attenzione ai costi per la società e l'economia, oltre che sotto il profilo della protezione degli individui

e delle delicate questioni etiche che l'AI solleva⁴³. Una nuova frontiera ancora inesplorata, soprattutto dal punto di vista giuridico, è poi anche quella della sostenibilità dell'Intelligenza artificiale rispetto all'ambiente.

Valga in merito un esempio che si trae dagli studi in tema di *AI Ethics* e sostenibilità. Si osserva che l'IA può essere utile nella individuazione e nel superamento delle cause delle disegualianze, ma che essa può altresì creare nuove forme di discriminazione⁴⁴: come avviene nel caso del *targeting* automatizzato della pubblicità di offerte di lavoro, che riproduca pregiudizi di sorta propri di coloro che hanno provveduto alla preparazione dei dati ed al design dei sistemi utilizzati per i processi di selezione. Il contributo del giurista risiede nell'individuare i rimedi giuridici invocabili in un simile caso alla luce del diritto vigente, nonché nel fungere da stimolo per il legislatore affinché, ove necessario, stabilisca regole vincolanti⁴⁵. Si pensi, rispetto al tema del rischio di decisioni discriminatorie, al dovere di controllare la qualità dei dati di cui alla proposta di AI Act.

Con riguardo a queste tecnologie, è dunque necessario assicurare il rispetto dei diritti fondamentali della persona, quali la vita privata e la riservatezza, ma anche la trasparenza e comprensibilità dei processi decisionali, il divieto di discriminazione e, soprattutto, la dignità umana⁴⁶. La protezione dei dati personali non può esaurire l'attenzione del giurista, il quale deve mostrarsi sensibile alla protezione della persona dalle invasioni della sfera privata⁴⁷.

Oltre alla dimensione individuale, viene in rilievo negli strumenti giuridici sovranazionali una nuova dimensione, quella collettiva o sociale.

Così è già nel *Libro bianco sull'intelligenza artificiale della Commissione Europea - Un approccio europeo all'eccellenza e alla fiducia* del 2020, il quale, a ben vedere, ripropone per l'IA i requisiti individuati negli orientamenti del Gruppo indipendente di Esper-

ti di alto livello sull'Intelligenza Artificiale (in particolare, nel documento Orientamenti etici per un'Intelligenza Artificiale affidabile del Gruppo del 2019): intervento e sorveglianza umana, robustezza e sicurezza, riservatezza e *governance* dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale ed ambientale e *accountability*.

Tra gli istituti giuridici contemplati dalla proposta di AI Act, compaiono, accanto a strumenti già sperimentati, come la standardizzazione e le norme tecniche, anche elementi di maggiore novità, quali l'obbligo di verificare che l'IA presenti i requisiti appena ricordati, ivi inclusa la robustezza della tecnologia, da intendere non solo dal punto di vista tecnico ma anche da quello sociale, giacché, al di là dell'indubbio accento posto sulla responsabilizzazione degli attori economici in vista della prevenzione dei rischi, si dovranno valutare le conseguenze che certe tecnologie di AI ed i loro impieghi potranno avere anche sulla collettività. Lo stesso è a dirsi della importante novità che si vorrebbe introdurre con tale proposta, costituita dalla valutazione dei rischi. Incertezze si registrano, però, in ordine all'oggetto e funzione di una simile valutazione (troppo angusto sarebbe il relativo ambito se si limitasse una simile valutazione venisse circoscritta ai soli rischi di lesione delle situazioni giuridiche individuali, escludendo i rischi c.d. sistemici).

Il volume prende spunto dalla conferenza sul tema della *Sostenibilità dell'innovazione digitale*, tenutasi l'8 giugno 2021 presso l'Università degli studi di Napoli L'Orientale, nell'ambito delle attività del Modulo Jean Monnet "Digital Citizenship in the European Union". Raccoglie contributi elaborati a partire dalle relazioni a tale conferenza, nonché scritti di altri studiosi, che integrano e arricchiscono gli spunti offerti dai relatori.

Note di chiusura

¹ In ordine alla rilevanza giuridica della categoria della sostenibilità secondo il diritto dei contratti, cfr. C. PONCIBÒ, *The contract governance of sustainable development*, in *Isaidat Law Review*, 2022/1, pp. 35 ss. Le origini del significato giuridico di sviluppo sostenibile sono tracciate da D. IMBRUGLIA, *Mercato unico sostenibile e diritto europeo dei consumatori*, in *Persona e mercato*, 2021/3, pp. 49 ss., cui si rinvia per riferimenti bibliografici. Si veda inoltre S. LANDINI, *Sostenibilità e diritto dei privati. Il caso dei contratti sostenibili nel settore del turismo*, in questo volume.

² Cfr. G. PERLINGIERI, «Sostenibilità», *ordinamento giuridico e «retorica dei diritti»*. A margine di un recente libro, in *Foro nap.*, 2020, p. 101 ss. Per ampi riferimenti nella letteratura, non solamente giuridica, si veda J. MENSAH, *Sustainable development: Meaning, history, principles, pillars, and implications for human action: Literature review*, in *Cogent Social Sciences*, 5/2019, p. 1 ss., <https://doi.org/10.1080/23311886.2019.1653531>.

³ L. FLORIDI, *Il verde e il blu*, Milano, 2020. Secondo l'a., "le nuove sfide del digitale si presentano, nei prossimi decenni, come legate soprattutto alla *governance* del digitale" (ivi, p. 256). Cfr. altresì K. PISTOR, *Il codice del capitale. Come il diritto crea ricchezza e disuguaglianza*, trad. it. Roma 2021, passim.

⁴ N. IRTI, *Meditazione del giurista su pagine dell'ultimo Croce*, in *Venti anni a Palazzo Filomarino*. Per Natalino Irti, Istituto Italiano per gli Studi Storici, Napoli, 2023, p. 73 ss.

⁵ E. CATERINI, *Artificial intelligence, persona e soggetto*, in questo volume.

⁶ M. BIANCA, *La filter bubble e il problema dell'identità digitale*, in *MediaLaws*, 2/2019, p. 39 ss.

⁷ G. COMANDÈ, *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in *An. Giur. Econ.* 1, 2019, p. 169 ss. Cfr. F. MEZZANOTTE, *Rischio e responsabilità nei sistemi dell'Internet of Things*, in questo volume.

⁸ Cfr. la Comunicazione della Commissione Europea "Una strategia per le PMI per un'Europa sostenibile e digitale" (10.3.2020 COM(2020) 103 final).

⁹ M. EBERS, *Liability for Artificial Intelligence and EU Consumer Law*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2021/12, p. 204 ss., p. 207

¹⁰ V. RICCIUTO, *L'equivoco della privacy. Persona vs dato personale*, Napoli, 2022.

¹¹ Si veda S. WACHTER, B. MITTELSTADT, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, in *Columbia Business Law Review*, 2019, no. 2, pp. 494-620, p. 614.

¹² M. Z. VAN DRUNEN, N. HELBERGER, R. Ó FATHAIGH, *The beginning of EU political advertising law: unifying democratic visions through the internal market*, in *International Journal of Law and Information Technology*, 2022, 30, 181–199.

¹³ M. R. FERRARESE, *Poteri nuovi. Privati, penetranti, opachi*, Bologna 2022. Cfr. altresì O. POLLICINO, G. DE GREGORIO, *Constitutional Democracy in the Age of Algorithms: The Implications of Digital Private Powers on the Rule of Law in Times of Pandemics*, in *MediaLaws*, 11 novembre 2020.

¹⁴ S. ORLANDO, *Per un sindacato di liceità del consenso privacy*, in *Persona e mercato*, 4/2022, p. 527 ss.; S. WACHTER, B. MITTELSTADT, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, in *Columbia Business Law Review*, cit., p. 613.

¹⁵ Cfr. la Comunicazione della Commissione Europea “Una strategia per le PMI per un’Europa sostenibile e digitale”, già menzionata.

¹⁶ Cfr. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>.

¹⁷ Cfr. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en

¹⁸ C. CAUFFMANN, C. GOANTA, *A New Order: The Digital Services Act and Consumer Protection*, in *European Journal of Risk Regulation*, (2021) 12:4, p. 758 ss., p. 770; Z. EFRONI, *The Digital Services Act: risk-based regulation of online platforms*, in *Internet Policy Review*, 2021, <https://policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606>; Gambino.

¹⁹ E. AL MUREDEN, *Tutela della persona e limitazione dell’errore umano tra Advanced Driver Assistance Systems e guida automatizzata di livello 3*, in questo volume, nonché M. CARLIZZI, *Sostenibilità e innovazione nell’attività bancaria: il conto base come soluzione per chi abbia ridotte capacità cognitive*, ibidem. Tali autori prendono in esame la digitalizzazione, e la relativa disciplina, come strumento per promuovere, rispettivamente, la sicurezza stradale e l’inclusione finanziaria di categorie vulnerabili.

²⁰ Toccato da A. ASTONE, *Consenso ed intelligenza artificiale: limiti e prospettive*, in questo volume, e da G. BERTI DE MARINIS, *L’Algo-governance nelle imprese di assicurazione e l’integrazione dei fattori ESG*, ibidem.

²¹ Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Una strategia europea per i dati (COM/2020/66 final).

²² Cfr., per un esame critico, lo studio dell’EPRS - EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Governing data and artificial intelligence for all. Models for sustainable and just data governance*, PE 729.533 – July 2022, p. 3 e 63.

²³ United Nations Office of the Secretary-General's Envoy on Technology, 'Digital Cooperation: 'Digital Public Goods' Implementation Plan (SEP. 2020 – DEC. 2022, TOWARDS 2030),' April 15, 2021, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/general/210415_Digital_Public_Goods_roundtable_w_orkplan.pdf.

²⁴ N. STREINZ, *The evolution of European Data Law*, in *The Evolution of EU Law*, a cura di P. Craig, G. de Búrca, Oxford University Press, 3^e ed., 2021, pp. 902 ss.

²⁵ Secondo il già citato studio dell'EPRS - EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Governing data and artificial intelligence for all. Models for sustainable and just data governance*, cit., p. 63, nella European Data Strategy "there is little emphasis placed on aspects of embedding sustainable practices within the creation of new bodies of data intermediation and altruism. Focusing on sustainability will involve setting standards and limits for the environmental impacts of computing systems and putting in place policy instruments and institutional architectures that enable different interests to be prioritised within these limits".

²⁶ M. FASCIGLIONE, *I diritti umani nell'era degli algoritmi e dell'intelligenza artificiale*, in questo volume. Cfr. altresì A. MANTELERO, *An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems*, in *Computer Law and Security Review*, 41 (2021), p. 1 ss.

²⁷ Cfr. I. GARACI, *La valutazione d'impatto sui diritti fondamentali dei minori di età nell'ambiente digitale. Riflessioni a margine della proposta di direttiva relativa alla due diligence delle imprese ai fini della sostenibilità*, in questo volume.

²⁸ C. N. GRIFFIN, *Systemically Important Platforms*, in 107 *Cornell Law Review* (forthcoming 2021), disponibile in C. N. GRIFFIN, *Systemically Important Platforms*; S. J. LINDSAY, T. R. SAMPLES, *On the Systemic Importance of Digital Platforms*, in *University of Pennsylvania Journal of Business Law*, vol. 25 (forthcoming 2022), p. 5 e 6, sul concetto di rischio sistemico, disponibile in <https://ssrn.com/abstract=4040269>. In ordine al DSA, cfr. Z. EFRONI, *The Digital Services Act: risk-bases regulation of online platforms*, in *Internet Policy Review*, 16 novembre 2021, in <https://policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606>

²⁹ S. WACHTER, B. MITTELSTADT, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, in *Columbia Business Law Review*, cit., p. 613.

³⁰ Cfr. I. BURI, J. VAN HOBOKEN, *The Digital Services Act (DSA) Proposal: a critical overview*, in DSA Observatory, disponibile in https://dsa-observatory.eu/wp-content/uploads/2021/11/Buri-Van-Hoboken-DSA-discussion-paper-Version-28_10_21.pdf.

³¹ I. GARACI, *La valutazione d'impatto sui diritti fondamentali dei minori di età nell'ambiente digitale*, cit.

³² R. CARLEO, *Il principio di accountability nel GDPR: dalla regola alla auto-regolazione*, in *NDC*, 2021, p.

³³ Si vedano le linee guida relative nella EU Commission's Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, 5.2.2., 114., ora confluite nel Considerando 74 del DSA.

³⁴ Si veda lo Studio di BEUC (The European Consumer Organisation), EU Consumer protection 2.0. Protecting fairness and consumer choice in a digital economy, BEUC-X-2022-015 – 10/02/2022, <https://www.beuc.eu/position-papers/eu-consumer-protection-20-protecting-fairness-and-consumer-choice-digital-economy>.

³⁵ T. RODRIGUEZ DE LAS HERAS BALLELL, *The Legal Anatomy of Electronic Platforms: A Prior Study to Assess the Need of a Law of Platforms in the EU*, in *Italian Law Journal*, (2020) Vol. 03 – No. 01, pp. 149 ss. Si veda R. PETRUSIO- G. SMORTO, *Trasformazione della filiera distributiva e responsabilità delle piattaforme del commercio elettronico nella proposta di direttiva "sulla responsabilità per danno da prodotti difettosi"*, in questo volume.

³⁶ V. RICCIUTO, *L'equivoco della privacy. Persona vs dato personale*, cit.; S. ORLANDO, *Per un sindacato di liceità del consenso privacy*, cit.

³⁷ B. VAN DER SLOOT, *Privacy as virtue. Moving Beyond the Individual in the Age of Big Data*, Intersentia. Per un'analisi del tema, cfr. M. FEDERICO, *Rappresentanza degli interessati, diritti individuali e group data protection*, in *Persona e mercato*, 4/2022, p. 674 ss.

³⁸ M. VEALE, F. ZUIDERVEEN BORGESIOUS, *Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach*, in *Computer Law Review International*, 4/2021, p. 97 ss., p. 99, <https://doi.org/10.9785/cr-2021-220402>.

³⁹ Direttiva (UE) 2020/1828 del Parlamento e del Consiglio del 25 novembre 2020 relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE (L 409/1).

⁴⁰ L. FLORIDI AT AL., *AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in *Minds and Machines*, 2018, p. 689 ss.

⁴¹ Cfr. US National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, Gennaio 2020e, p. 2, <https://doi.org/10.6028/NIST.AI.100-1>, recante tale definizione nello standard ISO/IEC TR 24368:2022.

La sostenibilità dell'innovazione digitale. Un'introduzione

⁴² A. VAN WYNSBERGHE, *Sustainable AI: AI for sustainability and the sustainability of AI*, in *AI and Ethics* <https://doi.org/10.1007/s43681-021-00043-6>

⁴³ Cfr. G. BERTI DE MARINIS, *L'Algo-governance nelle imprese di assicurazione e l'integrazione dei fattori ESG*, in questo volume, in merito all'impiego dell'IA per elaborare dati a supporto dell'adozione, da parte delle imprese, di decisioni sostenibili, per valutare i rischi ESG e per migliorare la propria performance sul punto.

⁴⁴ Cfr. E. BATTELLI, *Gli smart-contract nel mercato delle assicurazioni: limiti e opportunità*, in questo volume.

⁴⁵ L. FLORIDI, *The End of an Era: from Self-Regulation to Hard Law for the Digital Industry*, in *Philosophy and Technology*, 2021, 34(4), p. 619 ss., in <https://doi.org/10.1007/s13347-021-00493-0>.

⁴⁶ N. HELBERGER - O. LYNSKEY - H-W. MICKLITZ - P. ROTT -M. SAX - J. STRYCHARZ, *EU Consumer Protection 2.0, Structural asymmetries in digital consumer markets. A joint report from research conducted under the EUCP2.0 project*, 2021, p. 14 ss.

⁴⁷ A. CORRENTI, *Piattaforme tecnologiche: protezione ed educazione dell'utente all'utilizzo delle infrastrutture informatiche nei mercati a concorrenza imperfetta*, in questo volume, nonché, sul rapporto tra GDPR e intelligenza artificiale, A. ASTONE, *Consenso ed intelligenza artificiale: limiti e prospettive*, ivi.

Artificial intelligence, persona e soggetto

ENRICO CATERINI

Sommario: 1. Soggettività e *AI*. - 2. Soggetto e interesse. - 3. Persona e soggetto. - 4. L'uomo-macchinico e l'attante. - 5. *AI* e coscienza etico-giuridica. - 6. (segue) e coscienza neurofisiologica. - 7. Valori sociali e dignità umana. - 8. Soggettività e responsabilità. - 9. L'agire autonomo dell'attante. - 10. *AI*, responsabilità e distribuzione del rischio.

1. Soggettività e *AI*

Il tema della soggettività va riletto nella dimensione aperta dall'intelligenza artificiale. Questa ha la peculiarità di presentarsi come un'intelligenza «derivata» da quella umana¹ e di alimentare una soggettività² distinta da tutte le altre con caratteri simili alla persona umana³. Condivide con questa la proprietà dell'ideazione, cioè la forza di produrre idee utilizzando processi emulativi dell'intelligenza umana⁴.

Ma l'essere «derivata» non indica un'aire senza ritorno. Al di là dell'impropria assimilazione dovuta dall'uso comune del termine intelligenza, la questione che appare più interessante è se l'intelligenza artificiale sia destinata a modificare quella biologica e a generare un flusso di nuove energie e informazioni le quali alimentano un volano virtuoso che contribuisce a conformare «nuovi» processi intelligenti⁵. Ciò aiuta a persuadere che la c.d. intelligenza artificiale possa essere essa stessa una delle nuove insorgenze di soggettività giuridiche⁶, intese secondo l'accezione che si proverà a spiegare oltre⁷.

2. Soggetto e interesse

La ricerca giuridica sulla soggettività da tempo s'interroga sul superamento del c.d. antropocentrismo⁸, cioè della concezione che

ha posto l'azione del soggetto (ossia la sua volontà) quale condizione dell'individuazione dell'attore del diritto, indicando una soluzione segnata a favore esclusivo dell'uomo quale unico e solo effettivo destinatario delle utilità del diritto⁹. Tale concezione è da tempo contestata¹⁰. Tra le radici critiche quella che si ritiene di preferire è rinvenuta nella valorizzazione dell'*interesse*¹¹, in luogo dell'azione del soggetto. Nell'interesse si secerne la ragione della protezione che l'ordinamento seleziona al fine di destinare un beneficio ad alcuno e un sacrificio ad altri, interesse che diviene esso stesso il generatore della soggettività giuridica¹².

Questa rilettura dell'ordinamento ha posto a fondamento di ogni fenomeno giuridico, quindi anche della soggettività, l'interesse quale causa dell'intervento del diritto. In tale evenienza il diritto non richiede per il suo intervento un soggetto *agente* ma uno «depositario» dell'interesse, là dove l'azione sarà una conseguenza affidata a chi, munito di capacità, avrà i requisiti per agire¹³. A questo punto di elaborazione del pensiero non è più utile discorrere di semi-soggettività perché l'«ente» soggetto, per esser tale, non richiede un attore capace di «disporre» ma soltanto di «godere» della situazione giuridica¹⁴. Dunque, in tali casi la nuova soggettività non è parziale o dimidiata, essa è piena sebbene richieda un «rappresentante» capace di esercitarla.

L'imprevedibile dispiegarsi della «giurisprudenza degli interessi»¹⁵, ormai consolidata nella letteratura giuridica, s'è rivelato nel facilitare il moltiplicarsi delle soggettività per quanti centri di interessi l'ordinamento ha dotato di autonomia e indicato come meritevoli di protezione. Pertanto, sono o possono assurgere a tale dignità le comunità, gli embrioni¹⁶, la biologia sintetica¹⁷, l'intelligenza artificiale, la dignità *postmortem* dell'uomo¹⁸, le *class action*¹⁹, gli animali²⁰, l'ambiente²¹, i fiumi²², i ghiacciai²³ e via discorrendo²⁴.

Tali considerazioni inducono a rivalutare l'astrattismo concettuale della soggettivazione anche quando posto in relazione

con il valore della persona che la carta fondamentale ha anteposto allo stesso soggetto.

3. Persona e soggetto

Ciò che può apparire come conflittuale subisce una metamorfosi culturale che ne rende compatibile la coesistenza, ma ad alcune condizioni. Se da un lato si può affermare che ogni persona è soggetto, dall'altro non potrà dirsi che ogni soggetto è persona. Perciò, occorre sottolineare che i fondamenti del soggetto e della persona non sono i medesimi. Non è sufficiente spostare il baricentro dell'ordinamento dall'uomo al globo per consentire all'interesse, come fondamento del diritto, di dispiegare ogni sua potenzialità, anche ai danni della stessa persona. A nulla valgono le mirabili intenzioni di chi, contristato da un'azione umana distruttiva e dominante l'ambiente, trovi conforto in un pericoloso capovolgimento delle misure il cui rischio può rivelarsi opposto a quello già corso, ossia la *relativizzazione* del valore della persona. Questo è il pericolo che si corre se si transita dall'antropocentrismo all'e-co-centrismo una volta posto a base della soggettivazione l'auto-nomo interesse meritevole di apprezzamento dall'ordinamento. Qui la questione è di rilievo costituzionale se si riflette sul ruolo che la legalità costituzionale assegna alla persona. È pur vero che tale ruolo coinvolge l'umanità intesa anche come intreccio di relazioni sociali, e che essa è preservata da un rapporto equilibrato e non predatorio con il mondo senziente e inanimato, ragioni queste dello sviluppo sostenibile; ciò nondimeno, la persona non richiede un processo di soggettivazione al pari degli altri soggetti.

La persona è soggetto in quanto valore, giammai perché interesse. Dinnanzi alla persona umana l'ordinamento arresta ogni valutazione teleologica per riconoscerne il valore in sé. Ciò non esclude che anche la persona, proprio nelle sue espressioni di maggiore fragilità, possa ricorrere al «rappresentante agente», quando ella

non può che essere destinataria ma non esercente il valore o l'interesse agito. Ecco la ragione per la quale la persona-soggetto fonda sul valore, là dove il soggetto-non persona sull'interesse.

L'ordinamento può apprezzare nuovi interessi tanto da soggettivarli ma senza che ciò possa rivelarsi di nocumento al valore della persona, anzi più propriamente, tali interessi devono accrescerne la misura della tutela²⁵.

L'astrazione concettuale del soggetto, dunque, è teoria meritoria che dà emersione a quelle nuove soggettività dell'ordinamento, ma essa non include la persona la quale ha una fonte legittimante distinta dal soggetto.

4. L'uomo-macchinico e l'attante

In questo senso occorre distinguere la persona, e le sue propaggini, dagli altri soggetti. Pertanto, un conto è discutere di embrione o di intelligenza artificiale quali «complementi» umani, altra cosa è discutere di «attanti» artificiali quali nodi autonomi delle decisioni macchiniche²⁶. Nei primi l'*item* è la persona, nei secondi il soggetto²⁷.

In questi ultimi a nulla rileva, ai fini della soggettivazione, la circostanza che essi sono capaci di decidere autonomamente, quindi, capaci di disporre oltre che di godere dell'interesse di cui sono titolari. Come anzi detto, non è più l'azione che fa il soggetto, ma l'interesse, mentre la persona è valore.

Tuttavia, l'autoapprendimento di una specie di A.I.²⁸ consente il compimento di azioni che trovano propulsione nell'algoritmo il quale consente all'attante di esprimere una volontà protesa al perseguimento di un interesse²⁹. È ignota la consapevolezza, o discernimento, di detta volontà agente, ma è noto che essa si auto-consolida e si adegua a mezzo della sua stessa esperienza, sottraendosi alla prevedibilità dello stesso programmatore³⁰. È condivisibile la convinzione che non occorra sempre una nuova

soggettività per renderla imputabile della responsabilità connessa alle sue azioni³¹, ma deve pur ammettersi che un soggetto autonomo-decidente possa essere portatore di interessi alieni³² rispetto a quelli di chi lo ha concepito³³. È quest'ultima la ragione per la quale generalizzare la soluzione interpretativa che trovi fondamento nell'applicazione della responsabilità da cosa in custodia, da attività pericolosa, da prodotto difettoso, ovvero, da animali, sia soluzione persuasiva finché si presupponga l'esistenza di un nesso inscindibile tra l'interesse dell'attante e quello dell'attore³⁴.

5. AI e coscienza etico-giuridica

A questo punto è utile proporre qualche riflessione sull'elemento discriminante l'intelligenza umana dall'artificiale. È la coscienza che distingue³⁵. La coscienza persegue il senso della giustizia attraverso l'intelligenza -che la definisce-, e la volontà, che la attua. Un esempio tratto da un caso accaduto negli Stati Uniti può chiarire l'idea. Il *software* rileva anche il lieve eccesso di velocità al passare dell'auto. Il giudice esonera da responsabilità l'autista ultranovantenne, ammalato di tumore, che alla guida dell'auto accompagnava in ospedale il figlio ultrasessantenne per una importante terapia. Quale intelligenza artificiale avrebbe saputo giudicare il valore dell'azione di quell'uomo? Soltanto il senso concreto ed il valore etico della giustizia ha saputo raggiungere tale conclusione³⁶. Il senso di giustizia della coscienza umana ridimensiona alcuni brocardi come il *dura lex sed lex*³⁷. L'esempio spiega la differenza tra la conoscenza e la coscienza³⁸. Questa differenza accentua l'altra -nota- tra l'imputazione e la colpevolezza³⁹. Si può tenere un comportamento difforme da condotte standard senza consapevolezza, cioè senza comprendere il disvalore delle proprie azioni, pur essendo capaci di auto-determinarsi. E al contrario, si può violare la condotta standard nella consapevolezza che tale condotta non esprima nel concre-

to un disvalore sociale. L'intelligenza artificiale interagisce con l'apparato della conoscenza⁴⁰ ma senza coscienza⁴¹.

Essa ha il limite di essere priva del giudizio⁴² che, invece, è proprio dell'intelligenza umana. Essa non può possedere alcune di quelle che si dicono virtù cardinali⁴³. È impensabile definire l'intelligenza artificiale come saggia o giusta. La saggezza, intesa come qualità umana capace di ponderare e penetrare le cose e gli uomini, non è programmabile; la giustizia, intesa come qualità dell'uomo capace di contemperare l'interesse proprio con quello degli altri, tanto da esprimersi in un'esistenza equa e corretta, non è programmabile. L'intelligenza artificiale esprime la corrispondenza all'uomo istruito non a quello educato o colto⁴⁴.

6. (segue) e coscienza neurofisiologica

La coscienza non ha soltanto una dimensione etico-giuridica, ma anche una neurofisiologica. In questa dimensione, che indaga la modalità di funzionamento dell'organo cerebrale, s'è giunti a formulare un'ipotesi, dipoi suffragata da elementi esperienziali, secondo la quale per coscienza deve intendersi quella proprietà cerebrale che esprime, insieme, l'attitudine alla differenziazione e all'integrazione.

Queste due funzioni cerebrali, che si possono indicare altrimenti come la specializzazione e la complementarità, implicano la comprovata unitarietà del funzionamento cerebrale⁴⁵. Questo è un tutt'uno e allo stesso tempo un *unicum*. Non è raffigurabile nella fisiologia umana una funzionalità cerebrale che contempi una soltanto delle due funzioni anzi dette. Queste, a sé prese, tenderebbero a divaricarsi poiché la specializzazione soffre la complementarità, come anche il contrario. Lì dove v'è specializzazione v'è un flusso informativo settoriale altamente selettivo che esclude ogni informazione altra, estranea al settore. Mentre, lì dove v'è integrazione, il flusso informativo tende

ad espandersi in ogni settore e riduce al minimo ogni fattore selettivo. Le due proprietà cerebrali sono costantemente alla ricerca di una sintesi che costituisca il punto di equilibrio, temporaneo e dinamico, tra la differenziazione e l'integrazione. Quel punto di equilibrio è quanto realizza la coscienza nella sua fisiologica funzionalità umana. Qualora l'organo cerebrale perda il punto di equilibrio e si sbilanci verso una delle due proprietà, colloca il baricentro fuori dal cerchio della consapevolezza e genera azioni umane «in-coscienti».

La proposta di coscienza elaborata da studiosi della neurofisiologia ha in sé l'intuizione culturale di presupporre una coscienza dinamica in ogni persona e diversificata tra ogni persona. Pertanto, non esiste un singolo stato di coscienza della persona come non esiste un unico stato di coscienza per tutte le persone. La valenza *soggettiva* della coscienza è indeclinabile⁴⁶. Ciascuno ha il suo stato di coscienza ed esso sarà determinato anche dalle condizioni di contesto culturali di ogni persona. Si vuole dire che lo stato di coscienza personale dipende dalle condizioni del flusso informativo che caratterizzerà quella persona, diversamente dalle altre, ma che quel flusso informativo sarà tanto auto che etero poetico. Lo specialismo differenziante ogni essere umano è culturale e fisiologico insieme, e non desta meraviglia se lo stato di coscienza della persona muta nel tempo e nello spazio, come muta in parallelo la stessa capacità di giudizio della persona⁴⁷. In tutto questo le funzioni e le proprietà cerebrali non mutano. Esse riducono a sintesi e completano i flussi informativi di cui dispongono, di per sé mutevoli e mutageni. È una sorta di «fotosintesi» cerebrale, ove le energie dei flussi informativi ad opera delle cellule neurologiche sono trasformate in energie cogni-volitive, ossia in stato di coscienza. Questa constatazione empirica, ricavata dall'esperienza neurofisiologica, consente di osservare che tali proprietà cerebrali non possono che essere dell'intelligenza umana poiché i

flussi informativi dell'intelligenza artificiale lavorano come le *addizioni* algebriche, là dove quelli dell'intelligenza umana come le *moltiplicazioni*. La proprietà che integra le differenziazioni, si-
nora, è riconoscibile nell'intelligenza umana.

7. Valori sociali e dignità umana

L'osservazione appena svolta manifesta una qualità che si estende dallo «stato di coscienza» della persona alla relazione tra quest'ultima e i suoi simili. La stessa società, in fondo, è la sintesi integrata di molte differenze; non v'è società senza la relazione tra diversi. Così come l'eguaglianza è un processo di sintesi che persegue un punto di equilibrio tra le differenze e la complementarità integrativa. I processi complessi hanno molte similitudini. Ma ciò che connota tutti allo stesso modo è l'estrema «volubilità» culturale; lo stato di coscienza, come le società, mutano al mutare del punto di equilibrio tra le differenze dei flussi informativi e l'integrazione di essi.

Il fattore «cultura» è il fattore mutageno principale, ed è quel fattore che anche in presenza di flussi informativi astrattamente identici può generare stati soggettivi di coscienza differenti. Lo stesso tema dei diritti umani assume connotazioni differenti in considerazione degli stati di coscienza che gli uomini di differenti estrazioni culturali presentano⁴⁸. Per quanto tali diritti siano il prodotto della cultura occidentale, non sono estranei ad altre culture le quali ne declinano i significati in modi non sovrapponibili. Dunque, ciò che in un luogo esprime uno stato di coscienza condiviso, può non esserlo altrove. Ciò comprova che lo stesso senso di giustizia⁴⁹ muta in base al mutare dello stato di coscienza. Si può affermare che muta il processo di integrazione dei flussi informativi e si perseguono punti di equilibrio differenti.

In prima conclusione si può dire che anche l'empirico processo neurofisiologico volge a rappresentare la capacità umana

di esprimere il giusto, come equilibrio tra fattori divergenti, secondo condizioni soggettivamente variabili, ed in quanto tali infinite. Il concetto di «valore», come categoria giuridica insita in alcuni principi fondamentali, costituisce l'argine all'infinita variabilità soggettiva, e consente un numero finito di variabili⁵⁰.

Dunque, se la ricerca del giusto nella dimensione sociale traccia l'essenza dell'equilibrio dettato dai «valori», lo stato di coscienza soggettivo delinea ciò che diversamente può essere definita dignità dell'uomo. In fondo, il concetto di dignità è la risultante di un processo che riduce a sintesi i flussi informativi auto e etero poetici. Nella ricerca della sintesi v'è la ricerca di un equilibrio personale tra differenze e generalità, tra caratteri propri e comuni, per cui anche il valore della persona non è monolitico e identico, bensì un «prodotto» culturale. Ciò sta a significare che la dignità non è uno stato in essere dell'uomo, come non è una conquista generata dalle prestazioni dell'uomo, essa non è neppure una comunicazione-riconoscimento sociale. La dignità è un processo che si nutre dei flussi informativi interni ed esterni all'uomo. È un divenire mutevole che integra in un agire circolare fattori endogeni ed esogeni i quali, culturalmente elaborati, generano uno stato di coscienza. Anche la dignità umana subisce le conterminazioni dei valori espressi dall'ordinamento giuridico⁵¹.

Questi caratteri non sono -allo stato- propri dell'intelligenza artificiale, ecco la ragione che induce a distinguere la persona dal soggetto e ad includere l'intelligenza artificiale dell'attante nel secondo⁵².

8. Soggettività e responsabilità

Il tema del rapporto tra l'intelligenza artificiale e la soggettività assume rilievo soprattutto per le sue evidenti connessioni con l'altro tema della responsabilità. La questione riguarda la con-

cezione di nuove soggettività allo scopo di renderle centri di imputazioni delle connesse responsabilità, ovvero, di estendere la responsabilità alle soggettività che si sono avvalse degli attori o attanti artificiali⁵³.

Le risposte seguono due possibili tracciati, non incompatibili sul piano metodologico: da un lato, si prova ad estendere i concetti e le categorie già noti alla scienza giuridica per includervi i casi di responsabilità conseguenti all'agire degli attori artificiali; dall'altro, si concepiscono nuove soggettività distinte ed auto-responsabili⁵⁴.

La scelta tra le due soluzioni dipende dalla capacità di autodeterminazione che ha l'attante artificiale, al punto che quando esso si sottrae al controllo di chi lo progetta e assume la forza di decisioni autonome, non v'è più spazio per l'estensione di soggettività note all'ordinamento, ed occorre intraguardare nuove soggettività⁵⁵.

Il nesso soggettività-responsabilità corre lungo il filo dell'eguaglianza e della giustizia. In fondo, le soluzioni offerte dagli artt. 1228 e 2049 c.c. per i fatti compiuti con l'opera di terzi o di commessi, rispondono ad un'esigenza di eguaglianza, intesa come ragionevolezza e proporzionalità nella distribuzione delle responsabilità conseguenti ad alcune scelte proprie del debitore principale. Analogo argomentare si svolge lì dove si distingue la responsabilità del procuratore dal quella del rappresentato. In tali sistemi ciò che rileva è la riconducibilità del fatto all'autore, diretta o indiretta⁵⁶.

9. L'agire autonomo dell'attante

La soluzione deve mutare il paradigma qualora tra l'autore-attore e l'attante artificiale vi sia soluzione di continuità, quando cioè, la decisione di quest'ultimo sia indipendente⁵⁷, per cui ricondurre la responsabilità al primo risulterebbe ingiusto oltre che improprio, considerato che gli stessi criteri oggettivi e soggettivi della

responsabilità potrebbero non essere presenti, e questo potrebbe condurre l'effetto di una totale irresponsabilità con conseguente ribaltamento del rischio nella sfera del danneggiato.

Dunque, la presenza di un'intelligenza artificiale che può emancipare le sue decisioni da chi l'ha progettata, apre alla questione di nuove soggettività responsabili⁵⁸. Non è più soltanto una questione di *automazione* della decisione, ma di *autonomizzazione* della stessa. Si assiste vieppiù ad una perdita di controllo della macchina da parte del programmatore, produttore e utilizzatore⁵⁹. L'attante *software* non è più sempre prevedibile nei suoi comportamenti futuri. Il nesso tra soggetto generante e soggetto generato si recide. L'attante-*software* capace di auto-apprendimento non è più equiparabile a quello esecutivo per cui la riconducibilità del primo al soggetto germinale è irragionevole ed ingiusta sul piano del principio di eguaglianza.

D'altra parte, come la riconduzione ad ogni costo dell'attante al soggetto germinale può presentare profili di irresponsabilità del primo qualora non sussistano i criteri oggettivi e soggettivi di responsabilità, anche la germinazione di una nuova soggettività senza l'imputazione di una autonoma responsabilità corre il medesimo rischio⁶⁰. Occorre riconoscere l'emergenza di una soggettività *altra*, distinta dall'uomo e dalla persona giuridica, che raccoglie la capacità –sebbene *parziale e limitata*– del «nodo» decisionale algoritmico⁶¹. A questo si riconosce uno *status* derivante dall'idoneità del «nodo» ad esprimere la capacità di comunicare una determinazione imputabile ad un centro di decisione, al pari di quanto l'ordinamento fa con riguardo alle persone giuridiche⁶².

Tale emancipazione dell'algoritmo dall'uomo consente di concepire categorie giuridiche «originarie» piuttosto che «derivate». Secondo una tesi autorevole⁶³ ciò permetterebbe la simiglianza con la rappresentanza, ove l'agire autonomo del rappresentante ripartisce la responsabilità tra il *dominus* e il *procurator*. Ciò si vorrebbe riprodurre nel rapporto tra l'uomo e l'algoritmo, concepiti

come autonomi centri di decisioni ai quali corrispondono distinte titolarità. E per ciò che attiene ai vizi di esecuzione dei contratti la tesi rinviene nella disciplina dell'ausiliario i termini per un'applicazione analogica anche ai fini della responsabilità.

Per quanto persuasivo il pensiero che vuole distinti i poli di autonomia decisionali in quanto portatori di condotte non riconducibili o derivate le une dalle altre, ed in quanto le condotte non siano includibili in un'azione prevista e programmata da rendere l'«attante» *software* un mero esecutore di un piano umanamente concepito, l'accostamento alla persona giuridica o alle soggettività non personificate presenta alcune criticità. Infatti, se l'«attante» automato sembrerebbe recidere ogni connessione con il soggetto germinale, diversamente, nel soggetto personificato l'attore ricorre alla rappresentanza organica per integrarsi [e identificarsi] con la persona umana la quale continua a nutrire l'agire della nuova soggettività⁶⁴.

D'altro canto, l'apparente recisione tra l'attore e l'«attante» non è tale se si considera che l'agente automato è pur sempre germinato dall'uomo dal quale trae i caratteri ad esso conferiti⁶⁵. Ciò ricorda –per restare nello schema metodologico che estende categorie giuridiche esistenti– l'autonomia che l'ordinamento riconosce al minore, cioè la capacità di discernimento⁶⁶, quella capacità gradualmente sempre più autonoma, *parzialmente* e *dinamicamente* idonea al compimento di atti responsabili e imputabili⁶⁷. Tale accostamento consente di graduare e differenziare la distribuzione del rischio connesso ai fatti di responsabilità tra l'attore e l'attante, senza optare per una soluzione aprioristica e astratta⁶⁸.

La prospettiva è quella di assicurare alla responsabilità l'«attante» che abbia avuto un ruolo nel flusso decisionale⁶⁹. Ogni decisione comporta responsabilità secondo una ragionevole distribuzione del rischio che consideri non soltanto i costi e i benefici economici della scelta, ma il principio personalista della

legalità costituzionale, che non può tollerare una responsabilità senza la riconducibilità del fatto all'autore⁷⁰.

La partecipazione del «nodo algoritmico» al «rimbalzo» (o alla re-azione) che la decisione riceve come apporto autonomo dell'«attante»⁷¹, dev'essere sufficiente all'imputazione della responsabilità proprio quando la decisione algoritmica non è l'esito di un mero errore di calcolo del programmatore ma la risultante di un apporto imprevedibile⁷².

In termini metaforici è necessario distinguere l'apporto alla decisione dell'attore umano (che agisce e genera l'atto), apporto che «attraversa» la coscienza e la libertà dell'essere pensante, dall'altro apporto, quello dell'«attante», il quale consegue al primo come impatto che genera una re-azione, una contro-decisione. Necessita stimare i due apporti e il rischio connesso alla decisione imprevedibile dell'«attante», poiché in questo si annida la contro-decisione non raggiungibile dall'attore umano.

Occorre, dunque, scongiurare l'irresponsabilità da assenza di colpa o da insussistenza dell'attività pericolosa dei protagonisti della decisione, l'attore e l'attante, e valutare la meritevolezza di tutela della posizione del danneggiato, e se il valore in questo tutelato è preminente rispetto a quello dei due decisori, benché soggettivamente distinti.

10. AI, responsabilità e distribuzione del rischio

Pertanto, ferma l'emersione di nuove soggettività come quella algoritmica, la soluzione secondo giustizia della responsabilità generata dall'«attante» non trova una risposta univoca ed aprioristica⁷³ se non dopo la ponderazione degli interessi, dei valori⁷⁴ e dei soggetti concretamente in relazione⁷⁵. Non può sempre ammettersi come meritevole il rischio elevato connesso all'imprevedibilità decisionale dell'«attante»⁷⁶, benché rivolto al superamento di ciò che i matematici chiamano il *massimo locale*, cioè lo stadio di massimo

avanzamento della conoscenza, quando questo rischio pregiudica il *minimo vitale* dell'uomo, cioè l'indispensabile ad una vita dignitosa⁷⁷, ovvero, quando tale rischio può essere socialmente allocato⁷⁸. È pur vero che l'intelligenza artificiale pone dinanzi al rischio dell'avanzamento della conoscenza, ma neppure si può pensare che questo rischio debba essere per intero corso dal danneggiato⁷⁹. Nei casi di minimo vitale la sicurezza sociale può sostituire la responsabilità civile⁸⁰. Si ripropone il fondamento della responsabilità da illecito costituzionalmente costruito sul bilanciamento tra l'agire libero del danneggiante e il limite -condizionante il primoderivante dall'interesse protetto in capo al danneggiato⁸¹.

L'osservazione suesposta non subisce mutazioni significative quando il rischio di responsabilità derivi dall'ibridazione uomo-macchinico⁸². Questa definita «associazione» tra l'uomo e il *software* ha il carattere di integrare l'intelligenza umana a quella artificiale, con l'effetto di generare una nuova soggettività parziale e limitata, *de lege ferenda*, ovvero, di concepire uno «scopo associativo» quale nuovo centro di imputazione delle condotte, *de lege lata*. L'una e l'altra interpretazione pongono l'accento sull'innesto volitivo generato dal «nodo algoritmico» nella condizione umana secondo natura⁸³. L'apprezzamento del pensiero che intravede un nuovo soggetto, ovvero, vede uno scopo associativo, è rinvenibile nella sua massima espressione qualora in tali nuove entità si concepisce una vera mutazione umana, una potenzialità che sviluppi componenti altrimenti inesistenti nell'uomo e che in quanto tale tenda a generare una società di «omoidi»⁸⁴.

Tuttavia, in tali casi si avrà pur sempre a che fare con la persona e non con il soggetto *tout court*. Differente è la considerazione riguardante la responsabilità conseguente alle decisioni assunte da una moltitudine «reticolare» di agenti informatici. Ivi la maggiore difficoltà di imputazione della responsabilità ad una forma di semi-soggettività induce a prospettare l'abbandono della ricerca dell'agente (individuale o collettivo) per concentrare il «polo»

della responsabilità nelle «decisioni rischiose in quanto tali». Detto «polo» deve risultare da una scelta legislativa imposta all'autonomia dei privati la quale si manifesta soltanto nel momento di accesso alla rete di agenti. Occorre regolare la gestione del rischio connesso alle decisioni «reticolari» tanto per la liquidazione finanziaria dei danni che per il controllo a mezzo della programmazione delle azioni «reticolari»⁸⁵. Tuttavia, ciò non oblitera del tutto il bisogno di imputazione soggettiva della responsabilità se soltanto si considera il riferimento ad un'imputazione «non causale, ma collettiva». Tale imputazione serve «per realizzare le finalità della responsabilità collettiva, [e perché] il diritto [possa] identifica[re] autoritativamente le relazioni concrete di rischio che si instaurano tra il mondo *off-line* ed il mondo *on-line*».

Dunque, nel prendere atto della difficoltà, nuova al diritto, di identificare soggettivamente una collettività potenzialmente sparsa ovunque nello spazio digitale, una soggettività multipolare diffusa, non deve escludersi l'identificazione o, se si vuole, il ritrovamento di una «comunità di nodi algoritmici» soggettivamente semi-personificati in un agente collettivo al quale riferire l'«entità sociale» che ne domina le decisioni e le responsabilità.

In prima conclusione, l'intelligenza artificiale può assumere tre livelli graduati di soggettivazione⁸⁶: un primo che innesta la persona e le sue qualità cogni-volitive; un secondo che soggettivizza un attore che esegue un progetto umano; un terzo che è attante dell'uomo⁸⁷.

Quest'ultimo può manifestarsi in una rete diffusa nell'universo digitale e preferisce un intervento legislativo per l'esatto rinvenimento della comunità artificiale.

Il primo livello di soggettivazione si confonde con la persona, il secondo riconduce ad essa, il terzo è soggettività a sé⁸⁸.

Comunque, la soggettività (non la persona) e la responsabilità non sono scopi-valori dell'ordinamento ma strumenti –per quanto sofisticati– dei quali esso si avvale per meglio perseguire la tutela della persona⁸⁹.

Note di chiusura

¹ È la concezione proposta da A. TURING, *Computing Machinery and Intelligence*, in *Mind, New Series*, 1950, v. 59, n. 236, p. 433 e ss. ove si sostiene che l'idea sottesa al funzionamento digitale può spiegarsi con l'osservare se le macchine sono capaci di svolgere operazioni allo stesso modo di come sarebbe capace l'uomo, così introducendo il confronto emulativo allo scopo di riportare e ridurre la riflessione al dato oggettivo dell'operabilità della macchina.

² L'asserzione è controversa. Si ritiene che la soggettivazione dell'AI sia un elemento di complessità inutile ai fini della individuazione del criterio di responsabilità per i danni provocati dall'agente macchinico (*digital agent*), v. G. FINOCCHIARO, *Intelligenza artificiale e responsabilità*, in *Contr. Impr.*, 2020, 2, p. 713 e ss., la quale A. per lo stesso fine ritiene infruttuosa la ricerca dell'errore che ha provocato il danno: «La ricerca dell'errore *ex post*, indubbiamente utile per chi sviluppa i programmi informatici, è assai dispendiosa e non sempre percorribile con successo, se si tratta di applicazioni che operano in modo non deterministico». L'A. parla di responsabilità oggettiva basata sulla allocazione del rischio, «sulla responsabilizzazione del soggetto che trae vantaggio dall'applicazione di intelligenza artificiale», di tal che tale beneficiario è indotto ad adottare «le misure necessarie ad evitare il rischio».

³ G. GITTI, *Tecnologie digitali, persona e istituzioni*, in *Riv. dir. civ.*, 6, 2020, p. 1231, distingue l'intelligenza artificiale «debole» che è rivolta alla «raccolta e [al]la conservazione dei dati [e che] rappresenta la potenzialità più coltivata dalle applicazioni informatiche, anche in ambito giuridico», dalla robotica (o AI «forte») che dalla semplice conservazione ed elaborazione del dato è in grado di passare alla sua trasformazione, grazie ad una funzionalità ulteriore acquisita attraverso un processo di autoapprendimento. Sarebbe infatti caratteristica del robot la capacità di imparare a compiere attività non previste dal costruttore/programmatore, ma derivate dalla programmata elaborazione di operazioni poste in essere abitualmente. L'*output* della macchina potrebbe essere il frutto dell'esperienza pregressa dello stesso robot e non soltanto risultato di un'operazione statistico-matematica».

⁴ In questo senso è la riflessione nel diritto tributario, v. A. URICCHIO, *Robot tax: modelli di prelievo e prospettive di riforma*, in *Giur. It.*, 7, 2019, p. 1749 e ss., ove si legge: «Allo stesso tempo, appare necessario interrogarsi se e quali intelligenze artificiali possano essere assunte a tassazione stante la varietà e la complessità del fenomeno e soprattutto se e quando le macchine possano assumere una soggettività giuridico-tributaria, pur se prive di corporeità e di cervello. In questo senso, il *Committee on Legal Affairs of the European Union* il 31

maggio 2016, ha pubblicato un rapporto (poi accettato dal Parlamento europeo il 1 gennaio 2017) sulla crescente importanza dell'uso dei robot nella società moderna nel quale sono evidenziate le competenze cognitive dei robots che li rendono simili a soggetti (*"more and more similar to agents that interact with their environment and are able to alter it significantly"*)... Aggiunge il rapporto *"In this context, major changes to the current legal system could be contemplated, such as granting robots a sort of 'electronic personality' and the possibility to be liable for actions, not to mention aspects related to privacy, intellectual property or criminal law"*). Nell'affrontare il tema della soggettività dei robot ai fini dell'imposizione (ma ovviamente la questione può essere posta anche con riguardo ad altri settori dell'ordinamento), il rapporto rappresenta la necessità di una solida definizione legislativa in grado di superare i non pochi dubbi che possono porsi con riguardo alle differenti tipologie di intelligenze artificiali. A questo riguardo viene proposta la nozione di *smart robot* (robot intelligenti), non potendo estendere la soggettività a *computers* o a *software* e nemmeno a strumenti come le auto senza conducente che restano auto sebbene *self-driving* (c.d. *intelligenze artificiali weak*). Decisivo ai fini di un futuribile riconoscimento della soggettività tributario è la capacità del robot di assumere decisioni in autonomia e di accrescere le proprie competenze e conoscenza (*intelligenze artificiali hard*). [...] Secondo gli standard internazionali ISO 8373:2012 per robot si intende un *"actuated mechanism programmable in two or more axes with a degree of autonomy, moving within its environment, to perform intended tasks"*. *The standard further specifies that a robot includes the control system and interface of the control system. The International Federation of Robotics (IFR) uses the same definition as the ISO standard.*¹² *Nevadans suggests that a legal definition of robots be based on six conditions. In her view, a robot: (i) is a physical machine ("machine matérielle"); (ii) is alimented by energy; (iii) has a capacity to act in the real world; (iv) can analyse the environment; (v) can render decisions; and (vi) can learn"*. [...] Come è noto, l'ordinamento tributario accede ad una nozione di soggettività che non si identifica con la capacità giuridica di diritto comune né tantomeno con dati naturalistici o antropomorfici, assumendo una situazione giuridica, definita dal diritto positivo in grado di rivelare capacità contributiva. Depurato, quindi dai caratteri naturalistici della persona fisica e dai requisiti antropomorfici attribuiti alle organizzazioni formalmente entificate (l'omone di tradizione ottocentesca), il soggetto passivo d'imposta coincide, pertanto, con la situazione giuridico tributaria, presentando piena autonomia rispetto alle categorie civilistiche. Ciò consente di riconoscere un processo graduale di espansione della soggettività tributaria, in grado di comprendere, oltre a persone giuridiche e enti non personificati (associazioni non riconosciute, ecc.) anche

entità diversamente apprezzabili idonee a manifestare il presupposto d'imposta in modo unitario e autonomo (in questo senso si veda l'art. 73 T.u.i.r. n. 917/ 1986 sono compresi "oltre alle persone giuridiche, le associazioni non riconosciute, i consorzi e le altre organizzazioni non appartenenti ad altri soggetti passivi nei confronti delle quali il presupposto dell'imposta si verifichi in modo unitario ed autonomo")».

⁵ Interessante segnalare quanto osserva G. Finocchiaro, *Intelligenza artificiale*, cit., p. 721, ove si legge: «Infatti, come è noto, l'intelligenza artificiale si basa sui dati. Una delle ragioni per le quali, pur essendo stata ampiamente studiata già molti anni fa, e pur essendo sotto molti aspetti già matura, non aveva dato luogo ad applicazioni tecnologiche diffuse, era costituita dall'assenza di una grande quantità di dati a disposizione, oltre che dalla differente potenza di calcolo e dalla minore connettività disponibile. Si stimano in miliardi gli utenti che quotidianamente fruiscono dati, spesso non consapevolmente, per esempio attraverso i *social network* e i motori di ricerca, in tutto il mondo. L'intelligenza artificiale si nutre di dati e ora i dati sono certamente disponibili, spesso addirittura gratuitamente».

⁶ V., la Risoluzione del Parlamento europeo, 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103), (par. 59, lett. f), ivi la Commissione europea è invitata a considerare tra le possibili soluzioni giuridiche per la responsabilità dei robot anche «l'istituzione di uno *status* giuridico specifico per i robot nel lungo termine (...) nonché eventualmente il riconoscimento della personalità elettronica dei robot».

⁷ Scrive, P. CALAMANDREI, *Il nuovo processo civile e la scienza giuridica*, in ID., *Studi sul processo civile*, V, 1941, pp. 81 e 86: «ogni giurista è libero di adottare le distinzioni e le classificazioni che crede, purché servano agli scopi pratici del diritto di cui egli è servitore».

⁸ L'uso del termine non è da intendere come l'atteggiamento umano che tende a ricondurre i fenomeni che lo circondano secondo i canoni del suo pensiero ma in una accezione riduttiva volta ad osservare i modelli di azione dell'uomo con la lente del diritto.

⁹ Per una ricostruzione della cultura giuridica sul tema della soggettività, v. C. PERLINGIERI, *Enti e diritti della persona*, in *Pubblicazioni della Scuola di specializzazione in diritto civile dell'Università di Camerino*, 112, Napoli, 2008, spec. p. 69 e ss. ove l'Autrice ricostruisce le teorie che hanno spiegato le soggettività. In particolare, l'Autrice pone in evidenza come le elaborazioni sono incentrate sulla polarizzazione tra la concezione normativistica e l'altra sociologica. La

prima pone in risalto il ruolo costitutivo del diritto quale elemento generativo della soggettività; la seconda accentua la dimensione realistica del fenomeno associativo e, quindi, della soggettività. La contrapposizione teorica ripropone la diade norma-fatto. L'Autrice rileva che il tema della soggettività non deve essere omologato a quello della persona umana poiché il primo trova rilievo nell'ordinamento giuridico in considerazione esclusiva della prospettiva funzionale per la quale le soggettività (diverse dalla persona) sono tutelate. Dunque, emerge il profilo dell'interesse meritevole di tutela che connota la ragione giustificatrice della rilevanza giuridica della nuova soggettività. Questa considerazione tende al superamento della dicotomia fatto-norma giacché l'interesse, per quanto espressione della realtà, si completa nel giudizio di meritevolezza dell'ordinamento, il quale si esprime innanzitutto a mezzo della sua carta fondamentale. In questa i principi rilevano interessi di formazioni sociali non sovrapponibili a quelli dei singoli appartenenti al gruppo, sebbene in tale processo di identificazione soggettiva non può rilevarsi un atteggiamento omogeneo dell'ordinamento. I livelli di rilevanza degli interessi dei gruppi sono molteplici e ad essi corrisponderanno altrettante dimensioni delle soggettività. Tuttavia, tali considerazioni non attengono alla persona umana la quale non subisce siffatta profilazione teleologica per essere essa valore in sé, fondante dello stesso sistema giuridico. Dunque, lungi dal polarizzare il dibattito tra la persona giuridica e fisica, il tema della soggettività esprime nella sua complessità la varietà dei contenuti assiologici e teleologici che l'ordinamento tutela, divaricandosi in interessi meritevoli di tutela affidati ad una titolarità soggettiva che ne è portatrice-agente. Senza con ciò confondere la soggettività, come generata da interessi collettivi e autonomi meritevoli, con la sua titolarità, come soggetto al quale i primi sono intestati. Tra i casi più controversi si dibatte della famiglia. Premessa la ormai condivisa moltiplicazione in famiglie, la Costituzione nella società naturale fondata sul matrimonio connette interessi del gruppo che non sono sovrapponibili agli interessi dei singoli componenti. Dunque, non può negarsi una espressione sebbene minima di soggettività anche alla famiglia. Tuttavia, ognuna delle espressioni di soggettività deve comprendersi nella funzione strumentale di essa allo sviluppo della persona umana (art. 2 cost.).

¹⁰ Sull'argomento, v., F. DI GIOVANNI, *Attività contrattuale e intelligenza artificiale*, in *Giur. it.*, 7, 2019, p. 1677 e ss., ove l'A. segue la concezione normativistica e afferma che «Il contratto, perciò, non è un esercizio di libertà "grazie" alla legge: la conclusione del contratto segna, al contrario, il momento nel quale la libertà delle parti di fare quel che vogliono dei propri interessi (e del proprio patrimonio) viene assoggettata ad un vincolo, e viene regolata secon-

do un limite. [...] Si è parlato, come noto, di “scambi senza accordo”, e di contro si è replicato che anche in tali moderne modalità di contrattazione l'accordo è ravvisabile eccome, poiché né la trattativa, né il dialogo, né finanche l'espressione linguistica si richiedono perché vi sia contratto, e dunque perché vi sia accordo nel senso declinato dalla legge. Anzi, si osserva, di accordo contrattuale può e deve parlarsi sol che si adotti una accezione normativa di tale concetto capace di accogliere tutte le modalità previste dalle diverse e molteplici regole di formazione del contratto e di determinazione del suo contenuto. Insomma, chi ha visto nelle moderne modalità di attuazione degli scambi un declino o una evanescenza dell'accordo lo ha fatto sul presupposto dell'adozione di una determinata accezione dell'accordo come fenomeno empirico. [...] Il passo successivo consiste nel ravvisare in tale autonomia decisionale (se non addirittura in questa volontà propria dell'intelligenza artificiale) la manifestazione di una soggettività di diritto distinta da quella del contraente “umano”. Ed una volta postulata questa alterità soggettiva, non sarebbe difficile rivestire questo soggetto (“altro” rispetto al contraente umano) dei caratteri propri di ogni soggetto di diritto, non solo riferendo alla intelligenza artificiale stati soggettivi rilevanti, ma dotandola anche della “titolarità” di un patrimonio o meglio di un *peculium* (ad esempio sotto forma di criptovaluta), al fine di risolvere il problema di collegare al ruolo assunto dall'intelligenza artificiale anche una responsabilità distinta da quella della parte contrattuale “umana”. [...] Anzitutto, quella costruzione implica l'idea che meriti di essere applicata la categoria del “soggetto di diritto” per il solo fatto che si riscontra, nella realtà fattuale, una entità dotata di certi caratteri (cioè la capacità di esprimere scelte autonome, di autodeterminarsi secondo opzioni consapevoli, ecc.), e cioè che il soggetto di diritto non sia altro che la trasfigurazione sul piano giuridico di tale entità empirica, grazie alla sua somiglianza all'uomo (così come quest'ultimo è soggetto di diritto, la stessa qualificazione potrebbe essere attribuita per similitudine). Ma così ragionando, si travisa il senso dell'attribuzione della soggettività di diritto, di cui non v'è alcun bisogno nell'ambito della questione che stiamo esaminando, essendo quello di “soggetto di diritto” un concetto operativo che serve a tutt'altro. [...] L'utilità di tale rappresentazione soggettiva sta nel fatto che essa ci consente di esprimere mediante locuzioni semplici una serie complessa di norme, e soprattutto di esprimere la relazione di quelle valutazioni normative con altre catene di norme e di fatti. [...] In questo come in altri casi il concetto di soggetto di diritto ci serve essenzialmente ad esprimere il “tenersi assieme” di più rapporti, e rispetto a questo ruolo puramente logico, non v'è differenza tra soggetto “umano” e soggetto di altra natura, e non si può dire che il primo sia “vero”

soggetto ed il secondo lo sia solo per un espediente linguistico o per similitudine. Perciò, la nozione di “soggetto di diritto” viene in considerazione al fine di trattare in modo uniforme insiemi di rapporti unificati da un dato comune, a condizione, però, di non trattare “nessuno dei casi di soggettività” (nemmeno quello della soggettività umana) come la semplice traduzione giuridica di un dato della realtà materiale». Le osservazioni dell’A. presentano due elementi di criticità: la prima, si desume dalla considerazione che la «realtà materiale» non è soltanto materiale se si prende atto che la sussidiarietà orizzontale conferisce all’autonomia negoziale che persegue l’interesse generale il ruolo di fonte del diritto; la seconda, attiene alla necessità di dare alla «realtà materiale» del soggetto-uomo un radicamento valoriale differente dalle soggettività non umane. Ma su questi aspetti si ritornerà meglio nel testo.

¹¹ Scrive P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, quarta edizione riscritta e ampliata, I, *Metodi e tecniche*, Napoli, 2020, p. 257, che «La soggettività è giuridicamente rilevante ogni qualvolta la norma riconosce o attribuisce ad entità “esponenziali” l’idoneità ad essere punto di riferimento soggettivo di interessi e di attività. La soggettività è qualificazione giuridica che si desume non soltanto dalla previsione normativa generale ed astratta, ma anche dalle specifiche normative che attribuiscono a particolari entità il ruolo di soggetto, cioè di portatori di interessi morali o patrimoniali pur sempre rilevanti. La soggettività è, dunque, punto di riferimento soggettivo,» centro di imputazione di interessi e di situazioni soggettive. [...] Sotto il profilo metodologico è d’obbligo intendere la soggettività in forma plurima, con una accentuata diversificazione al suo interno, distinguendo i problemi della persona umana e i problemi di quei soggetti (differenti per scopi e funzioni) che persone umane non sono: le c.dd. persone giuridiche e ogni altro centro di imputazione soggettiva». Inutile aggiungere che la persona e valore-fine, mentre il soggetto è interesse-mezzo.

¹² Sul punto può essere interessante seguire il percorso che la dottrina e la giurisprudenza ha rinvenuto nel tema del condominio, si dibatte da tempo sulla soggettività dello stesso, v., *ex multis*, F. G. VITERBO, *Variabilità e relatività dei rapporti condominiali. Proprietà, persone, “gruppo”*, in *Pubblicazioni della Scuola di specializzazione in diritto civile dell’Università di Camerino*, 182, Napoli, 2022, in part. p. 137 e ss., ove si descrive il processo di soggettivazione –mai del tutto negato in dottrina- attraverso la differente considerazione dell’interesse patrimoniale e dei valori esistenziali di cui è portatore l’«organismo edilizio». Per quanto risulterebbe improprio generalizzare e omologare il fenomeno condominiale, non può dubitarsi che esso trae origine dalla pluralità di titolarità di situazioni giuridiche –alternativamente unitaria- che recano ad ogget-

to il medesimo bene, appunto l'edificio. Questo è strumento di realizzazione di detti interessi e valori, ma è al contempo patrimonio in gestione perché detti interessi e valori possano realizzarsi. Tale patrimonio non è elemento statico ma funzionale agli interessi predetti e richiede modelli di gestione variabili in considerazione della complessità dei primi, senza escludere che –in alcuni casi– in tale attività gestoria possa intravedersi anche una vera e propria impresa. Dunque, il tipo di interessi e valori che in concreto il condominio è chiamato ad assolvere richiede la scelta del modo più adeguato di organizzazione e gestione delle situazioni giuridiche strumentali e finali connesse ad esso. La minima unità effettuale è data dalla sicurezza, stabilità e decoro dell'edificio (art. 1122 c.c.), interessi e valori –questi– che possono combinarsi in modalità diversificata in considerazione del caso concreto, ma che, comunque, coesistono nell'edificio, e attorno ai quali si coagulano e conformano le situazioni giuridiche reali e personali dei condòmini. Pertanto, è *in re ipsa* che il condominio possa assumere una propria soggettività giuridica quando tali interesse e valori siano altri ed autonomi rispetto a quelli dei singoli condòmini, per quanto questi ultimi siano variamente collegati ai primi. In sintesi e con qualche approssimazione, si vuole sostenere che gli interessi e i valori sei singoli condòmini si espongono a inevitabili rischi quando gli interessi e valori del condominio non siano adeguatamente gestiti e mantenuti.

¹³ V. G. OPPO, *Declino del soggetto e ascesa della persona*, in *Riv. dir. civ.*, 6, 2002, p. 829 e ss., ove si legge che «La soggettività di diritto è anche questo ma non solo questo: non si esaurisce in una posizione passiva ma è anche una posizione attiva, nella quale si attesta la stessa nozione di capacità giuridica. Ma la distinzione resta, se “persona” è riferibile a una realtà umana che preesiste, anche giuridicamente, al diritto positivo e a causa della quale il diritto è costituito (con ciò rettifico, ma solo nella terminologia, quanto ho scritto altra volta). Ascesa di questa realtà rispetto alla soggettività dovrebbe allora significare maggiore riconoscimento, e maggiore incidenza sul sistema, della sua preesistenza, anche giuridica, al diritto positivo. [...] Può sembrare che sotto questo aspetto non debbano esservi divergenze e che non stia al diritto, in qualunque senso, giudicare dell'esistenza dell'uomo. Eppure così non è perché la natura si mescola con la tecnica che la modifica e a volte la sconvolge. Il che chiama in causa il diritto. [...] Il diritto positivo può negare il soggetto o limitare la soggettività, non può negare l'uomo; quando neghi il soggetto, persona e soggetto possono separarsi».

¹⁴ Scrive G. OPPO, *Ancora su persona umana e diritto*, in *Riv. dir. civ.*, 2007, 2, p. 259 e ss.: «a monte del diritto positivo vi è un diritto della società, insito nella medesima come principio e regola della coesistenza. Non si tratta di un diritto

naturale ma di un diritto proprio delle diverse società - ispirato quindi ai loro "valori", non necessariamente "universali" - capace di sostenere e sollecitare il diritto positivo e anche di prevalere su di esso, talvolta con l'azione di propri organi giurisdizionali. Nell'occasione ricordata, mi sono trovato d'accordo con Falzea e con Cotta che parlano, rispettivamente, di diritto sociale contrapposto ai diritti civili e di un diritto proprio dei gruppi sociali come tali. [...] Il diritto sociale riconosce come persona l'uomo: può dare rilievo anche a realtà diverse dall'uomo, realtà che il diritto positivo riconosce come soggetti, non può considerare persona altro che l'uomo. Si tratta quindi di stabilire quando vi sia l'uomo persona e quando vi sia l'uomo soggetto. [...] I "diritti dell'uomo" di cui tanto parlano gli ordinamenti positivi degli Stati e le dichiarazioni internazionali, sono in realtà, o dovrebbero essere, prima che diritti "soggettivi", nel senso di diritti "del soggetto", diritti della persona. I diritti alla vita, alla dignità umana, alla integrità fisica e psichica, alla libertà, all'uguaglianza, alla paternità e maternità, non sono beni elargiti dall'ordine giuridico positivo ma discendono dall'appartenenza a una società e sono ora riconosciuti da più Costituzioni, da ultimo quella europea. [...] La persona in una società umana è l'uomo; l'essere nella società gli attribuisce quei beni che il diritto positivo può riconoscerli e difendere e può anche menomare o sopprimere. Ma il diritto positivo, come non può distruggere l'appartenenza alla società, così non può distruggere la persona. [...] L'uomo quindi è persona per la sua esistenza nella società. [...] Il diritto positivo può, come dicevo, non solo riconoscere e regolare ma anche disconoscere e manipolare diritti della persona. Lo fa dettando lo statuto della soggettività giuridica e a volte incidendo direttamente sui diritti dell'uomo. Qui può incontrare controlli e contrasti anche al suo interno benché su questo piano il compromesso sia all'ordine del giorno. Al di là di esso vi è ora una possibilità di controllo da parte di un giudice superiore e vi è il giudizio della storia, che vuol dire della stessa società umana».

¹⁵ Sul ruolo metodologico dell'interesse rispetto alla volontà, v., con ampi riferimenti bibliografici, P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo europeo delle fonti*, quarta edizione riscritta e ampliata, I, *Metodi e tecniche*, Napoli, 2020, p. 115 e ss.

¹⁶ Cfr. Corte cost., 13 aprile 2016, n. 84, in Sito uff. Corte cost., 2016, che ritiene inammissibile la questione di legittimità costituzionale dell'art. 13, commi 1, 2 e 3, della legge 19 febbraio 2004, n. 40, impugnato, in riferimento agli artt. 2, 3, 9, 13, 31, 32 e 33, primo comma, Cost., in quanto vieta in modo assoluto qualsiasi ricerca clinica o sperimentale sull'embrione umano che non sia finalizzata, in assenza di metodologie alternative, alla tutela della salute e allo sviluppo dello stesso. Il quesito rimanda al conflitto, gravido di implica-

zioni etiche oltretutto giuridiche, tra il diritto della scienza (e i vantaggi della ricerca ad esso collegati) e il diritto dell'embrione, per il profilo della tutela (debole o forte) ad esso dovuta in ragione e in misura del (più o meno ampio) grado di soggettività e di dignità antropologica che gli venga riconosciuto. Sulla soluzione di questo conflitto i giuristi, gli scienziati e la società civile sono profondamente divisi; ed anche le legislazioni, i comitati etici e le commissioni speciali dei molti Paesi che hanno approfondito il problema non sono pervenuti a risultati generalmente condivisi. La Corte di Strasburgo, escludendo nella sentenza della *Grande Chambre* del 27 agosto 2015 (Parrillo contro Italia), in *Ragiusan*, 2016, pp. 385-386, che il censurato divieto di sperimentazione violasse l'art. 8 della Cedu, ha osservato che la donazione degli embrioni non destinati a impianto solleva delicate questioni morali ed etiche sulle quali non esiste un vasto consenso europeo e che il Governo italiano non ha ecceduto l'ampio margine di discrezionalità che gli compete. Pertanto, nella scelta (ampiamente divisiva sul piano etico e scientifico, in assenza di soluzioni uniformi nella legislazione europea) tra il rispetto del principio della vita, che si racchiude nell'embrione, e le esigenze della ricerca scientifica, la linea di composizione tra gli opposti interessi attiene all'area degli interventi con cui il legislatore, quale interprete della volontà della collettività, è chiamato a tradurre, sul piano normativo, il bilanciamento tra valori fondamentali in concorso, tenendo conto degli orientamenti e delle istanze che apprezzi come maggiormente radicati, nel momento dato, nella coscienza sociale. Quella recata dalla normativa impugnata è una scelta di così elevata discrezionalità, per i profili assiologici che la connotano, da sottrarsi, per ciò stesso, al sindacato di costituzionalità. Per di più, una diversa ponderazione dei valori in concorso, nella direzione di una maggiore apertura alle esigenze della collettività correlate alle prospettive della ricerca scientifica, non potrebbe comunque introdursi nel tessuto normativo per via di un intervento additivo, stante il carattere non «a rima obbligata» di esso. Il differente bilanciamento, che per mezzo dell'incidente di costituzionalità si vorrebbe sovrapporre a quello presidiato dalla normativa scrutinata, non potrebbe, infatti, non attraversare (e misurarsi con) una serie di molteplici opzioni intermedie, inevitabilmente riservate al legislatore. Unicamente a quest'ultimo compete la valutazione di opportunità (sulla base anche delle «evidenze scientifiche») e del loro raggiunto grado di condivisione a livello sovranazionale) in ordine, tra l'altro, all'utilizzazione, a fini di ricerca, dei soli embrioni affetti da malattia - e da quali malattie - ovvero anche di quelli scientificamente «non biopsabili»; alla selezione degli obiettivi e delle specifiche finalità della ricerca suscettibili di giustificare il «sacrificio» dell'embrione; all'eventualità, ed alla determinazione

della durata, di un previo periodo di crioconservazione; all'opportunità o meno di un successivo interpellato della coppia, o della donna, che ne verifichi la confermata volontà di abbandono dell'embrione e di sua destinazione alla sperimentazione; alle cautele più idonee ad evitare la «commercializzazione» degli embrioni residui.

¹⁷ In argomento, F. Viola, *Umano e post-umano: la questione dell'identità*, in F. Russo (a cura di), *Natura, cultura, libertà*, Roma, 2010, p. 93 s., S. Rodotà, *Il corpo e il post-umano*, in F. Ruscello (a cura di), in *Studi in onore di Davide Messinetti*, Napoli, 2008, p. 838; Id., *Dall'umano al postumano*, in Id., *Vivere la democrazia*, Bari, 2019, p. 132 ss.; spunti di riflessione si rinvencono nel lavoro di M.A. Lemley, IP in a world without Scarcity che è possibile reperire sul sito https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2413974.

¹⁸ V. M. TESCARO, *La tutela postmortale della personalità morale e specialmente dell'identità personale*, in *Studi in onore di Maurizio Pedrazza Gorlero*, I, Napoli, 2014, pp. 825 ss. e 846 ove si legge che «la personalità del defunto può continuare con la morte, con la conseguenza che, accogliendo la tesi della successione *mortis causa* nei diritti della personalità, si potrebbe anche recuperare, sia pur adattandola ai nostri tempi, l'idea, emersa nell'antichità romana, secondo cui il successore sarebbe appunto il continuatore della persona del defunto». Cfr. Cass. 15 maggio 2019, n. 13000, in CED Cassazione, 2019, che stabilisce che l'art. 8 della l. n. 40 del 2004, recante lo status giuridico del nato a seguito dell'applicazione delle tecniche di procreazione medicalmente assistita, è riferibile anche all'ipotesi di fecondazione omologa «*post mortem*» avvenuta mediante utilizzo del seme crioconservato di colui che, dopo aver prestato, congiuntamente alla moglie o alla convivente, il consenso all'accesso alle tecniche di procreazione medicalmente assistita, ai sensi dell'art. 6 della medesima legge e senza che ne risulti la sua successiva revoca, sia poi deceduto prima della formazione dell'embrione avendo altresì autorizzato, per dopo la propria morte, la moglie o la convivente all'utilizzo suddetto. Ciò pure quando la nascita avvenga oltre i trecento giorni dalla morte del padre» (in applicazione di tale principio, la S.C. ha ritenuto che nell'atto di nascita alla figlia minore della ricorrente, nata a seguito di inseminazione medicalmente assistita «*post mortem*», possa essere attribuito lo status di figlia del marito deceduto). Vedi, anche, Corte App. l'Aquila, 19 ottobre 2013, in *Pluris*, secondo cui lo *ius eligendi sepulchrum*, ovvero il diritto del vivente di poter scegliere il modo ed il luogo di sepoltura, è riconosciuto, dalla giurisprudenza, su base consuetudinaria, in assenza di specifiche norme che lo contemplano, come diritto personale ed assoluto del defunto, che può esercitarlo in vita o delegarne, senza particolari forme, a terzi l'esercizio *post mortem*. Quando non risulta

espressa alcuna volontà, opera in via sussidiaria il diritto dei congiunti di provvedere alla destinazione della salma con prevalenza dello *ius coniugii* sullo *ius sanguinis* e di questo sullo *ius successionis*.

¹⁹ V. M. SPANÒ, *Azioni collettive. Soggettivazione, governabilità, neoliberalismo*, Napoli, 2013, p. 143, «...in un'azione collettiva il soggetto dell'azione non presiste all'azione stessa; è piuttosto lo stesso interesse a produrre il soggetto dell'azione, soggetto che, nella sua stessa consistenza ontologica, esiste nel momento della rivendicazione e dell'istanza, e scompare, oppure si trasforma, con l'esaurirsi dell'azione stessa». Secondo Cass., S.U., ord., 30 settembre 2015, n. 19453, in CED Cassazione, 2015, la «*class action pubblica*» prevista dal d.lgs. n. 198 del 2009 è funzionale al conseguimento di un risultato che giovi, indistintamente, a tutti i contitolari dell'interesse diffuso al ripristino del corretto svolgimento della funzione amministrativa ovvero della corretta erogazione del servizio, mentre l'azione di classe prevista dal codice del consumo postula l'esercizio di un diritto individuale, oggetto di trasposizione in capo a ciascun titolare singolarmente identificato, sicché appartiene alla giurisdizione del giudice ordinario la domanda risarcitoria svolta, a norma dell'art. 140-bis del d.lgs. n. 206 del 2005, dall'utente di un servizio pubblico nei confronti del soggetto privato assunto come inadempiente in relazione al corrispondente contratto (nella specie, di trasporto pubblico) attuativo del servizio. Cfr. anche, TAR Basilicata Potenza Sez. I, 23 settembre 2011, n. 478, in *Corr. mer.*, 2012, 3, 309, con nota di M. NEFELI Gribaudo, *Pec: un'occasione per fare chiarezza sui requisiti di ammissibilità della class action amministrativa*, che afferma che la legittimazione e l'interesse ad agire nella *class action* per i diritti digitali vanno riconosciuti alle associazioni che «dimostrino di possedere sufficienti indici di rappresentatività degli interessi diffusi di una particolare categoria di utenti». Vale a dire che non è sufficiente essere costituiti in generica associazione, anche se a tutela del ripristino della legalità violata, per poter validamente azionare una *class action*. Pertanto, la tutela dei diritti digitali può essere invocata solo allorché l'associazione sia rappresentativa dello specifico interesse asseritamente leso dalla P.A. a causa della mancata attuazione delle disposizioni del codice dell'Amministrazione Digitale. Nel caso di specie, è stato ritenuto che la menzione nello statuto dell'Associazione del fine di «difendere le libertà digitali» potesse essere considerata sufficiente a dimostrare la legittimazione ad agire della detta associazione.

²⁰ V. F. RESCIGNO, *I diritti degli animali: da res a soggetti*, Torino, 2014, p. 50, ove si legge che «gli animali non sono cose, hanno bisogni, desideri, speranze, consce ed inconse, istinti, pulsioni, direzioni evolutive e realizzazioni naturali: essi sono portatori di interessi...», dunque, è utile che ad essi «venga rico-

nosciuta una particolare capacità giuridica alla quale collegare uno specifico bagaglio di diritti che, come nel caso degli umani marginali, abbisogneranno di tutela e rappresentanza da parte di apposite figure [umane]». Cfr. Corte giust. UE, 28 luglio 2016, n. 469/14, Masterrind GmbH c. Hauptzollamt Hamburg-Jonas, in Pluris, la quale sancisce che l'allegato I, capo V, punto 1.4, lettera d), del regolamento (CE) n. 1/2005 del Consiglio, del 22 dicembre 2004, sulla protezione degli animali durante il trasporto e le operazioni correlate che modifica le direttive 64/432/CEE e 93/119/CE e il regolamento (CE) n. 1255/97, dev'essere interpretato nel senso che, nell'ambito di un trasporto su strada di animali delle specie considerate, in particolare quelli della specie bovina tranne i vitelli, da un lato, il periodo di riposo tra i periodi di viaggio può essere di regola superiore a un'ora. Tuttavia, detta durata, laddove sia superiore a un'ora, non dev'essere tale, nelle condizioni concrete in cui si svolgono il riposo e il trasporto complessivamente considerati, da esporre a lesioni o a sofferenze inutili gli animali trasportati. Inoltre, i periodi di viaggio e di riposo combinati, previsti al punto 1.4, lettera d), di tale capo, non possono eccedere le 29 ore, fatta salva la possibilità di prolungarli di 2 ore nell'interesse degli animali, ai sensi del punto 1.8 di detto capo, e ferma restando l'applicazione delle disposizioni dell'articolo 22 del medesimo regolamento in caso di circostanze imprevedibili. Dall'altro lato, i periodi di spostamento della durata massima di 14 ore ciascuno possono includere una o più fasi di sosta. Tali fasi di sosta devono essere aggiunte alle fasi di spostamento ai fini del calcolo della durata totale del periodo di trasporto di un massimo di 14 ore di esse fanno parte.

²¹ In dottrina, vedi, P. Dell'anno, *Diritto dell'ambiente*, Milano, 2018, p. 24, dove si legge che la riforma «ha elevato la tutela dell'ambiente da interesse pubblico a valore costituzionale, cioè ha attribuito ad essa una posizione primaria nell'ordinamento» e p. 31: «La qualifica di “valore costituzionale” indica la rilevanza che l'ordinamento attribuisce al bene giuridico ambiente, la funzione che è destinato a svolgere nel contesto istituzionale, la scala di priorità nella quale è collocato nei confronti di altri beni giuridici ed interessi pubblici da tutelare, l'intensità e l'estensione della tutela» (corsivo dell'A.), ed ivi per altri ragguagli.

²² Cfr. Cass. pen. 11 gennaio 2005, n. 5766, in *Riv. pen.*, 2006, 2, 227, che ritiene: in tema di tutela delle zone di particolare interesse ambientale, è necessaria l'autorizzazione per effettuare un intervento in zone protette, salvo che esso sia di irrilevante entità e tale da non incidere neppure in astratto sull'ambiente. Pertanto, la realizzazione di un argine, con deviazione delle acque di un fiume, deve essere sottoposta al controllo di impatto ambientale, né è invocabile l'applicabilità dell'art. 58 del testo unico sulla disciplina delle acque

pubbliche, il quale – a sua volta – consente ai privati di eseguire opere idrauliche a difesa della proprietà solo quando non sia in alcun modo alterato il regime dell'alveo.

²³ V. R. MIGUEL NUNEZ, *Le avventure del soggetto. Contributo teorico-comparativo alle nuove forme di soggettività giuridiche*, Milano, 2018, p. 111 ss. ove si ha riguardo ai diritti «della natura» e si discutono pronunce di Corti di altri Paesi del mondo. «Il 20 marzo 2017 l'Alta Corte dell'Uttarakhand (Nainital, India) emette un'ordinanza in cui si afferma che il fiume Gange e il suo principale affluente, il Yamuna, “respirano, vivono e offrono sostentamento alle comunità dalle montagne al mare”, sicché “esiste il massimo vantaggio nel conferire [a questi fiumi] lo status di persona vivente/entità legale”». Di conseguenza i due fiumi, i loro affluenti e ogni corso d'acqua che scorre con flusso continuo o ininterrotto da essi sono dichiarati “*juristic/legalpersons/living entities*”, con tutti i corrispondenti diritti, doveri e responsabilità di una persona vivente. Dieci giorni più tardi, la stessa Corte, in una sentenza ancora più documentata, sancisce per “i ghiacciai compresi il Gangotri e il Yamunotri, fiumi, torrenti, ruscelli, laghi, aria, prati, valli giungle, foresta, zone umide, praterie, sorgenti e cascate» la qualità di *legal entity/legal person/juristic person/juridicial person/moral person/artificial person*” al fine della loro preservazione. Allo stesso modo la Corte costituzionale colombiana riconosce «l'Amazzonia colombiana come entità “soggetto di diritti” titolare della protezione, conservazione, mantenimento e ripristino a carico dello Stato e delle entità territoriali competenti (*sentencia* STC 4360-2018 (5 aprile 2018), p. 45, in www.legal.legis.com.co/document). L'A. riferisce che nel 2010 il consiglio comunale della città di Pittsburgh, sulla base degli «*inalienable and fundamental right to exist and flourish*» delle comunità naturali e degli ecosistemi adotta la prima ordinanza statunitense che vieta alle *corporations* l'attività di *fracking*, pratica inquinante e dannosa.

²⁴ V. R. MIGUEL NUNEZ, *Le avventure del soggetto*, cit., pp. 109-110, «Parafra-
sando Ross, “nulla impedisce che il diritto riconosca come interesse protetto da un diritto soggettivo qualcosa di diverso da un interesse umano”. In questa prospettiva è evidente che la teoria dell'interesse, lungi dal pretendere di definire i confini dell'universo dei potenziali titolari dei diritti, lascia interamente aperta la gamma di entità che possono essere racchiuse entro tali confini. Conseguentemente, dalla prospettiva puramente formale, la nozione di soggetto di diritto si allarga o restringe a seconda siano o meno positativi i giudizi morali di certi ceti, i quali agiranno in rappresentazione dell'interesse giuridificato. Siamo così di fronte ad un significativo sviluppo della nozione del soggetto che, prendendo le mosse dalle acquisizioni dottrinarie del Novecento, proietta nel futuro soluzioni per tutelare le entità “incerte” o “intermedie”».

²⁵ Sul punto v. le considerazioni di U. RUFFOLO E A. AMIDEI, *Intelligenza Artificiale e diritti della persona: le frontiere del "transumanesimo"*, in *Giur. It.*, 2019, p. 1658 e ss., ove si discute dell'incidenza dell'A.I. nella personalità umana e dei problemi giuridici connessi, «Talune pratiche, inizialmente osteggiate dall'ordinamento, sulla base di una visione paternalistica della protezione della salute, in quanto "superflua esposizione a menomazioni fisiche", costituiscono poi, secondo una giurisprudenza che si consolida parallelamente alla loro accettazione sociale, lecita attività ludica volta anche al "superamento dei limiti umani", e positivamente valutata dall'ordinamento in quanto fattore di perseguimento della salute, intesa come condizione dinamica di benessere psicofisico, e, soprattutto, di sviluppo della personalità dell'individuo (vedasi, ad esempio, Cass. pen., 19473/2005). Non è, dunque, il mero consenso dell'interessato, bensì l'esercizio di un diritto fondamentale della persona a legittimare in linea di principio le attività sportive estreme "accettate" (pur essendo il libero e consapevole consenso dell'atleta sempre necessario, in modo non dissimile da quanto avviene in ambito medico-sanitario). [...] Siffatti parallelismi sembrano poter confortare indirizzi interpretativi idonei a legittimare molte pratiche, anche invasive, di *human enhancement* sulla base di una nozione di "salute" ex art. 32 Cost. interpretata attraverso la lente dell'art. 2 Cost., quale "condizione [...] di benessere fisico e psichico della persona", come la definisce anche il Codice di deontologica medica. Definizione condivisa anche dall'Organizzazione Mondiale della Sanità, che qualifica la "salute" come condizione di perfetto benessere fisico, psichico e mentale, ben lontano dalla mera "assenza di malattia", e soprattutto correlato alle possibilità per il singolo, *dominus* del proprio corpo, di realizzazione della propria personalità in sintonia con la percezione che ha di sé. [...] Torniamo, invece, alle questioni della compatibilità di tali tecnologie con gli attuali approdi nella vasta materia dei diritti umani e della persona. Inevitabile allora chiedersi se ed in che misura possano essere ipotizzabili limiti alla praticabilità di (talune) forme di *human enhancement* quando queste siano suscettibili di sortire siffatti effetti ultrattivi sul piano intergenerazionale; anche a tutela delle generazioni future quali "soggetti deboli", come protezione di un diritto "super-individuale" a non vedere alterata la natura della propria specie. E riflettiamo anche su un differente, connesso, problema: non si è ancora in grado di escludere l'ipotesi che, a fronte di profonde modificazioni della "essenza umana", la "natura si ribelli", innescando reazioni in qualche misura "protettive". Allora, l'eccessivo ed "ubrico" superamento delle barriere della specie dovrà essere considerato illecito anche in virtù di un generale "principio di precauzione", per prevenire non prevedibili rischi di dare ingresso a nuove patologie? Quando il

diritto (e la libertà) del singolo ad autodeterminarsi entra in conflitto con la esigenza di preservare e perpetuare integra la “condizione umana”, quest’ultimo “interesse collettivo” deve prevalere su ogni diritto individuale protetto. In altri termini, deve negarsi il diritto ad apportare al proprio corpo alterazioni modificative capaci di incidere sul patrimonio genetico e divenire così trasmissibili ereditariamente sino, in prospettiva, a rendere “mutante” la specie umana. Basti solo considerare parallelamente come l’art. 32 Cost. assicura sacrale protezione al diritto individuale alla salute, ma lo subordini alle esigenze di tutela dell’interesse collettivo alla salute stessa. Tale norma è rappresentativa del prevalere di taluni fondamentali interessi superindividuali quando in conflitto con “diritti” del singolo, allora eticamente e giuridicamente comprimibili in nome di “superiori” interessi della collettività. Ce lo conferma il Preambolo alla Carta di Nizza, che dichiara l’obiettivo di voler “rafforzare la tutela dei diritti fondamentali alla luce dell’evoluzione della società, del progresso sociale e degli sviluppi scientifici e tecnologici”, confermando il principio secondo il quale “il godimento di questi diritti fa sorgere responsabilità e doveri nei confronti degli altri come pure della comunità umana e delle generazioni future”».

²⁶ V., N. F. FRATTARI, *Robotica e responsabilità da algoritmo. il processo di produzione dell’intelligenza artificiale*, *Contr. Impr.*, 1, 2020, p. 458 e ss., ove si legge che «Oggi, infatti, un sistema informatico intelligente può essere progettato per interagire fisicamente con il mondo esterno. Ed è proprio tale facoltà che esprime la portata rivoluzionaria dell’innovazione robotica. Sebbene al pari dei vecchi sistemi intelligenti, il loro funzionamento sia garantito dal flusso di dati e dal ricorso alla rete, i nuovi sistemi AI sono ideati per agire “materialmente” nella realtà esterna. Tale capacità si traduce, a sua volta, nella possibilità di arrecare danni alle persone e ai loro beni con più frequenza di quanto non avvenga per gli altri strumenti informatici. I robot, dunque, attraverso l’acquisita “corporeità”, combinano per la prima volta e in maniera continuativa – quale ne fosse un tratto indispensabile – lo scambio e l’elaborazione di data e la capacità di arrecare lesioni fisiche. [...] A fronte degli enormi progressi compiuti in campo tecnologico ed informatico, la creazione di macchine intelligenti in grado autoprogrammarsi non sembra essere un traguardo così lontano. Seppur in una prospettiva meramente futuribile, l’idea di un robot avulso dal controllo dei soggetti che lo producono o lo utilizzano non può più essere considerata un’utopia. [...] la Risoluzione del Parlamento europeo del 2017 [...] [f]ornsce, quindi, una definizione del concetto di “autonomia”, identificandola con la “capacità di prendere decisioni e metterle in atto nel mondo esterno, indipendentemente da un controllo o un’influenza esterna”. Il livello

di autonomia, poi, varierebbe in base al “grado di complessità con cui è stata progettata l’interazione di un robot con l’ambiente”». Sui livelli di autonomia l’A. afferma che «La terza categoria, infine, comprende quelle intelligenze artificiali in grado di autoprogrammarsi; si tratta di quelle ipotesi classificate come “autonomia forte”. A sua volta, all’interno di questo gruppo, è possibile distinguere due varianti: quella “chiusa”, nel senso che l’“autoprogrammazione” è prevista e calcolata nei suoi sviluppi evolutivi; e quella “aperta” che prevede l’installazione di un algoritmo *self-learning* che consente al robot di apprendere dalla propria esperienza in maniera incontrollata e imprevedibile. In relazione a simili ipotesi si parla generalmente di “autonomia totale”». Sul piano della responsabilità connessa all’agire dei robot, l’A., in conseguenza ai livelli di responsabilità afferma che la «Problematica [è] destinata quindi ad accentuarsi in maniera esponenziale nel caso di algoritmo *self-learnig*, inteso quale massima espressione della c.d. autonomia “forte”: non solo il produttore sarebbe tenuto a testare ogni linea di codice, ma anche a programmarle delle aggiuntive, in relazione a ciascuno dei possibili scenari ottenibili a seguito dell’operatività di quelle originarie. I principi di equità e di ragionevolezza inducono a ritenere che un simile onere non sia imponibile: pretendere l’eshaustività delle procedure di controllo risulterebbe eccessivamente costoso (sia costi strettamente legati all’espletamento della procedura, sia correlati ai tempi, inevitabilmente lunghissimi, per il suo completo esaurimento) e in termini sociali (si pensi ai benefici dello sviluppo tecnologico). Del resto, è già da tempo assodato – anche a livello legislativo – come l’obbligo di garantire la totale assenza di rischi non gravi nemmeno sul produttore di beni “tradizionali”».

²⁷ A. GORASSINI, *Il valore della cultura giuridica nell’era digitale*, in *Tecnologie e diritto*, 2, 2021, p. 48: «[...] ma ciò fondandosi sempre su una forte differenza tra soggettività della A.I. e il valore della persona umana/soggetto. Il valore della persona passa per la carne, il volto in cui si evidenzia la fragilità e la sofferenza delle scelte, non la meccanicità degli algoritmi».

²⁸ V. A. VITERBO E A. CODIGNOLA, *L’intelligenza artificiale e le sue origini culturali*, in *Giur. it.*, 2004, 7, p. 1541 e ss.: «Turing esaminava l’ipotesi dell’intelligenza meccanica in termini parabiologici e prevedeva che la futura calcolatrice sarebbe stata autonomamente in grado di elaborare programmi, di progettare miglioramenti alla propria struttura e di raccogliere dati. La realizzazione di questa ipotesi è sotto i nostri occhi: di anno in anno la potenza dei *computer* è raddoppiata ogni diciotto mesi come previsto dalla legge che Gordon Moore formulò nel

1965; la struttura dei *computer* sta per passare ad utilizzare *chip* quantitativi, *chip* biologici; si progettano e si realizzano *computer* autoesperti capaci di raccogliere informazioni e anche capaci di apportare modificazioni migliorative alle loro architetture. Sembra così dimostrata dai fatti l'ipotesi di Turing a proposito dello sviluppo dell'Intelligenza Artificiale, che avrebbe seguito un percorso di tipo biologico aumentando progressivamente la propria cultura. [...] Ovverosia, come avviene per la maggioranza degli uomini, queste macchine del primo ordine non avrebbero prodotto nuova conoscenza, ogni «idea che si presenti ad una mente di questo tipo farà nascere in risposta in media meno di un'idea». È ciò che avviene alla popolazione mondiale nella sua grande maggioranza, osservava Turing. Invece altre apparecchiature elettroniche più potenti e costruite con un'apposita architettura complessa, avrebbero operato come menti poste «sopra il livello critico». Per Turing «un'idea che si presenti a una di queste menti può far nascere un'intera teoria fatta di idee del secondo ordine, del terzo o di ordini maggiori e remoti», così come avviene agli scienziati, ai ricercatori, agli sperimentatori.»

²⁹ V., G. COMANDÈ, *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in *An. Giur. Econ.* 1, 2019, p. 169 e ss.: «Secondo tale ricostruzione alcuni fattori particolari delle IA determinerebbero il verificarsi di un danno attribuibile all'operato dell'IA non agevolmente riconducibili alle regole tradizionali: i) l'obiettivo dell'IA di preservare se stessa al fine di massimizzare la soddisfazione dei suoi attuali obiettivi finali; ii) l'obiettivo dell'IA di preservare il contenuto dei suoi attuali obiettivi finali; altrimenti, se il contenuto dei suoi obiettivi finali viene modificato, l'obiettivo finale non sarà soddisfatto; iii) l'obiettivo dell'IA di migliorare la propria razionalità e intelligenza per migliorare il proprio processo decisionale, permettendogli di massimizzare la soddisfazione degli attuali obiettivi finali; iv) l'obiettivo dell'IA di acquisire quante più risorse possibili, in modo che queste risorse possano essere trasformate e messe al lavoro per la soddisfazione degli obiettivi finali dell'IA. Sono tutte caratteristiche inerenti ad agenti intelligenti e finalizzate alla massimizzazione crescente di efficienza ed efficacia, ma non valori assoluti neppure in una logica di mera programmazione delle IA. Da questa descrizione emerge una immagine dell'IA in termini psicopatologici. In altri termini, il problema (l'unico problema forse interamente originale nella dinamica r.c.-IA) dell'IA e di

una sua eventuale pericolosità sarebbe da ricondurre ad una sua intrinseca monomaniacalità verso i propri obiettivi. Tale profilo è certamente interessante ma riguarda le ipotesi per così dire estreme e che richiedono una connessione operativa con l'ambiente esterno alla IA. Questo profilo è legato al dibattito sulla utilità/necessità di riconoscere, a fini di r.c., personalità giuridica ad alcune intelligenze artificiali».

³⁰ Affronta il tema, sebbene in una differente prospettiva. R. MESSINETTI, *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contr. Impr.*, 3, 2019, p. 861 e ss., ove si legge che «Larga parte della letteratura di Computer Science ritiene che la logica che governa i processi automatizzati nei sistemi Machine Learning non sarebbe attualmente conoscibile proprio relativamente alla fase – cruciale nella prospettiva del GDPR – della costruzione degli outputs. Resterebbe incognito, specificamente, l'algoritmo “in azione”; il suo funzionamento nell'elaborazione dei nuovi dati (personali) e quindi nella costruzione delle “risposte” che il sistema intelligente restituisce all'ambiente esterno. [...] Siffatta impossibilità epistemica avrebbe la sua ragione nel *proprium* dei sistemi ML applicati all'IA: l'apprendimento autonomo. Si osserva, infatti, che in questi sistemi la logica del processo computazionale non sarebbe stabilita ex ante ma verrebbe coniata in itinere, dalle dinamiche peculiari dell'apprendimento concretamente realizzato; non sarebbe, cioè, predeterminata (dall'uomo) bensì verrebbe auto-definita (dal sistema) a mano a mano che il sistema apprende; ciò che, per definizione, avviene secondo modalità che non sono pre-configurate in virtù della programmazione, non risultando incluse in modo intelligibile nei suoi codici. Il limite cognitivo conseguente sarebbe insensibile alle scansioni cronologiche del processo automatizzato e, in questo senso, opererebbe come limite “assoluto”: la logica effettivamente utilizzata dal sistema non soltanto non sarebbe esaustivamente rappresentabile ex ante, attesa l'imprevedibilità degli effetti computazionali dell'apprendimento autonomo, ma resterebbe incognita anche ex post per una ragione pratica: i sistemi ML e i c.d. *explanatory tools* a disposizione degli utilizzatori sarebbero stati sinora progettati non per fornire spiegazioni nel senso atteso dal GDPR ma per finalità affatto diverse, preordinate all'efficienza dei sistemi; in primis, curare l'affidabilità delle valutazioni predittive». L'Autrice prosegue con il criticare l'impostazione secondo la quale l'identità personale «computazionale» non sarebbe spiegabile e conoscibile dal suo stesso titolare; prosegue nella critica quando afferma che «In tale ipotesi, dal punto di vista dell'individuo soggetto al potere decisionale altrui, la “fede” nelle capacità cognitive e predittive dell'intelligenza artificiale avrebbe sostituito (e obliterato) l'intelli-

genza umana del “come” e del “perché” delle decisioni che lo riguardano. La questione intercetta un nodo cruciale del mutamento che sarebbe implicato dal governo statistico della realtà: il costo dell’efficienza del sistema è la nuova vulnerabilità della persona digitalizzata».

³¹ È il pensiero di U. RUFFOLO, *Intelligenza Artificiale, machine learning e responsabilità da algoritmo*, in *Giur. It.*, 2019, p. 1703: «Non è, in altri termini, indispensabile la transizione da bene a persona (non lo era neppure per lo schiavo quando dotato di un qualche “*peculio*”). Si può essere “responsabili”, e titolari di risorse patrimoniali, anche senza avere personalità giuridica, e comunque senza dover necessariamente ricevere la equiparazione allo *status* della persona umana. E si può essere responsabili anche quando si sia enti ai quali sia irriferribile il concetto di “colpa”, essendo questa (non solo sempre più oggettiva, ma) ormai ridotta ad uno tra i tanti criteri di attribuzione della responsabilità; e non l’unico, e neppure il preminente. [...] Sono, questi, problemi tutti ancora lontani, e oggi solo astratti e logici, anche prescindendo dai quali va comunque sempre ricordato che lo status di persona è presupposto indefettibile per il riconoscimento soltanto di (particolari) diritti, e non anche di responsabilità; ed ancor meno di responsabilità patrimoniali». L’equivoco, ivi non condiviso, è la sovrapposizione tra soggettività e persona: «Tali problemi etici, tradotti sul piano giuridico, possono evolvere nel riconoscimento di diritti, o comunque di protezioni, sulla base della sensibilità etica della società civile che supporta l’ordinamento. Come è avvenuto per la liberazione degli schiavi, o per il (non immediato) riconoscimento dello *status* di persona umana agli abitanti del nuovo mondo (senza contare il crollo solo relativamente recente degli odiosi e discriminanti steccati delle varie forme di *apartheid*); come, in misura diversa e minore, va accadendo con riferimento al riconoscimento di “diritti” o protezioni per gli animali “senzienti”. Con la peculiarità che, nel settore dell’intelligenza artificiale, corpo-macchina e “cervello”, a differenza (fino ad oggi) che per l’uomo e per gli altri esseri “viventi”, sono per il robot interamente separabili; con ogni conseguenza sull’attribuzione e sull’ambito dei “diritti”, se e quando ad una qualche intelligenza non umana sarà accordato lo *status* di persona, o quantomeno il riconoscimento di diritti o protezioni in quanto “pensante”».

³² Scrive R. PICARO, *Relazioni consumeristiche, intelligenza artificiale e nuove identità*, in *Rass. dir. civ.*, 4, 2020, p. 1485 e ss., che «[...] la soggettività non coincide con la personalità, poiché quest’ultima richiama “valore obiettivo, interesse, bene giuridicamente rilevante”. Per questa strada, risulta corroborata la constatazione che, in quanto espressioni del sistema biochimico dell’uomo, l’agire morale così come l’intenzionalità intrinseca sono ontologicamente umani e non

sono sussumibili nei processi di apprendimento di sistemi cognitivi strutturati da algoritmi o da intelligenze artificiali». L'A. prosegue con l'affermare che il tema della soggettività dell'intelligenza artificiale necessita di sviluppi «che siano funzionali alla piena realizzazione della persona umana». Sulla stessa linea di pensiero l'A. afferma che «le numerose riflessioni esplicitate in argomento inducono a insistere sulla dirimente diversità identitaria e giuridica di un'ipotetica soggettività giuridica digitale rispetto a quella della persona umana, che prescinde da ogni elemento di comparazione, ancorché in *minus*. Il presupposto indefettibile da cui muovere è rinvenibile nella necessità di distinguere la personalità, [...], che è presente anche là dove la capacità giuridica viene a mancare o non è ancora presente, dalla capacità giuridica, intesa quale meccanismo neutro atto ad esplicitare l'astratta idoneità alla titolarità oppure all'imputazione di situazioni giuridiche». E, ancora, «quale centro autonomo di imputazione, l'agente digitale può diventare titolare di svariate situazioni giuridiche del diritto privato nei limiti determinati dalla congruità rispetto alle funzioni specifiche che risultano ad esso in concreto assegnate. Non si tratta, dunque, di attendere che l'agente digitale sia in grado di realizzare un interesse proprio, per poter "discorrere di soggettività piena", dal momento che esso esiste unicamente in quanto sinolo funzionale al soddisfacimento di bisogni umani. Soltanto in questo modo si potrà evitare che la macchina, protesi dell'uomo, trasformi l'essere umano in una sua protesi». Per quanto la disposizione assiologica del pensiero dell'A. sia condivisibile, essa troverà pieno rispetto se si tiene distinto il concetto di persona (e personalità) da quello di soggetto, ipotesi, questa, sostenuta nel testo. I rispettivi fondamenti giuridici non sono sovrapponibili, sebbene, lo strumentario concepito per il soggetto giuridico possa trovare anche utili applicazioni alla persona. L'attante che agisce con autodeterminazione diviene portatore di un proprio interesse che l'ordinamento gli affida, se meritevole di tutela; ciò non è bastevole per assimilarlo alla persona, la cui tutela precede l'interesse protetto. Tale differenza ha riflessi sui temi della responsabilità che nel testo si prova ad affrontare.

³³ Per la soggettivazione dell'AI, v., G. TADDEI ELMI, *I diritti dell'intelligenza artificiale, tra soggettività e valore: fantadiritto o jus condendum?*, in *Il meritevole di tutela. Studi per una ricerca coordinata da L. Lombardi Vallauri*, Milano, 1990, p. 687 e ss.; G. SARTOR, *L'intenzionalità dei sistemi informatici e il diritto*, in *Riv. trim. dir. proc. civ.*, 2003, p. 23 e ss.; *Id.*, *Gli agenti software: nuovi soggetti del ciberdiritto?*, in *Contr. e impr.*, 2002, p. 465 e ss.); G. TEUBNER, *Rights of Non-Humans? Electronic Agents and Animals as New Actors*, in *Politics and Law*, 2006, p. 498 e ss.; E. Palmérini, *Robotica e diritto: suggestioni, intersezioni, sviluppi a margine di una ricerca europea*, in *Resp. civ. prev.*, 6, 2016, p. 1826 e ss.

³⁴ U. RUFFOLO, *Intelligenza Artificiale, machine learning e responsabilità da algoritmo*, cit., p. 1698, «Le responsabilità sia del produttore di un bene che la incorpori, sia (ove non coincidente) dell'autore dell'algoritmo che conferisce alla macchina la capacità di apprendere, sembrano – abbiamo visto *retro* – regolabili invocando la disciplina in materia di danno tanto da prodotto che da attività pericolosa. Mentre le responsabilità di chi “addestra” una entità artificiale intelligente, o comunque la espone ad “esperienze” che ne mutano la “*mentalité*”, sembrano poter essere regolabili mediante il ricorso all'art. 2051 c.c. e – quando ve ne siano i presupposti – all'art. 2050 c.c.».

³⁵ V., A. VITERBO E A. CODIGNOLA, *L'intelligenza artificiale e le sue origini culturali*, cit., ove si legge: «Taluni studiosi si soffermano sui limiti dell'AI, enfatizzando il fatto che l'automa non ha coscienza di sé e non è capace di formulare pensiero creativo, artistico e di avere intuizioni, associazioni, illuminazioni mentali. Questi studiosi (così, tra altri, Roger Penrose in *La mente nuova dell'imperatore*) sostengono che molti caratteri legati alla filogenesi, e quindi dovuti alla storia evolutiva dell'uomo, non vengono trasferiti all' AI e non lo potranno mai. Questi studiosi affermano che la mente umana col suo pensare anche intuitivo, con la sua autoconsapevolezza, con la sua efficacia in termini di creatività e progettualità, con i suoi istinti e le sue profonde pulsioni, non è eguale alla intelligenza logica, ordinatrice e calcolatrice delle macchine. E questo è certamente vero, ma nulla toglie al fatto che l'uomo sia riuscito nella straordinaria opera di esternalizzare i propri algoritmi, le proprie fondamentali strutture mentali logico-matematiche. Una cosa è la razionalità e un'altra è il complesso filogenetico proprio dell'uomo costituito dalla sua mente, dalla sua coscienza di sé e dalla sua istintualità ed emotività ed anche dalla sua capacità di essere morale: un complesso che caratterizza l'essere umano in un modo peculiare, ma nel quale l'intelligenza logico-matematica è una parte rilevante».

³⁶ V. P. PERLINGIERI, *Sul trattamento algoritmico dei dati*, in *Tecnologie e diritto*, 1, 2020, p. 184: «La macchina cataloga utilizzando un arbitrio classificatorio; calcola mediante misurazione aritmetica; commisura –o pretende di commisurare- anche le stesse qualità secondo misurazione geometrica o topologica, con criteri di pura quantificazione, in una sorta di ossessiva ripetizione che cancella ogni valore ed ogni interiorità. Il risultato è la perdita di “buon sen-

so” inteso come percezione di “ciò che è irragionevole, disumano, comico, assurdo”. Così la macchina, protesi dell’umano, tende a trasformare l’essere umano in una sua protesi».

³⁷ G. PERLINGIERI, *Profili applicativi della ragionevolezza nel diritto civile*, in *Cultura giuridica e rapporti civili*, 14, Napoli, 2015, p. 142: «Bilanciamento degli interessi e dei valori, ragionevolezza, adeguatezza, proporzionalità, valenza dei principi sono canoni ermeneutici, parti essenziali del bagaglio culturale di qualsiasi interprete e, come tali, contribuiscono [insieme] al ridimensionamento dei vecchi broccardi duri a morire, come in *claris non fit interpretatio* e *dura lex sed lex*, con una rinnovata attenzione verso le conseguenze pratiche della decisione che dovranno non soltanto non essere assurde (poiché l’argomento apagogico è in ogni caso tra gli argomenti dell’interpretazione giuridica), ma conformi alla legalità costituzionale».

³⁸ V. G. COMANDÈ, *Intelligenza artificiale e responsabilità tra liability e accountability*, cit., p. 181 e s., «Algoritmi addestrati in ambienti ad elevata capacità e risorse possono imparare a preferire trattamenti che in realtà sono i trattamenti migliori solo se eseguiti in quegli stessi ambienti ad elevate risorse. Quando questi algoritmi vengono applicati in scenari con risorse inferiori, possono risultare in un’assistenza di qualità inferiore, e quel calo in qualità può essere difficile da osservare e correggere. E questo porta a problemi di responsabilità civile e di definizione degli standard di diligenza, per esempio. Proviamo ad illustrare il problema. Il cancro alla cistifellea e la colecistite mostrano una differenza enorme nella scelta ottimale del trattamento basata sulle risorse del *setting* medico. Il primo è estremamente raro ma estremamente aggressivo; se si metastatizza oltre la cistifellea le speranze di vita del paziente sono alquanto basse. La colecistite, assai comune, è trattata con un intervento chirurgico tecnicamente semplice in cui il chirurgo laparoscopicamente rimuove la cistifellea infiammata. Ove però un paziente si presenti a un medico con quella che sembra essere colecistite, ma in realtà è un cancro alla cistifellea il chirurgo deve notare – nel mezzo della chirurgia laparoscopica – i segni di un probabile cancro e poi decidere – sempre a metà dell’intervento chirurgico – se provare a rimuovere il cancro o fermare l’intervento chirurgico e inviare il paziente ad un ospedale con maggiori risorse. La scelta di proseguire nella rimozione del cancro richiede molta più abilità da parte del chirurgo, strumenti operativi diversi e più specializzati, maggiore tempo operatorio. Se eseguito correttamente, il paziente avrà avuto il trattamento oncologico più appropriato al momento della (sospetta) diagnosi e con le migliori aspettative di sopravvivenza a lungo termine. [...] Dunque proseguire l’operazione può essere l’opzione giusta in un ambiente con chirurghi adde-

strati e attrezzature migliori, ma può essere quella peggiore nelle strutture senza queste risorse. Pare ovvio che se la decisione è assistita da una IA che suggerisca il percorso ritenuto migliore si potrebbe facilmente fare la scelta sbagliata se l'IA è addestrata solo in ambienti con chirurghi altamente qualificati. E i chirurghi operanti in strutture meno qualificate potrebbero rimanere «succubi» delle proposte dell'IA».

³⁹ G. GITTI, *Tecnologie digitali, persona e istituzioni*, cit., p. 1234 e s., delinea la questione e traccia la differenza con la decisione umana ove si legge: «La decisione robotica, insomma, è una super-decisione, poiché avviene a seguito dello svolgimento di procedure che non sono percorribili dalla mente umana, la quale, com'è ovvio, costituisce il paradigma dell'agente decisore nel diritto dei contratti. Super-decisione perché il robot è dotato di una capacità computazionale a noi preclusa [...], il robot è in grado di organizzare e processare i dati raccolti e combinati, fornendo un *output* in tempi pressoché istantanei».

⁴⁰ V., P. PERLINGIERI, *Sul trattamento algoritmico dei dati*, in *Tecnologie e diritto*, 1, 2020, p. 191, ove scrive «Il pensiero, imprigionato in un circuito chiuso, è ingessato nella sua finitezza computazionale, nell'illusione che dalla accresciuta conoscenza tecnologica scaturisca un'accresciuta coscienza morale, una "mistica della neutralità"».

⁴¹ Questa differenza trova riscontro nei cinque livelli di automazione che la *Society Automotive Engineers International* ha definito con riguardo agli autoveicoli, v. M. TAMPIERI, *L'intelligenza artificiale: una nuova sfida anche per le automobili*, in *Contr. Impr.*, 2, 2020, p. 732 e ss., ove si legge: «I successivi livelli di automazione dei veicoli si distinguono nel livello 3 (settore denominato *Conditional Automated Driving Functionalities*), ove il software ha il pieno controllo dell'ambiente di guida e ne svolge tutte le funzioni, ma spetta al conducente la sorveglianza sul corretto funzionamento del sistema e il tempestivo intervento, ogni qual volta lo scenario prefigurato nella mappatura si modifichi e renda necessarie determinate operazioni. Si tratta dei veicoli *self-driving* che offrono una guida integrativa, ma che richiedono al conducente una diligenza sostanzialmente simile alla guida manuale: il conducente deve infatti rimanere vigile e riprendere il controllo del mezzo quando ciò si renda necessario. In questo tipo di veicoli che presuppongono un'interazione con il pilota riveste fondamentale importanza fornire a quest'ultimo informazioni dettagliate, chiare, e facilmente comprensibili anche per utenti non esperti. Giova rilevare che tra il livello 2 e il livello 3 esiste una notevole differenza, non solo dal punto di vista ingegneristico: mentre al livello 2 il soggetto che monitora le condizioni di guida rimane il guidatore-persona, nel livello 3 il sistema è capace di operare tale valutazione in forma autonoma. Una guida sostitutiva è propria dei veicoli *driverless*, la cui circolazio-

ne richiederà comunque notevoli cautele. Questi veicoli hanno un livello 4 di *high automation*, ove il controllo del pilota è più ridotto, e la sua presenza è utile (anche) per fornire al sistema parametri quali la destinazione e la velocità massima. In questi mezzi la presenza a bordo di strumenti di guida si giustifica per le seguenti ragioni: la volontà del pilota di dedicarsi personalmente alla guida, oppure in presenza di condizioni (anche non segnalate dalla macchina) che rendono impossibile la guida automatizzata. È previsto inoltre un livello 5 di *full automation* in cui il sistema si sostituisce al guidatore al quale pertanto non solo è consentito di estraniarsi dal controllo del mezzo, ma è escluso ogni suo intervento: sono infatti auto prive dei classici strumenti di guida. [...] Giova richiamare la riforma tedesca sul traffico stradale: *Straßenverkehrsgesetz* (StVG) del 16 giugno 2017, diretta a dare impulso al trasporto automatizzato, e a regolare la circolazione dei veicoli dotati di sistemi di guida molto o del tutto automatizzata, ossia veicoli che, con l'attivazione del sistema, sono in grado di controllare la guida, di rispondere alle prescrizioni del traffico, e di segnalare tempestivamente al conducente l'esigenza della guida manuale. Quest'ultimo deve quindi intervenire se il sistema lo richiede, o se vengono a mancare i presupposti (per un uso conforme alle regole) delle funzioni di guida automatizzata. In altri termini, il pilota deve mantenere una soglia di attenzione che gli permetta di assumere tempestivamente il controllo del veicolo quando vengono meno le condizioni che permettono un utilizzo sicuro della guida automatica. Si aggiunga che la nuova disciplina dedica un'apposita sezione all'elaborazione dei dati nel veicolo. Inoltre, in caso di sinistro provocato da un errore del software è previsto l'obbligo risarcitorio a carico del proprietario del mezzo. Secondo un condivisibile orientamento dottrinale, si tratta di una scelta "che lascia invero insoddisfatti, a fronte della constatazione che il proprietario del veicolo si trova a svolgere il ruolo di 'capro espiatorio' in caso di malfunzionamento di un sistema sul quale egli non ha alcuna influenza"».

⁴² V., P. PERLINGIERI, *Il diritto civile nella legalità costituzionale*, cit., II, *Fonti e interpretazioni*, p. 455, «La valutazione quantitativa delle probabilità non è da confondere con il tema della decisione robotica e del suo rapporto con la discrezionalità dell'interprete. La prima è questione di natura essenzialmente matematica, che è utilizzabile nelle valutazioni prognostiche; la seconda, invece, coinvolge necessariamente una possibilità di scelta tra alternative nel rispetto dei parametri ermeneutici e quindi di un corretto e persuasivo uso dell'argomentazione sulla base di fondamenti logici, teologici e assiologici rinvenibili nel sistema ordinamentale auto ed etero-integrato».

⁴³ Sul punto chiarificatrici le parole di A. GORASSINI, *Il valore della cultura giuridica nell'era digitale*, in *Tecnologie e diritto*, cit., p. 45: «Per quanto si provi a

dare una risposta a tutto, non si possono spiegare deterministicamente i fenomeni biologici (non solo umani), e resterà sempre fuori dalla scienza l'aspetto umano che è rappresentato dall'intuito, non raggiungibile dagli algoritmi. Malgrado le ottimistiche previsioni di costruzioni di reti antagonistico-generative e *disentanglement*, "una macchina dotata di coscienza sembra ancora lontana", anche perché non si sa bene cosa sia la coscienza dell'uomo. Il mistero umano resiste alla ricerca di comprensione della creatività: noi siamo il risultato di una serie di imperfezioni che hanno avuto successo».

⁴⁴ Scrivono A. VITERBO E A. CODIGNOLA, *L'intelligenza artificiale e le sue origini culturali*, cit., «Turing ha potuto realizzare l'AI sia perché la scienza logico-matematica si è adeguatamente sviluppata, sia perché nella coscienza collettiva della modernità si è fatto strada il convincimento della profonda complessità del reale, insieme col convincimento che la stessa mente umana è un prodotto di questa complessità, conoscibile soltanto in misura relativa. [...] Dunque con Gödel il pensiero logico-matematico nel suo progredire verso l'AI assume il paradigma della complessità, arricchendosi della dinamica complessa, prospettica ed evolutiva propria della mente umana, attraendo all'interno della logica formale il dubbio metodologico necessario per elaborare una gerarchia infinita di algoritmi per comprendere un mondo profondo, infinito ed in perenne modificazione nello spazio-tempo. [...] La logica matematica indicava così essa stessa, con Gödel, l'esistenza di un confinamento invalicabile: la macchina universale col suo calcolo raziocinante non appariva più concepibile perché essa, se fosse stata costruita, avrebbe potuto non dare risposte ovvero avrebbe dato risposte valide soltanto relativamente al sistema adottato e a suoi assiomi di base. [...] Infatti, secondo Turing la macchina calcolatrice duplicava, esternalizzava il modo di funzionare della mente umana e la stessa cultura matematica aveva dimostrato l'incompletezza e la fallibilità della logica umana e, quindi, anche di tale macchina. Per altro se la macchina calcolatrice, osservava Turing, fosse stata infallibile non sarebbe stata capace di imparare sbagliando e, perciò, non sarebbe stata definibile intelligente. Turing invocava *fair play* nei confronti delle macchine, osservando come ogni matematico umano si formi dopo una prolungata fase di apprendistato e che, quindi, anche alla macchina doveva essere concessa la facoltà dell'errore. Quello che

realmente importava era il fatto che la macchina fosse perfezionabile, fosse in grado, cioè, di migliorare progressivamente così come impara, crescendo, un bambino. Coerentemente Turing riteneva che così come la mente dell'uomo è un sistema complesso fatto di elementi fisico-chimici, di impulsi elettrici e di programmi elaborativi, così la macchina universale sarebbe stata un sistema complesso evolutivo fatto di *hardware*, di *software*, di estesa memoria e di grande forza elaborativa, un tutt'uno ove l'insieme non sarebbe stato divisibile e riducibile ai suoi componenti, ma sarebbe consistito nell'essere un processo, elaborativo e cognitivo. [...]».

⁴⁵ V., M. MASSIMINI, G. TONONI, *Nulla di più grande. Dalla veglia al sonno, dal coma al sogno. Il segreto della coscienza e della sua misura*, ed. kindle, Milano, 2013, «Se, secondo la teoria, il livello di complessità/coscienza è una quantità esprimibile con un numero (bit di informazioni integrata), ne consegue che qualsiasi insieme di neuroni potrebbe avere un certo grado di complessità. Persino il cervelletto, il midollo spinale e un verme potrebbero averne un po', magari pochissima; ma pur sempre di informazione integrata si tratterebbe. E, andando oltre, qualsiasi pezzo di materia, vivente o non vivente, avrebbe la sua piccola dose di Φ , purché si possa riscontrare una benché minima capacità delle sue parti di integrare l'una con l'altra in modo causale. In sintesi, se la teoria è corretta, e se la complessità è un *continuum*, si dovrebbe derivare che anche la coscienza è graduale. In effetti è difficile credere che il confine tra coscienza e incoscienza sia assolutamente netto [...] verosimilmente la costruzione della complessità è un processo lungo che inizia in utero, con la progressiva differenziazione di un abbozzo di sistema nervoso, dove i neuroni diventano gradualmente più selettivi e più connessi. Anche quando ci risvegliamo dal sonno la coscienza riappare gradualmente [...] Dire che la coscienza è graduale, che non esiste la soglia tutto o nulla proposta da Cartesio non significa sposare il pansichismo di Montaigne e non equivale ad affermare che la coscienza è distribuita dappertutto in egual misura, tra gli atomi le singole cellule, i vermi e i diversi sistemi nervosi che popolano il pianeta».

⁴⁶ *Ibidem*, «In conclusione, non abbiamo ancora idea di come il grafico della distribuzione della coscienza nel mondo debba essere disegnato. Ma, fino a quando la teoria non sarà confutata dal prossimo esperimento, possiamo supporre che questo grafico non rappresenterà tutto o nulla, come quella tracciata da Cartesio, e neppure la distribuzione egualitaria proposta da Montaigne. È probabile che il mondo sia popolato da una maggioranza di oggetti, grandi e piccoli, che sono unitari solo in apparenza, oggetti che si polverizzano in una

miriade di moduli indipendenti, o debolmente connessi, per cui l'informazione integrata è trascurabile dal punto di vista dell'esperienza soggettiva. Tra questi ci sono sicuramente il cervelletto e i nuclei della base, le reti internet, i supercalcolatori attuali, le telecamere e, forse, il cervello di qualche animale. Poi, è possibile che su questo sfondo si staglino qua e là dei picchi, dei valori talmente alti che la scala delle ordinate dovrebbe essere, come minimo, logaritmica. Per quanto ne sappiamo, questi massimi locali d'informazione integrata dovrebbero corrispondere ai sistemi talamocorticali, nuclei unitari d'informazione irriducibile [...] possiamo già affermare con cognizione di causa che cani, gatti, scimmie e delfini posseggono un sistema talamocorticale neuroanatomicamente molto simile al nostro. Possiamo dunque inferire che, se il sistema talamocorticale umano è in grado di ospitare un complesso cosciente, anche il sistema talamocorticale di un gatto, di un cane o di una scimmia dovrebbero fare lo stesso, anche se presumibilmente con valori di Φ più bassi. E non importa se il linguaggio è assente o alcuni di questi animali non sono in grado di riconoscersi allo specchio per denunciare il privilegio dell'autocoscienza». Queste considerazioni valgono anche a differenziare le coscienze umane per via del livello di complessità soggettiva delle connessioni integrative di informazioni.

⁴⁷ Scrive A. ALPINI, *Identità, creatività e condizione umana nell'era digitale*, in *Tecnologie e diritto*, 1, 2020, p. 6: «L'uomo è molto più dei suoi dati personali. L'identità personale non si esaurisce nell'identità digitale: quest'ultima è pur sempre una parte della identità personale che è mutabile, indisponibile e inviolabile. Se, infatti, l'identità personale fosse immutabile, la personalità umana non potrebbe svilupparsi liberamente, verrebbe privata del suo potenziale, si negherebbero l'originalità della natura umana e la sua dignità che, com'è ovvio, non costituisce un principio a se stante, bensì un tutt'uno con la persona umana».

⁴⁸ Cfr., G. ALPA, *I diritti fondamentali e il ruolo dell'Avvocatura*, in *Il controllo di legittimità costituzionale e comunitaria come tecnica di difesa. Corte Costituzionale italiana e spagnola a confronto*, a cura di L. Mezzasoma, V. Rizzo, L. Ruggeri, Camerino-Napoli, 2010, p. 64, che sottolinea: «i diritti fondamentali non sono la cifra del livello di democrazia di una società ma l'essenza stessa della democrazia» e p. 65, «il fatto che si parli di diritti "umani", di diritti "dell'uomo", di diritti fondamentali, non muta il loro significato intrinseco né l'impegno delle società moderne nell'offrire loro una garanzia adeguata».

⁴⁹ Scrive N. BOBBIO, *Piero Calamandrei*, in *ID., Etica e politica. Scritti di impegno civile*, 2013, p. 294: «Per chi considera la giustizia come l'ideale del diritto, il *ius quod iussum* non può costituire l'ultima meta. Giurista completo è soltanto co-

lui che non solo interpreta rettamente le leggi vigenti, ma scoprendone i difetti, prepara e promuove il diritto futuro».

⁵⁰ Asserisce R. DWORKIN, *La giustizia in toga*, trad. it. di S. F. Magni, Bari, 2010, p. 184: «Dobbiamo essere in grado di vedere come l'abbracciare una concezione del valore piuttosto che un'altra significhi prendere una decisione piuttosto che un'altra [...]. Dovrebbe essere chiaro quale sia questo valore: è quello della legalità o, come qualche volta è più enfaticamente chiamato, il principio di legalità [*rule of law*]. La legalità è un valore reale, ed è chiaramente un valore giuridico» (corsivo originale). Per una ricostruzione del principio di legalità fondata sui principi nazionali e sovranazionali, P. PERLINGIERI, *Diritto comunitario e legalità costituzionale. Per un sistema italo-comunitario delle fonti*, Napoli, 1992, p. 147. ss.

⁵¹ Vedi, Corte Edu, 13 novembre 2007, n. 15619, A. c. Italia, in *Fam. pers. succ.*, 2008, 6, p. 572 ss., secondo la quale quando un individuo viene privato della libertà, l'utilizzo nei suoi confronti della forza fisica nel momento in cui non è strettamente resa necessaria dal suo comportamento lede la dignità umana e costituisce pertanto una violazione dell'art. 3 della Convenzione europea; vedi, anche, Corte giust., 14 ottobre 2004, C-36/02, Omega Spielhallen e altri c. OberbürgermeisterinderBundesstadt Bonn, in *Corr. giur.*, 4, 2005, p. 486 ss., con nota di R. Conti, *La dignità umana dinanzi alla Corte di Giustizia*, che afferma che il diritto comunitario non osta a che un'attività economica consistente nello sfruttamento commerciale di giochi di simulazione di omicidi sia vietata da un provvedimento nazionale adottato per motivi di salvaguardia dell'ordine pubblico perché tale attività viola la dignità umana, non essendo indispensabile che la misura restrittiva emanata dalle autorità di uno Stato membro corrisponda ad una concezione condivisa da tutti gli Stati membri relativamente alle modalità di tutela del diritto fondamentale; nonché, Corte cost., ord., 16 novembre 2018, n. 207, in *Corr. giur.*, 2019, 4, p. 457 ss., con nota di E. BILOTTI, *Ai confini dell'autodeterminazione terapeutica. Il dialogo tra il legislatore e il giudice delle leggi sulla legittimità dell'assistenza medica al suicidio*, secondo cui il principio del consenso informato in ambito sanitario, che trova fondamento negli artt. 2, 13 e 32 Cost., comprende anche il diritto del paziente capace di rifiutare o interrompere qualsiasi trattamento sanitario, ancorché necessario alla sua sopravvivenza. Neppure il rilievo riconosciuto al valore della vita può pertanto escludere il dovere del personale sanitario di rispettare la decisione del malato di porre fine alla propria esistenza tramite l'interruzione dei trattamenti, anche quando ciò richieda una condotta attiva. Di conseguenza il rilievo riconosciuto al valore della vita neppure può rappresentare un ostacolo assoluto, penalmente presidiato, all'accoglimento della

richiesta del malato di un aiuto a morire, che valga a sottrarlo al decorso più lento, apprezzato come contrario alla propria idea di morte dignitosa, che fa seguito all'interruzione di un presidio di sostegno vitale. Il divieto assoluto di aiuto al suicidio rappresenta pertanto un limite all'autodeterminazione terapeutica del malato affetto da patologia irreversibile, la cui sopravvivenza dipenda da un trattamento sanitario in atto, del quale chieda l'interruzione, con lesione del principio della dignità umana (art. 2 Cost.) e dei principi di ragionevolezza e di uguaglianza in rapporto alle diverse condizioni soggettive (art. 3 Cost.). V., C. Mignone, *Identità della persona e potere di disposizione*, in Pubblicazioni della Scuola di specializzazione in diritto civile dell'Università di Camerino, Napoli-Camerino, 2014, 144, p. 101 ove si legge «Una volta rimosso il velo di maya del “diritto ad essere se stessi”, l'identità rileva meglio la sua vera natura, quella di una componente ineliminabile del fatto da qualificare, che incide sul procedimento di qualificazione introducendo un elemento di differenziazione di cui l'interprete deve tener conto, pena la violazione della gerarchia delle fonti. [...] I limiti del processo di oggettivazione giuridica dell'identità lasciano fatalmente intravedere una costruzione del sé contingente e fluida: mai interamente definita una volta per tutte, che abbraccia la molteplicità delle differenti relazioni che ognuno può intrattenere nella società e la loro naturale variabilità nel tempo». Cfr., anche L. Lonardo, *Il valore della dignità della persona nell'ordinamento italiano*, in *Rass. dir. civ.*, 2011, p. 778 ove si legge: «il funzionamento del nostro ordinamento costituzionale è tutto calibrato sul valore persona umana e quindi della sua dignità di essere umano, non più suddito, ma parte fortemente attiva, protagonista del processo democratico: ed è un aspetto del quale dovrebbero tener conto le proposte di revisione costituzionale prima di procedere a modifiche inerenti ai profili lato sensu procedurali della democrazia» e p. 798: «la dignità in sé [...] non è destinata a cedere in alcuna ipotesi perché sottratta al bilanciamento: essa è elemento di valutazione, proprio in quanto essenza, in quanto qualità, “irriducibilmente” legata alla persona, e non va confusa con gli altri principi insieme ai quali si applica». Altri ragguagli in F. D. Busnelli, *Le alternanti sorti del principio di dignità della persona umana*, in *Riv. dir. civ.*, 2019, p. 1071 ss.

⁵² V., C. PERLINGIERI, *Responsabilità civile e robotica medica*, in *Tecnologie e diritto*, I, 2020, p. 178, ove l'Autrice prefigura il passaggio dal *software* al *wetware*, cioè di un robot «misto in cui il sistema di controllo è di natura organica mentre il sistema di attuazione è meccanico-biologico in misura diversa a seconda delle diverse realizzazioni». L'A. riferisce le evoluzioni scientifiche tese a riprodurre le funzioni mnemoniche dell'ippocampo, il quale trasforma la memoria da breve a lungo termine. Indubbiamente i progressi della scienza sono

destinati a mutare l'apprezzamento valoriale dei robot, sebbene tali sviluppi afferiscono pur sempre ai profili razionali, e non emotivi e volitivi dell'uomo.

⁵³ Scrive P. Perlingieri, *Sul trattamento algoritmico dei dati*, in *Tecnologie e diritto*, cit., p. 186 e s.: «Particolarmente la materia degli algoritmi mostra in modo esemplare la fondatezza della gradualità e della relatività della teoria della soggettività giuridica, nonché l'attualità delle riflessioni che la dottrina germanica contemporanea ha riservato alla c.d. personalità elettronica [...]. Invero la capacità di agire digitale va considerata per le sue peculiarità e finalità e secondo il ruolo che di fatto assume l'intelligenza artificiale che varia dalla sua esclusiva strumentalità da parte dell'uomo alla sua completa autonomia, sia pure associata o integrata con quella dell'uomo in una nuova simbiosi uomo-macchina con reciproci flussi informativi, tale da costituire comunque una propria identità capace di autodeterminarsi, adattandosi alle più varie strategie decisionali. Tant'è che si auspica l'utilizzo, da un punto di vista pratico, di una *black box*, di una scatola nera che consenta di ricostruire il processo decisionale, distinguendo l'errore di calcolo computazionale, tale sin dall'origine, dalla decisione assunta in un contesto –prevedibile in chi lo programma– di incertezza misurato *ex post* nelle sue conseguenze».

⁵⁴ V., C. PERLINGIERI, *Responsabilità civile e robotica medica*, cit., p. 178: «In tali ipotesi, dunque, il legislatore necessariamente dovrà introdurre una nuova e specifica soluzione normativa –sia quella di un'assicurazione obbligatoria, sia quella di un patrimonio dedicato–, accanto alle quali affiancare un fondo nazionale che subentri in loro assenza –che consenta di garantire il risarcimento del danno subito dal paziente operato in autonomia da un robot».

⁵⁵ *Ibidem*, p. 179: «Se, dunque, è crescente l'interazione tra robotica, Intelligenza Artificiale e neuroscienze cognitive tale da incrementare la fusione tra l'umano e l'artificiale, sarà oltremodo sempre più complessa la questione della gestione dell'autonomia decisionale dei nuovi protagonisti della scena giuridica, non più soltanto “agenti software autonomi”, ma anche agenti con un cervello a *wetware* biologico sempre più simili all'uomo».

⁵⁶ Ma pur sempre riconducibile all'autore, poiché lì dove il fatto è del terzo, cioè di un centro di interesse autonomo imputabile ad un soggetto altro, le regole della rappresentanza, del preposto o dell'ausiliario, trovano disciplina nell'art. 1180 c.c., ovvero, nell'art. 1399 c.c. V. R. NICOLÒ, *L'adempimento dell'obbligazione altrui*, Milano 1933, *passim*, ove l'A. distingue l'adempimento dell'obbligazione altrui da quello del terzo. V., Cass., sezione 3, 20 ottobre 2021, n. 29001, ove si legge: «[...] al riguardo questa Corte (Cass., 11 novembre 2019, n.

28987) ha chiarito che la più frequente ricostruzione dell'istituto, oggi peraltro smentita testualmente dal disposto dell'art. 7, comma 1, della legge n. 24 del 2007, sovrappone, erroneamente, la fattispecie di responsabilità diretta per fatto proprio ex art. 1228, cod. civ., dell'ente impersonale (che si serve di ausiliari quale strumento di attuazione dell'obbligazione contrattuale verso il paziente) pur sempre fondata sull'elemento soggettivo dell'ausiliario (il che ne esclude la configurabilità in termini di responsabilità oggettiva, salva un'autonoma responsabilità "organizzativa" della struttura stessa), con la responsabilità indiretta per fatto altrui (concordemente ritenuta di tipo oggettivo) dell'imprenditore per i fatti dei propri dipendenti, disciplinata dall'art. 2049 cod. civ.; si tratta di fattispecie astratte radicalmente differenti per morfologia ed effetti; nel primo caso (art. 1228, cod. civ.) l'attività dell'ausiliario è incardinata nel programma obbligatorio originario che è diretto a realizzare, e per la cui realizzazione il debitore contrattuale si è necessariamente avvalso dell'incaricato, essendogli preclusa, attesa la natura giuridica di ente, ogni possibilità di adempimento "diretto"; nel secondo caso (art. 2049, cod. civ.), la condotta pregiudizievole non si traduce propriamente nella mancata o inesatta esecuzione di un contenuto obbligatorio del committente verso un creditore, quanto piuttosto nello svolgimento di mansioni dannose per un terzo privo di una pregressa relazione qualificata con il debitore, ferma l'alterità dei soggetti imputabili dell'illecito (il preponente, il preposto): e proprio per ciò si richiede la preposizione e l'occasionalità necessaria (Cass., Sez. U., 16 maggio 2019, n. 13246) per la configurazione di una responsabilità (concordemente ritenuta oggettiva) del "dominus"».

⁵⁷ V., G. COMANDÈ, *Intelligenza artificiale e responsabilità tra liability e accountability*, cit., p. 184: «Qui il problema principale, rilevante sul piano della responsabilità, è il *trade off* tra efficacia di norma della IA, che la rende preferibile, e il rischio in situazioni estreme, che implicherebbe la costante vigilanza di una decisione umana. [...] Ma ancora una volta l'esempio dell'*automation bias* e delle c.d. *bias* di contesto o traslazionali (l'uso di una IA fuori dal contesto di apprendimento originario) mette in luce i limiti di una risposta di r.c. tradizionale. Peraltro, questo risultato può essere più ricorrente se la raccomandazione proviene da una IA che non offra spiegazioni per la sua scelta. E di nuovo ciò ha un effetto sulle regole di responsabilità e sul loro sviluppo».

⁵⁸ G. COMANDÈ, *o.u.c.*, p. 185: «Con *accountability* si allude all'obbligo di chi prenda delle decisioni e operi delle scelte di 1) giustificarle dinanzi a coloro che di tali scelte subiscono gli effetti ed eventualmente 2) debbano, non solo rendere il conto per le scelte fatte, ma debbano anche 3) rispondere nelle sedi opportune (responsabilità politica, civile, penale, amministrativa, deontologi-

ca, sociale) per loro eventuali fallimenti e mancanze. Dunque al suo interno rientra anche la responsabilità civile, nelle sue possibili declinazioni, del produttore/distributore di IA di assistenza diagnostica nelle narrative precedenti, ma ancora una volta a fini di prevenzione e risarcimento ciò non è sufficiente. Come gli esempi illustrati prima indicano, la responsabilità civile potrebbe al massimo riallocare la perdita da lì dove è caduta (il paziente ad esempio) su un altro soggetto (la struttura o il professionista) senza però dare gli incentivi di prevenzione corretti».

⁵⁹ V., M. GAMBINI, *Algoritmi e sicurezza*, in *Giur. It.*, 2019, p. 1726 e ss., ove a proposito del trattamento dei dati ad opera dell'algoritmo afferma «Da tali fenomeni consegue che la quotidianità degli individui viene ad essere permeata da un continuo flusso di dati (anche personali) che può sfociare in forme di illecita manipolazione algoritmica degli stessi: dipendenti dal fatto che i dati di partenza utilizzati nei trattamenti algoritmici possono essere errati, imprecisi o incompleti; e, in modo ancora più preoccupante, dal fatto che gli algoritmi sono creati da decisori umani che, già in fase di progettazione, ne possono influenzare l'analisi e distorcere l'elaborazione, conducendo a risultati lesivi dei diritti e delle libertà individuali. La diffusione dei trattamenti algoritmici non comporta solo la perdita di controllo sui dati personali, ma può influire anche su aspetti ulteriori, che superando il problema della riservatezza, investono la dignità umana, la libertà, l'autonomia e lo sviluppo delle persone, la sicurezza e la loro salute e implicare evidenti rischi di stigmatizzazione e discriminazione degli individui. Si pensi, alla portata di decisioni algoritmiche che impediscono ad un soggetto l'ingresso in uno Stato o l'accesso ad un sussidio o ancora all'erogazione di un servizio essenziale. [...] Ora, al fine di garantire la sicurezza della "società dell'algoritmo", si ritiene auspicabile l'adozione di un analogo approccio, ispirato ai principi di prevenzione e di precauzione, che – in misura ancor più incisiva – centri l'attenzione sulla previsione di un articolato sistema di controlli a carico dei soggetti responsabili della progettazione, programmazione e implementazione degli algoritmi, volti a ridurre i rischi ed evitare gli eventi dannosi per i diritti e le libertà degli individui, prima che ad eventualmente risarcirli. In un'ottica di massima responsabilizzazione delle fasi di ideazione e sviluppo delle applicazioni algoritmiche». L'Autrice avverte l'urgenza di monitorare l'evoluzione attuativa del *software* che, se di autoapprendimento, si sottrae viepiù al controllo umano, né può ritenersi sostenibile una controllabilità diffusa della smisurata quantità di *software* immessi nel mercato.

⁶⁰ C. IORIO, *Intelligenza artificiale e responsabilità: spunti ricostruttivi*, in *Tecnologie e diritto*, 2, 2021, p. 51 e ss., in part. p. 66 e s., critica il ricorso alla sogget-

tivazione dell'AI: lo giudica non conforme al sistema costituzionale di riferimento per la primazia della persona e dei suoi diritti fondamentali; lo ritiene soluzione sovrabbondante giacché il risultato di assicurare al danneggiato la misura risarcitoria può realizzarsi più agevolmente «rimettendosi ad un fondo pubblico l'indennizzo dei danni non imputabili alla produzione di beni *sub standard*». L'obiezione sulla difformità dal sistema costituzionale sarebbe fondata se non si distinguesse il soggetto dalla persona, distinzione di cui si dà premura il presente scritto. L'obiezione della eccedenza dello strumento rispetto allo scopo non considera che la soluzione assicurativa, unita al fondo di garanzia, ivi sostenuta, richiede un soggetto giuridico per consentire con maggiore accessibilità l'eventuale azione di rivalsa del soggetto giuridico obbligato (al risarcimento della parte lesa) nei riguardi degli attori della filiera progettista-produttore-distributore. Anche il fondo pubblico, della cui solvibilità è lecito nutrire qualche dubbio, implicherebbe un centro di interesse autonomo (al pari della soluzione assicurativa) chiamato, nell'attività di gestione, ad esperire azioni di rivalsa con un elevato livello di incertezza sul buon fine delle stesse. Una soggettivazione responsabile e patrimonializzata può contribuire con il premio assicurativo all'equa distribuzione del rischio di danni causati dall'attante macchinico.

⁶¹ C. PERLINGIERI, *Responsabilità civile*, cit., p. 176.

⁶² V., G. F. ITALIANO, *Le sfide interdisciplinari dell'intelligenza artificiale*, in *An. Giur. Ec.*, 1, 2019, p. 9 e ss. ove si legge: «Ma cosa sono gli algoritmi? Semplificando al massimo, potremmo dire che gli algoritmi sono sequenze di istruzioni, linee di codice, che possiamo scrivere e che possiamo leggere. Ad esempio, nel recente scandalo *Dieseldgate*, lo scandalo delle emissioni in cui sono state coinvolte varie case automobilistiche, il problema risiedeva in un'applicazione software, che era in grado di riconoscere se il veicolo fosse sottoposto a un test di omologazione (e di conseguenza di ridurre le emissioni). In quel caso, è stato possibile prendere quel codice software, sezionarlo ed esaminarlo con attenzione, e capire esattamente cosa facesse e perché producesse un certo risultato durante i test di omologazione e un risultato molto diverso durante il normale funzionamento. In modo del tutto trasparente, spiegabile, interpretabile e riproducibile. Gli algoritmi di *machine learning* agiscono in modo diverso dagli algoritmi tradizionali. La differenza principale è che *machine learning* usa del codice per consentire a un sistema automatico di imparare e di creare un modello del problema che bisogna risolvere. Un modello che non è però spesso facilmente interpretabile come le linee di codice degli algoritmi tradizionali. Per fare un esempio molto approssimativo, e forse anche un po' esagerato, potremmo pensare al modello prodotto da un algoritmo di *machine*

learning come a un cervello umano. Non possiamo dissezionare il cervello per capire cosa è successo, perché è stata presa una certa decisione. Possiamo provare a osservare dall'esterno, a fare delle domande, interrogare la persona e analizzare le sue risposte. Ma questo è un processo lungo, non sempre conduce a conclusioni esatte, e non sempre fa capire perché è stata presa una certa decisione. In questo caso, il meccanismo con cui è stata presa una decisione è poco chiaro, poco trasparente e più difficilmente spiegabile. Per questo gli algoritmi di *machine learning* sono come una scatola chiusa, una *black box*, che non può essere aperta molto facilmente. Non è realmente chiaro come fa una macchina a riconoscere le immagini. Si costruisce un suo modello, e ovviamente può anche fare errori. Anche se una macchina può ottenere risultati confrontabili a quelli di un essere umano, il suo modo di operare, la sua logica è completamente diversa da quella di un essere umano. Può riconoscere un'immagine o fare un errore, ma per motivi completamente diversi da quelli di un essere umano».

⁶³ V. GUNTHER TEUBNER, *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, a cura di P. Femia, Napoli, 2019, spec. p. 51 ss. ove si legge «La capacità di pensare o l'intelligenza artificiale sono spesso riproposte in dottrina quali il criterio peculiare, decisivo per l'attribuzione della soggettività giuridica. Ma qui però si deve correggere una rappresentazione sbagliata, piuttosto diffusa. Quando si discorre di capacità di agire [degli algoritmi], non si tratta di rispondere alla domanda su quale genere di qualità ontologiche – intelligenza, spirito, anima, capacità riflessiva, capacità introspettiva – debba possedere un'agente software per poter essere un attore. Anche in questo caso è di aiuto il paradigma delle organizzazioni formali persone giuridiche: affinché sia riconosciuta la capacità di agire di agenti on umani, i processi psicologici interiori non sono determinanti [...] Non le qualità interiori dell'agente, ma le interazioni sociali, cui prendono parte le operazioni correnti dell'algoritmo – e cioè una sequenza chiusa e autonoma di comunicazione ricorsiva – costituiscono l'algoritmo come persona, come artefatto semantico, attore dotato di capacità comunicativa [...] Sembra, dunque, inammissibile sostenere che solo quando l'autonomia digitale si rafforzi sino a divenire autocoscienza siano ravvisabili indici di personalità giuridica. Sono esattamente questi gli interrogativi che si pongono alla filosofia dell'informazione nella ricerca di una possibile moralità digitale. Ma se tali qualità fossero richieste come criteri fondanti l'autonomia della regolazione giuridica della responsabilità da illecito, si finirebbe con il favorire il comportamento opportunistico dei giuristi, che nel tempo presente si adagiano fiduciosi sulla dommatica tradizionale, lasciandosi tuttavia aperta una scappatoia, nel caso nel

quale, con la loro insistenza sull'imputazione esclusiva [degli effetti giuridici] agli essere umani, dovessero un giorno trovarsi in una condizione di totale emarginazione sociale», e p. 109, ove si legge «Dovremmo allora immaginare soluzioni dogmatico-giuridiche altrettanto ibride? Dovremmo quindi introdurre l'associazione uomo-macchina anche nella costruzione tecnico-giuridica? È un'alternativa, questa, da prendere risolutamente sul serio, benché sino ad ora non sia stata ancora esaminata adeguatamente. Le singole condotte negoziale degli agenti software e degli esseri umani coinvolti confluiscono tutte, senza che sia necessario separare l'una dall'altra, in una unitaria condotta dell'associazione uomo-macchina, sì che tale condotta unitariamente imputabile all'associazione implica la creazione tanto di vincoli giuridici quanto di fattispecie di responsabilità. All'opposto della visione giuridica individualista connessa al fenomeno della rappresentanza [...] qui è la stessa associazione uomo-macchina a divenire una parte contrattuale unitaria». Per una più estesa valutazione del pensiero dell'A. citata sia consentito il rinvio A E. CATERINI, *L'intelligenza artificiale «sostenibile» e il processo di socializzazione del diritto civile*, in *Diritto Scienza Tecnologia*, 10, collana diretta da S. Faro, N. Lettieri, C. Perlingieri, Napoli, 2020, p. 66 e ss.

⁶⁴ V., Cass., seconda sezione, sentenza, 19 gennaio 2022, n. 1682: «Il Collegio osserva che un punto fermo, e pacifico nella giurisprudenza di questa Corte, è rappresentato dalla possibilità di predicare la responsabilità solidale della persona giuridica, o dell'ente privo di personalità giuridica, non solo quando l'autore è legato al soggetto collettivo da un formale rapporto organico ovvero da un rapporto di lavoro subordinato, ma anche in tutti i casi in cui i rapporti siano caratterizzati in termini di affidamento (inteso come materiale consegna all'autore della violazione del materiale pubblicitario) o di avvalimento (inteso come attività di cui il committente si giova), a condizione, però, che l'attività pubblicitaria sia comprovatamente riconducibile all'iniziativa del beneficiario. Si tratta di un indirizzo nomofilattico costante che, nella sentenza n. 1040 del 2012, si trova compendiato nell'affermazione secondo cui il terzo comma dell'art. 6 individua “nel rapporto oggettivo e funzionale della condotta tenuta con l'interesse ovvero gli scopi di una persona giuridica o di un ente di fatto” il titolo stesso della solidarietà di detti enti con l'autore della violazione, indipendentemente dalla identificazione della persona fisica che ha commesso materialmente la violazione. La sentenza n. 13770 del 2009 lo declina e lo scolpisce nella necessità di una comprovata riconducibilità dell'attività pubblicitaria al beneficiario. [...] Il terzo aspetto condiviso è costituito dal rilievo che a giustificare l'imputazione solidale non basta la circostanza di fatto del mero giovamento. La sentenza n. 1370 del 2009 richiede che l'attività pubblicitaria sia

comprovatamente riconducibile all'iniziativa del beneficiario quale committente o autore del messaggio pubblicitario o che sia documentato il rapporto tra autore della trasgressione ed ente o persona giuridica opponente ed esclude che il beneficiario del messaggio pubblicitario possa essere ritenuto solidalmente responsabile della violazione per il solo fatto di averne potuto trarre giovamento. Tale sottolineatura è ribadita anche nella giurisprudenza successiva: ordinanza n. 29891 del 2018 e ordinanza n. 100 del 2019».

⁶⁵ C. PERLINGIERI, *Responsabilità civile*, cit., p. 173: «Se l'algoritmo può essere definito quale "serie di istruzioni specifiche, passo dopo passo, per prendere un input e convertirlo in output", gli algoritmi sono, principalmente, una creazione umana come è umana la fonte dei dati forniti e trattati (gli input) per costruire modelli statistici diretti alla formulazione di previsioni o di comprensione critica i quali, in presenza di un test del programma per ciascuna classe di input del problema con un risultato diverso da quello atteso, dovranno essere riformulati».

⁶⁶ Di differente avviso, U. RUFFOLO, *Intelligenza artificiale*, cit., p. 1698 ove si legge: «per gli artt. 2047 e 2048 c.c., in ragione della loro specificità. Essi paiono infatti destinati a normare responsabilità derivanti dal controllo o dalla "educazione" di particolari "tipi" di esseri umani, dettando così una disciplina molto settoriale. La quale si rivela particolarmente tarata: (i) sulla particolare tipologia di minorate capacità di intendere e volere; (ii) su una responsabilità per fatto di altro soggetto il quale appare comunque dotato di personalità giuridica, oltre che potenzialmente corresponsabile o quantomeno dotato di patrimonio idoneo a poter corrispondere "equa indennità"; (iii) su una responsabilità di tipo colpevole, con inversione di taluni oneri probatori. Se non di *ius singulare*, si tratta di previsioni così peculiari, con criteri di attribuzione della responsabilità così specifici, da rendere scarsamente proponibile ogni loro estensione analogica alle responsabilità per danni cagionati dalla fallibilità di intelligenze non umane». Questa impostazione –come si sostiene nel testo– implica che la c.d. responsabilità dell'algoritmo abbia una natura derivata da chi ha concepito l'idea artificiale, tale da ricondurre ad esso la responsabilità, là dove deve considerarsi che l'autoapprendimento genera una graduale autodeterminazione volitiva che ha le sembianze di quanto l'ordinamento riconosce al discernimento del minore.

⁶⁷ Di altro avviso, sembra, M. COSTANZA, *L'Intelligenza Artificiale e gli stilemi della responsabilità civile*, in *Giur. it.*, 7, 2019, p. 1687, ove scrive: «Si suole tuttavia guardare alla A.I. come ad un ente in grado di esercitare delle scelte, di compiere decisioni, di pensare oltre ciò che le viene indotto. All'A.I. si attribuiscono sensazioni e sentimenti che sono riconosciuti agli esseri umani. L'A.I. po-

trebbe sfuggire al controllo del suo “creatore” e così proporsi come un ente al quale attribuire condizione umana, pur se con qualche deficit di capacità di discernimento che la renderebbe prossima all’incapace legale (e/o giudiziale), rispetto al quale, seguendo l’ordine di pensiero della tradizione, si darebbe luogo, sul versante della responsabilità civile (nella impostazione dell’ordinamento nazionale), ad ipotesi di responsabilità per difetto di sorveglianza. Lo stato infantile o di “debolezza mentale” della A.I. appare però soluzione bizzarra, nella quale si eleva a soggetto ciò che non si vuole trattare come tale almeno sul piano dell’imputazione delle conseguenze del suo operato. Né la ragione della esenzione da responsabilità dirette dipenderebbe dalla irreperibilità di un patrimonio della A.I. La surroga nelle responsabilità dell’incapace non è solo prevista per offrire garanzie di ristoro al danneggiato. La individuazione del soggetto responsabile è condizionata dal pre-concetto che senza colpa (anche remota) non vi è responsabilità. Se questo è il principio che aleggia o che informa (almeno sul versante nazionale) il regime della responsabilità civile, postulare la innocenza della intelligenza artificiale, per collocare altrove la responsabilità equivale alla negazione della sua coscienza e dunque contraddire il tentativo d’una sua umanizzazione in senso etico e soprattutto la rappresentazione dell’A.I. come ente affatto eterodiretto o preordinato o guidato nel suo agire. Se la intelligenza artificiale non può considerarsi entità passibile in sé di responsabilità, ciò significa che non le si riconosce autonomia di discernimento. La educazione al bene quale canone al quale si dovrebbe attenere l’impostazione della intelligenza artificiale postula la sua permeabilità e l’inevitabile abbassamento del livello della sua capacità di giudizio. Il suo sapere, cioè, non basterebbe a fornire strumenti decisionali o di valutazione che non siano già predisposti o predefiniti. Non soltanto mancherebbe alla A.I. una propria volontà, ma soprattutto alla A.I. non apparterebbe la libertà dell’errore, con l’onere delle sue conseguenze, almeno finché del suo agire altri venga richiesto di rispondere». La tesi sembra non considerare che l’A.I. può acquisire una sua volontà senza avere capacità di giudizio, cioè senza discernimento, e che anche il minore incapace può risultare responsabile (art. 2047 ul.co.). Ciò a riprova della considerazione che la responsabilità è l’esito di un bilanciamento di interessi e valori che richiedono la valutazione della circostanza concreta e dei soggetti a cui si riferisce. Dunque, un conto è misurare la capacità dell’A.I. con le gradazioni riferite alla persona umana, altra cosa assimilare i due fenomeni e ricavarne conseguenza automatiche in termini di responsabilità.

⁶⁸ Un banco di prova può rinvenirsi nella responsabilità causata da veicoli *self-driving* o con supporti automatici alla guida, sul punto, v., U. RUFFOLO E E.

AL MUREDEN, *Autonomous vehicles e responsabilità nel nostro sistema ed in quello statunitense*, in *Giur. it.*, 2019, p. 1704 e ss., ove si legge: «Fra i futuri scenari, dunque, emerge, in taluni casi, la possibilità di invocare anche una “responsabilità da algoritmo”, e quindi la potenziale estensione della responsabilità da prodotto difettoso e dannoso anche a colui che “fornisce” la componente “algoritmo” al costruttore dell’automobile “intelligente”. Con una serie di rilevanti conseguenze: da un canto, la esposizione a diretta corresponsabilità da prodotto per quel co-produttore di una componente (“immateriale”) del bene finale; dall’altro, le conseguenti maggiori possibilità, per il produttore finale medesimo, di chiamare come corresponsabili agenti apparentemente mediati, e non immediati, della produzione stessa; e, dunque, di agire verso tali soggetti eventualmente anche in regresso o in garanzia. [...] Seria via percorribile, se si volesse alleggerire la responsabilità oggettiva del produttore, sarebbe l’imposizione di coperture assicurative non da responsabilità ma da evento. Oppure sostituire le stesse con la creazione di un fondo, finanziato con contribuzione – o prelievo anche di tipo fiscale – a carico dei produttori di settore. [...] Quanto ora detto conforta altresì la già illustrata tesi circa la cumulabilità fra la tutela da *product liability* e quella ex art. 2050 c.c.: la “sicurezza” garantita dagli standard non elide la pericolosità di una particolare attività produttiva e del conseguente prodotto, così come non esclude che un prodotto omologato come “sicuro” si possa poi rivelare difettoso e dannoso. Un cruciale problema che concerne in generale tutti i prodotti incorporanti A.I., ma in particolare l’automazione dei veicoli (quella futura, ma già anche quella attuale e parziale), è connessa ai rischi di *hackeraggio*. La esposizione ai quali può rendere al tempo stesso non sicura e difettosa un’auto *self-driving* che sia permeabile alle intrusioni da parte di *hacker*. [...] Prendiamo le mosse dalla classificazione prevalente. La quale riconosce cinque livelli di automazione, ove il livello 5 è attribuito alle auto interamente *driverless* e quelli precedenti sono caratterizzati dalla possibilità di guida umana sostitutiva (livello 4) o integrativa (livello 3), con differenziati compiti assegnati al conducente: nel caso del livello 4 sarà un guidatore-sentinella: dovrà assumere i comandi solo quando la macchina lo chiede; per le auto di livello 3 resterà guidatore attivo: dovrà rimanere vigile anche quando inerte, ma sempre pronto a passare tempestivamente alla guida in ogni occasione giudicata necessaria. Dunque, la diligenza esigibile poco si discosta da quella relativa alla ordinaria guida manuale. In entrambe le ipotesi avremo un “conducente” ai sensi dell’art. 2054 c.c. Permanendo dunque identico il criterio sia di attribuzione della responsabilità che di valutazione della diligenza del driver, potrebbe sorprendentemente risultare talora più facile incorrere in responsabilità per il guidatore assistito, perché

indotto di fatto ad essere meno vigile, con tempi di reazione meno tempestivi. [...] Anche quando sarà permessa la circolazione alle auto *driverless*, senza pedaliere né sterzo, dove l'unica operazione manuale consentita a bordo potrebbe essere l'avvio o l'arresto della marcia, la Convenzione di Vienna del 1968, in assenza di modifiche, continuerà ad imporre la presenza di un driver. Un tale "conducente-sentinella" conserverà, quindi, obblighi e doveri di diligenza parametrati alla capacità di intervenire tempestivamente quando necessario, anche solo arrestando la marcia o segnalando le anomalie all'esterno. [...] Lo sforzo di assicurare il massimo sociale in termini di tutela delle vittime ed al tempo stesso il massimo economico con una disciplina non disincentivante della responsabilità da prodotto, può ben essere conciliato con le tesi qui sostenute: – (i) una *product liability* che veda interpretativamente limitati i danni risarcibili da "lesione" alla persona, nel senso retro indicato; – il possibile selettivo cumulo di (ii) una concorrente responsabilità da attività pericolosa, se e quando invocabile (*v. retro*); – l'eventuale effetto di temperamento e razionalizzazione che potrebbe conseguire dalla integrativa previsione di (iii) idonei obblighi assicurativi, o di (iv) costituzione di "fondi" idonei a coprire taluni danni (anche) da evento (*v. retro*). Il ristoro del pregiudizio, in quest'ultimo caso, potrebbe essere accordato a prescindere dalle responsabilità; e potrebbe venire, allora, eventualmente limitato a previsioni indennitarie e non risarcitorie». Gli Aa. sostengono la superfluità di una normazione specifica, mentre ritengono adeguato il ricorso al sistema giuridico di responsabilità esistente che include le concorrenti responsabilità del conducente, da attività pericolosa, da cosa in custodia, del produttore, del preposto o dipendente. Allo scopo di non riversare il rischio sul danneggiato, nelle ipotesi in cui nessuna delle precedenti forme di responsabilità dovesse incorrere, gli Aa. ricorrono alla responsabilità sociale senza con ciò escludere che anche nelle precedenti forme non possa delinearsi la co-responsabilità da algoritmo, che distingue l'attante dall'attore.

⁶⁹ Di diverso avviso è A. AMIDEI, *Intelligenza Artificiale e product liability: sviluppi del diritto dell'Unione Europea*, in *Giur. It.*, 2019, p. 1715 e ss., ove si legge: «Stando alla definizione di "autonomia" adottata dalla Risoluzione del Parlamento Europeo del febbraio 2017 in materia di norme di diritto civile sulla robotica, tale caratteristica si estrinseca nella "capacità di prendere decisioni e metterle in atto nel mondo esterno, indipendentemente da un controllo o un'influenza esterna", con un livello variabile a seconda del grado di complessità con cui è stata progettata l'interazione della macchina con l'ambiente. [...] sul piano delle responsabilità per danni cagionati da una imponderabile evoluzione dell'intelligenza artificiale, la più o meno elevata autonomia dell'A.I. ap-

pare, secondo alcuni, potenzialmente idonea a determinare una interruzione del nesso causale tra condotta umana e danno eventualmente cagionato dall'impiego della macchina, con specifico riguardo alla possibilità che la capacità di "autoapprendimento" della macchina la conduca a comportamenti impensati, a scelte imprevedibili e, talora, ad esiti dannosi. [...] Pare, infatti, difficile pensare che il produttore dello *smart product* possa davvero, in ultima istanza, non rispondere del danno che quest'ultimo abbia cagionato, al di là della prevedibilità o meno dell'evento lesivo da parte di chi ha messo in commercio quel prodotto. [...] Ancora una volta emerge la necessità di distinguere il piano etico da quello delle responsabilità giuridiche. Ebbene, al di là delle implicazioni etiche di un tale interrogativo (ossia se una siffatta attribuzione di responsabilità in capo al produttore sia o meno "giusta"), in termini strettamente giuridici e di politica legislativa la risposta circa l'opportunità di responsabilizzare il fabbricante del prodotto per ipotesi quali quelle descritte non può che essere positiva. [...] Esiste, però, nel caso degli *smart product*, un'ulteriore possibile casistica che rappresenta specifica peculiarità di tale tipologia di prodotti. Ci si riferisce all'ipotesi in cui il prodotto non presenti alcun difetto "genetico" nel momento in cui viene messo in commercio, ma che, in virtù della successiva esperienza elaborata in base alle regole fornitegli dall'algoritmo che ne anima apprendimento ed evoluzione (ossia dei dati che raccoglie, del contesto in cui opera, delle caratteristiche ed abitudini del suo utente, ecc.), modifichi la propria condotta sino a dare corso ad indesiderate conseguenze dannose, più o meno imprevedibili anche per il suo stesso ideatore, programmatore o produttore. [...]». L'A. dopo avere distinto la sicurezza dalla difettosità del prodotto [«La tematica del danno da prodotto non difettoso non ha ancora trovato una definitiva sistemazione nella giurisprudenza della Corte di Giustizia (invero esigua sul tema). Larga parte della giurisprudenza italiana, invece, la risolve, da un lato, garantendo tutela al danneggiato non sulla base della disciplina della responsabilità da prodotto, bensì di altre previsioni codicistiche nazionali, come quella relativa alla responsabilità da attività pericolosa, responsabilizzando così il fabbricante del bene ritenuto pericoloso anche in assenza di un suo difetto; dall'altro, riconoscendo che l'*assessment* circa la difettosità di un prodotto può, e deve, ricomprendere anche la verifica del rispetto dei requisiti previsti dalla normativa tecnica di settore applicabile, ma in tale verifica non può esaurirsi»], afferma che la reinterpretazione del significato di «difetto» del prodotto può includere anche le ipotesi derivanti dall'intelligenza artificiale *self-learning*. L'A. prosegue con alcune esemplificazioni: «Ad esempio, potrà assumere rilevanza, ai fini dell'esame della difettosità del prodotto, la mancata attivazione di "blocchi di sicurezza" idonei ad impedire al prodotto "intelli-

gente” di porre in essere determinate condotte. Ci si potrebbe, poi, interrogare anche sugli effetti della possibile interazione tra uomo e macchina “intelligente”. “Difetto” potrebbe, allora, essere altresì la mancata previsione di meccanismi volti a impedire l’esecuzione di comandi errati provenienti dall’uomo o, comunque, a correggere l’errore umano [...]. Senza contare, poi, la necessità di riflettere sul rischio di “aggressioni esterne” e *hacking* da parte di un soggetto terzo che potrebbe intervenire nell’operatività dell’intelligenza artificiale, alterandone il funzionamento o addirittura pilotandola verso esiti potenzialmente lesivi o comunque diversi rispetto all’*expected outcome* [...]. Una tale impostazione consentirebbe anche di superare il limite della esclusione di responsabilità prevista dall’art. 7 della Dir. 85/374/CEE per il caso in cui il prodotto non fosse difettoso nel momento della sua immissione in commercio, senza rivoluzionare l’impostazione di fondo della Direttiva medesima: il prodotto sarebbe, infatti, “nato difettoso” in quanto fabbricato ab origine privo dei blocchi che avrebbero dovuto limitarne l’evoluzione comportamentale ed impedirne le condotte lesive». Tale interpretazione muove dall’indifferenza della responsabilità dalla prevedibilità dell’effetto dannoso. Tuttavia, gli stessi esempi proposti non risultano neutri rispetto alla prevedibilità degli effetti connessi al comportamento dannoso, poiché in essi v’è insito il tema della prevedibilità o imprevedibilità di quanto potrà seguirà dall’atto dell’intelligenza artificiale. Già il codice civile, all’art. 1637, distingue il caso fortuito *ordinario* (ragionevolmente probabile, quindi prevedibile), dall’altro *straordinario* (neppure probabilmente prevedibile). Ora, in siffatta prevedibilità v’è una componente soggettiva che attiene al fattore colpa, che risulta escluso quando ragionevolmente la conseguenza accaduta risulta imprevedibile perché improbabile. Mentre nella prima ipotesi la difettosità del prodotto è ascrivibile al non avere previsto ciò che ragionevolmente sarebbe probabilmente potuto accadere, nella seconda, non v’è riconducibilità alcuna dell’evento all’attore-attante e, dunque, risulterebbe di dubbia conformità a costituzione ammettervi una responsabilità. Ecco la ragione della responsabilità sociale, assicurativa o del fondo: lo scopo è evitare che il rischio del danno da progresso possa essere sopportato dal danneggiato quando non sia ascrivibile al produttore latamente inteso. Una differente soluzione comporta la responsabilità di quest’ultimo anche nel caso fortuito straordinario, con l’effetto che, allo scopo di cautelarsi da tale evenienza, il presunto responsabile sia indotto a previamente addossare tale rischio in capo alla categoria dei consumatori senza alcuna condivisione con gli altri produttori. Né gli argomenti appena espressi mutano quando si reputa il progettista dell’algoritmo, responsabile (o co-responsabile insieme al produttore), in quanto a sua volta «produttore» di un componente del prodotto

finale. Si tratta pur sempre di un comportamento valutabile in termini di prevedibilità o imprevedibilità degli effetti dannosi.

⁷⁰ Scrive P. PERLINGIERI, *Sul trattamento algoritmico die dati*, in *Tecnologie e diritto*, cit., p. 188 e s.: «Non sempre, tuttavia, la responsabilità civile ha fondamento in un illecito, potendo pur essere collegata ad un'attività lecita dannosa, né è sempre condizionata dall'estensione del risarcimento del danno in base ad una funzione necessariamente compensativa ed in séguito al verificarsi di eventi tipici e univoci, né ai suoi fini è richiesta la capacità di agire tradizionalmente non riconosciuta agli agenti *software*. Sì che non è per niente peregrino escludere loro –che possono avere elevate capacità cognitive ancor maggiori di quelle umane– dal rispondere civilmente se patrimonialmente dotati e interpretando nel concreto la relazione instaurata tra programmatore, produttore e utilizzatore dell'agente *software* individuandone l'effettivo ruolo svolto, sia singolarmente sia in forma associata e ponendo sempre la dovuta attenzione al *cui prodest* secondo il brocardo *ibi commoda ubi incommoda*! Il tema attende di essere affrontato anche per la dimensione che i danni possono assumere non tanto in chiave di responsabilità oggettiva o di esposizione al pericolo, quanto piuttosto –sia pure *de iure condendo*– di sicurezza sociale, e quindi, nell'ambito del sistema fiscale, specie là dove la interconnessione tra agenti *software* rende praticamente impossibile qualsiasi controllo del funzionamento dell'articolata “rete” algoritmica».

⁷¹ C. PERLINGIERI, *Responsabilità civile*, cit., p. 175.

⁷² V., G. F. ITALIANO, *Le sfide interdisciplinari dell'intelligenza artificiale*, cit, p. 13 e s.: «La parte più delicata di tutto questo processo è proprio la creazione del modello, che viene costruito a partire dai dati. Questa è la fase di *training*: gli algoritmi di *machine learning* usano i dati per imparare, cercano di trovare segnali nascosti all'interno dell'enorme quantità di dati su cui lavorano (da cosa possiamo capire che c'è un gatto nella foto? Da cosa possiamo capire che c'è un pedone che sta attraversando la strada? O comprendere la segnaletica stradale?). Gli algoritmi usati per creare questi modelli sono molto sofisticati. Come diceva lo statistico George Box, “tutti i modelli sono sbagliati, ma qualcuno è utile” (*all models are wrong, but some are useful*). Gli algoritmi di *machine learning* fanno esattamente questo: costruiscono modelli complicati, modelli sbagliati, ma fondamentalmente molto utili. Soprattutto se i dati sui cui hanno fatto *training* sono molti e di buona qualità. Altrimenti si rischia di creare un modello non solo sbagliato, ma anche inutile: come dicono i nostri colleghi anglosassoni, *garbage in garbage out*: prendendo spazzatura in ingresso (dati molto sporchi o di cattiva qualità), produciamo spazzatura in uscita (un modello sbagliato e inutile). [...] Come è avvenuto ad esempio nella medicina. Oggi ci sono molti

algoritmi di *machine learning* che sono in grado di diagnosticare i primi segnali di malattie, come ad esempio patologie mentali, cardiopatie, tumori. Lavorano su grandissime quantità di dati provenienti da pazienti, costruiscono i loro modelli, e dai primi esperimenti riescono ad avere accuratèzze confrontabili e a volte superiori a quelle dei medici. A scoprire i primi segnali di patologie che i medici non riescono ancora a vedere, così da poter intervenire tempestivamente con le terapie necessarie e salvare vite umane. Ma questo genera anche problemi completamente nuovi. Innanzitutto c'è un problema di fiducia: in un campo così delicato, come quello della medicina, come faccio ad avere fiducia in un sistema che non è trasparente, non è interpretabile da un essere umano? Nella medicina non è poi così immediato riuscire ad avere fiducia in un oracolo, uno stregone, o in una *black box*. E inoltre, in medicina è molto importante la fase di validazione clinica. In questo caso chi la fa? I medici spesso non hanno gli strumenti per capire e utilizzare algoritmi e modelli molto complicati. Gli informatici non hanno nè gli strumenti nè gli incentivi per aiutare i medici nelle fasi di validazione clinica. Molto spesso, i modelli funzionano molto bene per la popolazione su cui sono stati sviluppati, ma se vengono applicati a una popolazione diversa, proveniente da altre nazioni o semplicemente da altre aree geografiche, rischiano di fare degli errori».

⁷³ V., G. COMADÈ, *Intelligenza artificiale e responsabilità*, cit., p.186 e ss. «La scelta della regola di responsabilità civile collegata all'uso di IA in questo rinnovato e più ampio quadro può essere scelta di volta in volta per la sua maggiore capacità di servire uno o più delle sue tradizionali finalità (*compensation, deterrence*) senza dovere per forza farle carico di una soluzione olistica. Questa invece andrebbe ricercata nel più ampio principio dell'*accountability*. Di questa logica, che del processo, dei controlli, del sapiente uso dei diritti degli interessati e delle prerogative imprenditoriali è ormai da tempo un territorio di sperimentazione la *data protection*», l-A. ritiene che l'*accountability* sia il criterio più ragionevole per definire la distribuzione dei rischi connessi all'uso dell'AI: «Ribadita la centralità dei dati personali «per la formazione di sistemi di apprendimento automatico e di intelligenza artificiale» e i rischi che essi “contengano distorsioni intrinseche che possono portare a decisioni che possono ingiustamente discriminare determinati individui o gruppi, limitando potenzialmente la disponibilità di determinati servizi o contenuti, interferendo così con i diritti individuali come la libertà di espressione e di informazione o provocando l'esclusione di persone da determinati aspetti della vita personale, sociale e professionale” le autorità sottolineano in particolare “che i sistemi basati sull'intelligenza artificiale le cui decisioni non possono essere spiegate sollevano questioni fondamentali di *accountability* non solo per la normativa

sulla privacy e sulla protezione dei dati, ma anche di responsabilità in caso di errori e danno”. Se si tralascia qui il riferimento, ovvio ma non scontato, all’invito a progettare, sviluppare e utilizzare le IA “nel rispetto dei diritti umani fondamentali e in conformità con il principio di equità”, “prendendo in considerazione non solo l’impatto che l’uso dell’intelligenza artificiale può avere sull’individuo, ma anche dell’impatto collettivo sui gruppi e sulla società in generale” emerge centrale il ruolo della *accountability* nel limitare i rischi e gli eventuali effetti negativi delle IA».

⁷⁴ Condivisibile la tesi di A. ALPINI, *Sull’approccio umano-centrico all’intelligenza artificiale. riflessioni a margine del “progetto europeo di orientamenti etici per una IA affidabile”*, in *Comp. dir. civ.*, in www.comparazionedirittocivile.it, p. 7 e s., ove afferma che «A questo si collega il principio di trasparenza che, esigendo il pieno controllo e la comprensibilità umana dei processi di IA, sembra di fatto escludere la configurabilità della c.d. intelligenza artificiale forte (strong AI). Sí che le *machine learning* che evolvono apprendendo dalla propria esperienza e in modo non sempre prevedibile, o i più complessi sistemi adattivi in grado di modificare il proprio codice autonomamente per adattarlo alle circostanze esterne appaiono in contrasto con tali principi. Da questa prospettiva la proposta di riconoscere ai robot uno *status* giuridico di persone elettroniche dal quale deriverebbe una piena personalità giuridica e dunque persino l’esercizio di diritti fondamentali appare una scelta non compatibile con i valori costituzionalmente garantiti. Se infatti la macchina è servente, ausiliaria alle attività umane, non si può sostenere che l’autonomia del software giunga al punto di escludere il controllo umano e di agire nel proprio interesse. Ciò significherebbe accettare tutti i rischi connessi alla imprevedibilità dei comportamenti degli algoritmi poiché si tratterebbe non di errori di calcolo del programmatore ma di decisioni imprevedibili di algoritmi». La tesi espressa dall’Autrice pone in evidenza il limite della soggettivazione algoritmica (o algorismica), limite teso ad impedire che detta soggettività si sostituisca alla persona nello svolgimento di attività (e, quindi, nell’assunzione di responsabilità) che attengono allo svolgimento della personalità e al valore della dignità dell’uomo.

⁷⁵ Emerge dalla proposta di Regolamento 2021/0106 (COD) sull’AI la distinzione di un differente livello di rischio connesso all’impiego dell’AI; tale diverso livello è da connettere al differente livello di autonomia e autodeterminazione dell’AI. Osservazione rilevata da U. SALANITRO, *Intelligenza artificiale e responsabilità: la strategia della commissione europea*, in *Riv. dir. civ.*, 6, 2020, p. 1274 e ss., ove descrive le ipotesi di responsabilità indicate nella proposta di Regolamento: «Entrambe le tipologie di operatori [*front-end*, che controlla il funzionamento dell’AI e ha beneficio da esso; *back-end*, che definisce le carat-

teristiche del software e ne conserva il controllo] sono soggette a una regola di responsabilità solidale, in caso di concorso di colpa o di coinvolgimento in un danno causato da attività ad alto rischio, e sono tenuti, stavolta soltanto nel caso di attività ad alto rischio, a stipulare un'adeguata polizza assicurativa a copertura. Seguendo il modello della Commissione, resta centrale il concetto di attività ad alto rischio, per il cui esercizio l'operatore è soggetto a responsabilità oggettiva. Le attività ad alto rischio sono definite in base alla gravità dei possibili danni, al grado di autonomia della macchina, alla probabilità del danno, e alle modalità o al contesto di utilizzo dello strumento: per garantire l'affidamento degli operatori, però, sono sottoposte al regime di responsabilità solo le attività individuate in apposito elenco, che deve essere allegato al Regolamento, da sottoporre alla verifica e all'aggiornamento della Commissione. È previsto inoltre un massimale per ogni persona danneggiata, secondo un modello coerente con il regime della responsabilità oggettiva. Restano invece sottoposte a un regime di responsabilità più attenuato le altre attività che impiegano intelligenza artificiale. Nella proposta di regolamento si evoca la responsabilità per colpa, aggravata da un sistema di presunzioni. Spetta all'operatore dimostrare di avere esercitato diligentemente le operazioni appropriate all'uso dell'intelligenza artificiale (selezionando un sistema idoneo al compito e alle competenze, mettendo debitamente in funzione il sistema, monitorando le attività e mantenendo l'affidabilità operativa mediante periodici aggiornamenti); in alternativa, l'operatore deve dimostrare che il sistema si sia attivato al di fuori del controllo dell'operatore, nonostante l'adeguatezza delle misure adottate per evitare tale attivazione».

⁷⁶ Scrivono A. VITERBO E A. CODIGNOLA, *L'intelligenza artificiale e le sue origini culturali*, cit., «Secondo Turing anche se è vero il teorema di Gödel che dimostra che in qualsiasi sistema logico sufficientemente potente si ottengono enunciati che non possono essere né provati né confutati all'interno del sistema stesso, è altresì anche vero però che nessuna limitazione è applicabile alle capacità della mente umana e che, quindi, nessuna limitazione sarà applicabile all'Intelligenza artificiale delle macchine del secondo ordine, capaci di andare oltre il livello critico. Queste macchine intelligenti, a parte gli errori di funzionamento, potranno incorrere in errori di «conclusione», ovvero di elaborazione, e di questa possibilità di errore gli uomini dovranno tenere conto. Secondo Turing la supermacchina di secondo livello, crescendo, avrebbe imparato («come fanno i bambini») a ragionare fino a produrre algoritmi e giungere a conclusioni di contenuto conoscitivo nuovo».

⁷⁷ G. F. ITALIANO, *Le sfide interdisciplinari dell'intelligenza artificiale*, cit, p. 16 e s.: «Un ultimo caso che può essere interessante analizzare, sempre indicativo dei problemi risolti ma anche dei nuovi problemi che possono essere creati dagli algoritmi, è un esempio concreto che è accaduto l'anno scorso a Boston. Riguarda il servizio degli scuolabus, per accompagnare gli studenti nelle scuole pubbliche. A Boston, vengono spesi ogni anno oltre 120 milioni di dollari per fornire questo servizio a più di 25.000 studenti di oltre 200 scuole pubbliche con un totale di 650 scuolabus. Organizzare bene questo servizio è un problema complicatissimo. Bisogna decidere quanti scuolabus utilizzare, che giro far fare a ogni scuolabus, decidere tutte le fermate degli scuolabus in modo che ognuna delle fermate sia raggiungibile a piedi. A questi vincoli se ne aggiungono molti altri, come ad esempio la presenza di studenti disabili o con necessità speciali, strade piccole in cui non possono accedere tutti gli scuolabus e, nel caso di Boston, ovviamente i grandi problemi di traffico tipici delle grandi città. In poche parole, trovare una buona soluzione a questo problema è veramente un incubo computazionale. Non lo può fare un essere umano, ma è anche molto complicato per un algoritmo. Nel 2017 Boston Public Schools avviò una collaborazione con Dimitris Bertsekas, una delle superstar di ricerca operativa della Sloan School of Management di MIT, con l'obiettivo di ridurre di 50 unità il numero di scuolabus utilizzati, per un risparmio stimato di 5 milioni di dollari l'anno. Sia Boston che MIT fecero una grandissima pubblicità a questa partnership tra pubblico/università/privato, che avrebbe sicuramente migliorato l'efficienza di un servizio pubblico, e consentito di investire le risorse risparmiate in progetti per il miglioramento della qualità dell'istruzione. Era un successo annunciato, e tutti si aspettavano che questo avrebbe dimostrato ancora una volta l'incredibile impatto degli algoritmi e delle tecnologie sul miglioramento della società. Ma purtroppo non è andata esattamente così. Appena è stato annunciato il cambiamento nell'orario degli scuolabus, alcune famiglie hanno trovato il nuovo orario inaccettabile e hanno protestato veementemente, marciando verso la City Hall. Questa protesta ha costretto il sistema delle scuole pubbliche di Boston a ritornare all'orario precedente, facendo sprecare tutto il lavoro fatto, tutte le risorse finanziarie e il tempo investito nel progetto. [...] Chi ha protestato ha criticato l'algoritmo, che è stato visto come una scatola chiusa, qualcosa di non trasparente, che prendeva decisioni sulla vita personale dei cittadini».

⁷⁸ V., P. PERLINGIERI, *Sul trattamento algoritmico dei dati*, in *Tecnologie e diritto*, cit., p. 189.

⁷⁹ Questione, questa, nota come *gap liability*, ossia quel vuoto di irresponsabilità che costituirebbe il rischio dell'utilizzatore. Se, per un verso, deve evitarsi

che il sistema delle responsabilità possa essere un fattore d'inibizione o rallentamento della conoscenza scientifica, dall'altro deve evitarsi che l'irresponsabilità del produttore o del custode -secondo le regole della responsabilità civile- possa spostare il rischio a carico dell'utilizzatore. Affronta il tema U Salanitro, *Intelligenza artificiale e responsabilità*, cit., p. 1273 e s., ove scrive: «A fronte dei dubbi derivanti da possibili opacità del mercato, mi sembra che resti insuperabile l'idea che il sistema della responsabilità oggettiva, se adeguatamente tarato, è preferibile a quello di un fondo indennitario che socializza il rischio, perché ne incentiva la riduzione, costringendo a fissare il livello della produzione o dell'attività in modo economicamente sostenibile e al contempo promuovendo le politiche per il miglioramento della sicurezza: se il produttore o il *provider* potessero collocare altrove il costo dei rischi inevitabili, ma calcolabili, non sarebbero spinti a migliorare le performance dei sistemi di intelligenza artificiale per ridurne ulteriormente l'impatto. [...] Piuttosto, potrebbe essere utile approfondire una diversa versione del *compensation fund*, il cui onere di finanziamento non ricada sugli utenti, quanto piuttosto sui produttori, ed eventualmente sui *provider*, secondo un criterio legato non tanto alla quota di mercato, che ridurrebbe l'effetto incentivante della responsabilità, quanto piuttosto alla frequenza e alla gravità degli incidenti in cui il prodotto o la rete sia coinvolta. Il fondo, che potrebbe essere integralmente sostitutivo della tecnica di responsabilità, avrebbe anche la funzione di coprire i danni anonimi, consentendo una parziale socializzazione dei rischi, e avrebbe il vantaggio di consentire un risparmio dei costi amministrativi di gestione del conflitto».

⁸⁰ Occorre considerare che la tutela delle posizioni minime esistenziali dell'uomo possono essere più agevolmente attentate dal malfunzionamento ei mercati, e ciò può risultare facilitato anche dall'AI, si pensi ai c.dd. algoritmi dei prezzi, ai fenomeni discriminatori che ne derivano connessi a quelli collusivi o pre-collusivi messi in atto dalle imprese, v., A. PEZZOLI e A. TONAZZI, *Discriminazione e collusione tacita tra lessico, intelligenza artificiale e algoritmi*, in *An. Giur. Ec.*, 1, 2019, p. 201 e ss.: «Le cose però si complicano con l'uso degli algoritmi e, soprattutto, con la grande disponibilità di dati sul comportamento dei consumatori che hanno reso realizzabili forme sempre più sofisticate di discriminazione, fino ad arrivare ai «prezzi personalizzati». In linea di principio – e questo è un punto da approfondire – appare ora possibile che a ogni singolo consumatore sia praticato un prezzo diverso e perfettamente corrispondente alla sua disponibilità a pagare, arrivando così a quella discriminazione perfetta (o, di primo grado, nel linguaggio degli economisti) che fino a poco tempo fa appariva soltanto un'ipotesi astratta da manuale di economia. [...] A seconda di quanto ci si avvicini alla discriminazione perfetta il *consumer welfare* può essere

azzerato a totale vantaggio del produttore. [...] Infine, non va escluso il ricorso a norme anti-discriminazione quando la disponibilità di dati sulle caratteristiche dei consumatori porti ad una differenziazione di trattamento in contrasto con la tutela dei diritti umani. [...] Premesso che la ratio degli algoritmi di prezzo è tradizionalmente la ricerca di una maggiore efficienza e che, quindi, dalla diffusione degli algoritmi sarebbe lecito attendersi innanzitutto benefici per i consumatori, non può essere trascurato il fatto che grazie agli algoritmi è però sempre più agevole raggiungere equilibri collusivi, in tempi rapidi e con maggior frequenza, rendere più stabili cartelli pre-esistenti e, attraverso meccanismi di *hub & spoke*, offuscarne la formazione [...].»

⁸¹ Questo induce ad escludere una risposta univoca in termini di responsabilità oggettiva, per colpa, o colpa presunta, o colpa oggettiva, ovvero, nuova soggettività; per una disamina delle differenti soluzioni v., U. SALANITRO, *o.u.c.*, p. 1249 e ss. ove, a proposito della nuova soggettività si legge: «Obiettivi analoghi si pongono invero anche i sostenitori della soggettività digitale. La migliore dottrina che propone questa soluzione è consapevole che il problema non deve essere posto in termini naturalistici, ossia non è conseguente alla eventuale similitudine dei robot con gli uomini, quanto piuttosto è volto alla soluzione dei conflitti di interessi. L'estensione della soggettività giuridica è una scelta normativa volta a individuare nuovi centri di imputazione, evitando di mettere in tensione il sistema della responsabilità civile. In questa prospettiva la soggettività sarebbe collegata alla formazione di un patrimonio o alla costituzione di un fondo assicurativo dedicato, vincolando ai conferimenti o ai premi quegli operatori che si ritiene congruo debbano sopportare il rischio: la qualifica di soggetto potrebbe risultare efficiente nel caso in cui il dispositivo sia un sistema aperto ai prodotti e ai servizi di altri operatori, potendo superare le difficoltà derivanti dalla frammentazione della produzione per individuare un unico responsabile. È stato obiettato, tuttavia, che tale impostazione sembra essere soltanto una tecnica per imputare indirettamente la responsabilità a una pluralità di imprenditori e utenti, quelli tenuti ai conferimenti o ai premi assicurativi, attraverso il velo di un nuovo soggetto, mettendo in tensione il sistema della soggettività e rischiando di incorrere nei problemi tipici della sottocapitalizzazione dei patrimoni dedicati: osservando al riguardo che il medesimo problema potrebbe essere risolto con uno sforzo minore adattando le discipline della responsabilità civile». L'obiezione non è condivisibile. La via della socializzazione della responsabilità da algoritmo è compatibile con la legalità costituzionale quando si tratta di danni provocati da un'AI che agisce con un'autonomia incontrollabile, sebbene statisticamente prevedibile. V., sul punto, anche C. PERLINGIERI, *Responsabilità civile*, cit., p. 163.

⁸² V., C. PERLINGIERI, *Responsabilità civile*, cit., p. 175.

⁸³ Il riferimento è sempre a G. Teubner, *Soggetti giuridici digitali*, cit., p. 105 e ss.

⁸⁴ V., R. MORO VISCONTI, *L'intelligenza artificiale: modelli di business e profili di valutazione*, in *Dir. ind.*, 5, 2018, p. 421 e ss., il quale nell'indicare le metodiche di misurazione dei valori incrementali dell'AI ne considera i molteplici fattori di sviluppo aziendali: «Uno dei contributi fondamentali che l'intelligenza artificiale ha fornito all'informatica è stato l'aver posto l'accento sulla nozione di problema, affiancandola a quelle di algoritmo e di dato, studiando ed evidenziando le varie modalità per la sua modellazione. La realtà *aumentata* inizia a diventare di dominio pubblico, ad esempio grazie ai *Google Glass* che, tramite un piccolo display posizionato sopra l'occhio, riempie il campo visivo di dati e informazioni sull'ambiente circostante di chi lo indossa. Essa, però, ancora prima di conquistare l'intero settore mobile (*smartphone, laptop, tablet*, occhiali e visori abbinati ad appositi software o applicazioni) ha mosso i primi passi in ambiti molto più tecnici e specifici, come quello militare, della ricerca scientifica e della medicina. I primi esempi di realtà aumentata, non a caso, sono introdotti nel settore dell'aeronautica militare sotto forma di head-up display (HUD). Questa tecnologia successivamente è stata adottata dall'aviazione civile».

⁸⁵ È la questione affrontata da Teubner e ripresa da P. Femia, *Soggetti responsabili. Algoritmi e diritto civile*, Introduzione a G. TEUBNER, *Soggetti giuridici digitali?*, cit., p. 14, ove si legge: «Quando poi le macchine intelligenti siano più e si colleghino in rete – in un certo senso si facciano rete, si 'retifichino' (tale sarebbe stata una traduzione 'creativa' di *Vernetzung*), allora diviene impossibile parlare di soggettività. Il rischio di interconnessione (*Vernetzungsrisiko*) – qui Teubner richiama i risultati raggiunti in un altro suo saggio fondamentale – è prodotto da una 'matrice anonima', da una rete discorsiva e decisionale di macchine intelligenti, ciascuna delle quali si giova e moltiplica la conoscenza e l'azione delle altre. Il limite costitutivo della soggettività, dice Teubner, è superato, la rete di computer interconnessi non è un soggetto, neanche nella forma di una società commerciale: troppo elevata l'intensità degli scambi tra nodo decisionale (singolo computer) e ambiente (la massa degli altri agenti software collegati o collegabili). Il soggetto è innanzitutto un confine tra una entità ed il suo ambiente; e se la soggettività si definisce comunicativamente, allora l'incrementata intensità delle comunicazioni e degli scambi comunicativi non consente di definire un soggetto, ma soltanto di descrivere una rete. La rete è la matrice di discorsi, matrice senza nome, anonima, perché non personificata. Il rischio di interconnessione si concepisce quindi soltanto come polo di rischio (*risk pool* lo definisce Teubner con terminologia inglese). E come polo di rischio potrà essere trattato dal diritto soltanto transitando dal

diritto individuale al diritto collettivo e forse, ci permettiamo di aggiungere, dalla responsabilità civile alla sicurezza sociale, secondo una idea avanzata già molti anni fa da Pietro Perlingieri».

⁸⁶ C. PERLINGIERI, *Responsabilità civile*, cit., p. 163 e s., «Occorre superare una considerazione unitaria della robotica, che pur ha consentito di prospettare anche la eventuale soggettività giuridica del robot, in favore di un'analisi che tenga conto della peculiarità del robot, delle particolari funzioni e utilizzazioni evidenziandone i compiti specifici riproducenti il lavoro umano e dunque le capacità funzionalizzate all'impiego, sì da consentire l'individuazione di funzioni adeguate al caso concreto in ordine alla natura e ai criteri di imputazione della responsabilità civile anche mediante la messa in evidenza della gradualizzazione e della diversificazione delle attività svolte dai robot».

⁸⁷ V., E. CATERINI, *L'intelligenza artificiale «sostenibile» e il processo di socializzazione del diritto civile*, cit., p. 100 e ss.

⁸⁸ V., A. ALPINI, *Sull'approccio umano-centrico*, cit., p. 6, ove si dà conto della posizione assunta dalla società giapponese per l'intelligenza artificiale che all'«art. 9 [delle linee guida etiche] riconosce una soggettività alle creazioni di IA, [dunque] una autonomia così elevata rispetto ai suoi programmatori tale da rendere necessario che le stesse applicazioni di IA debbano a loro volta rispettare le linee guida, sì che il prodotto della ricerca viene riconosciuto come autonomo membro della società. A tale riconoscimento consegue altresì il riconoscimento in capo al robot di diritti e di doveri non soltanto con riferimento alla legge sul copyright ma anche in ambiti particolarmente delicati quali il diritto di famiglia».

⁸⁹ V., P. PERLINGIERI, *Sul trattamento algoritmico dei dati*, in *Tecnologie e diritto*, cit., p. 190 ove si invoca la necessità di un «ordine pubblico di valenza internazionale» e di «una tavola di principi valoriali e una diffusa consapevolezza culturale che possano trovare attuazione nella prassi e nella decisione dei giudici»; l'A. richiama un'«adeguata istruzione quale antidoto alle distorsioni del fondamentalismo macchinico e delle sue simmetrie informative».

I diritti umani nell'era degli algoritmi e dell'intelligenza artificiale¹

MARCO FASCIGLIONE

Sommario: 1. Introduzione. - 2. Algoritmi e nuove forme di potere. - 3. Nuove tecnologie, valori ed individuo. - 3.1. L'incidenza sulla formazione del consenso individuale e la comunicazione delle idee. - 3.2. L'incidenza sull'autonomia e della capacità di autodeterminarsi dell'individuo. - 3.3. L'incidenza sul valore della dignità umana. - 4. Responsabilità e diritti umani nella società degli algoritmi. - 5. Conclusioni.

1. Introduzione

Il *machine learning*, gli algoritmi e le altre applicazioni dell'intelligenza artificiale stanno influenzando in modo sempre più crescente ogni tipo di attività umana. Gli effetti derivanti dallo sviluppo di queste tecnologie sono ovunque e hanno dimostrato di comportare sia conseguenze positive sia il rischio di interferire negativamente sulla vita delle persone. Da un lato, esse hanno aperto la via a nuove opportunità di espansione della produttività, di sviluppo economico e di progresso in molteplici settori. Dall'altro lato, il loro sviluppo, celere e non regolamentato, e la loro capacità intrusiva nella società pongono rischi per gli individui e per la salvaguardia dei loro diritti umani. Sotto il primo aspetto, tali tecnologie possono essere utili alla salvaguardia dei diritti umani grazie all'impatto positivo che esse possono avere, tra le altre cose, sui diritti delle donne, sul diritto alla salute, sui diritti degli anziani. L'automazione di lavori pericolosi può migliorare significativamente la salute e la sicurezza sul lavoro. Allo stesso modo, l'uso delle tecnologie collegate all'intelligenza artificiale, lo sviluppo di c.d. '*smart cities*' e di dispositivi connes-

si può contribuire a ridurre le emissioni di gas serra e ad aiutare pertanto a mitigare l'impatto negativo derivante dai cambiamenti climatici. Sotto il secondo punto di vista, tuttavia, le potenzialità dell'intelligenza artificiale, basate sui *big data*, sugli algoritmi e sui calcoli predittivi, combinate con la pervasività dei dispositivi e dei sensori del c.d. *Internet of Things*, sono in grado di incidere nel governo delle funzioni fondamentali della società, dall'istruzione alla salute, dalla scienza all'economia fino alla sfera del diritto, della sicurezza e della difesa, del discorso politico e del processo decisionale democratico. Tutto ciò sta animando da diversi anni un profondo e vivace dibattito nell'opinione pubblica, e tra gli studiosi, circa l'impatto del progresso tecnologico sui valori fondanti delle società contemporanee: la democrazia, il rispetto dello stato di diritto e la *rule of law*, la garanzia dei diritti umani. Un dibattito quindi niente affatto nuovo ma che, proprio a causa della vertiginosa accelerazione del processo tecnologico è di stringente attualità².

Queste brevi pagine perseguono, senza pretesa di esaustività, l'obiettivo di capire quale possa essere il ruolo del diritto internazionale dei diritti umani nella società dell'intelligenza artificiale e come prevenire conseguenze negative sui diritti umani di individui, comunità, eccetera, messi in pericolo da processi decisionali algoritmici. Ebbene, a giudizio di chi scrive le risposte a tale quesito richiedono l'utilizzo di tre chiavi di lettura. La prima attiene all'analisi del ruolo giocato dalle *nuove forme di potere* che si affacciano e agiscono nella contemporanea società degli algoritmi. La seconda chiave di lettura, riguarda l'analisi della capacità delle nuove tecnologie di incidere sui *valori* che si sono cristallizzati nell'ordinamento giuridico internazionale, ed in particolare negli strumenti internazionali di tutela dei diritti umani. La terza chiave di lettura, infine, attiene all'emersione di nuove *forme di responsabilità* dei diversi attori che operano nella contemporanea società degli algoritmi.

2. Algoritmi e nuove forme di potere

Partiamo dalla nozione di *potere*. Nella società degli algoritmi e dell'intelligenza artificiale emergono *nuove forme* di potere che possono mettere a rischio i diritti umani. Tali nuovi poteri si affiancano – o possono sostituirsi del tutto – ai tradizionali centri di esercizio del potere, sarebbe a dire gli Stati, intorno ai quali è si è tradizionalmente configurato il sistema internazionale di tutela dei diritti umani. Le imprese, tanto quelle del settore *High-tech* che sviluppano le tecnologie in esame, ma anche quelle che poi utilizzano tali tecnologie nei propri processi produttivi e commerciali, rappresentano una di queste nuove forme di potere, in grado di incidere sul godimento e sulla protezione dei diritti umani. Provo a spiegarmi con un esempio, quello delle c.d. *smart supply chains* in cui l'intelligenza artificiale può essere applicata in ottica di *capacity planning* come strumento per 'ottimizzare' le decisioni nell'organizzazione della catena del valore. Immaginiamo un'intelligenza artificiale che venga installata nei server di una grande azienda, ad es. una multinazionale dell'*automotive* che vende veicoli destinati al trasporto di beni e persone. Nei servizi e nei prodotti commercializzati da una tale ipotetica azienda possono rientrare: auto, furgoni, motrici, i pezzi di ricambio, le soluzioni energetiche (magari elettriche o ibride) che alimentano tali veicoli, le soluzioni finanziarie per il loro acquisto (e le relative banche e finanziarie gestite o partecipate dall'impresa) e tutta la filiera di fornitori e sub-fornitori situati in diverse aree del Pianeta. Immaginiamo che tale intelligenza artificiale sia 'autorizzata' dai suoi 'creatori' ad interagire sull'intera filiera dell'impresa allo scopo di migliorarne ed ottimizzarne la *value chain* per aumentare la produttività e massimizzare il profitto, e che nell'esercizio di tale compito le sia imposto come 'limite regolamentare' l'osservanza delle singole normative esistenti nei rispettivi or-

dinamenti nazionali interessati dalle attività dell'impresa. Quali le conseguenze? Essa potrà trovare soluzioni creative per raggiungere gli obiettivi dell'impresa: dalla creazione di sofisticate *shell companies* per sottoporsi a regimi fiscali più convenienti rispetto a quelli dove la multinazionale ha la propria sede, a strategie di acquisizione di risorse (materie prime, personale di ricerca, manodopera etc..) volte a contenere i costi attraverso l'impiego di processi di produzione che, seppur non illegali in quello specifico Stato, potrebbero sfociare in danni all'ambiente, alle persone e a comunità. In altri termini, quest'ipotetica intelligenza artificiale potrebbe sfruttare i *gap* regolamentari tra gli ordinamenti giuridici dei diversi Stati (ad es, le leggi nazionali giuslavoristiche, quelle sulla salvaguardia dell'ambiente) in modo tale che, pur rispettando le leggi dello Stato di origine, potrebbe ripianificare l'intera filiera spostando la produzione dove è 'più conveniente' per l'impresa. Il tutto per massimizzare il profitto! Non una novità per i modelli di business contemporanei in cui il principio della c.d. *shareholder primacy* obbliga le aziende a sfruttare l'opportunità concessa dai meccanismi di produzione lungo le catene di fornitura globali per ridurre i costi e massimizzare i profitti³, ma che un sistema di *machine learning* altamente evoluto può realizzare con migliore efficacia, spingendolo all'estremo con un potenziale 'effetto scalare' devastante per il pianeta e la società.

È esattamente in questa prospettiva di analisi che il dibattito sulle nuove tecnologie interseca quello sulle 'nuove forme di potere' ed in modo particolare quello sull'emersione di *nuovi attori* sulla scena internazionale che sempre più spesso contribuiscono, accanto agli Stati, alla formazione e all'attuazione delle norme di diritto internazionale. In un ambiente digitale globale le interferenze con il godimento dei diritti umani "non provengono solo dall'attuazione di tecnologie digitali da parte di attori pubblici, ma anche, e principalmente, dalla capacità

degli attori privati transnazionali di sviluppare e applicare standard privati in concorrenza con valori pubblici”⁴. In questa ottica, uno dei settori maggiormente in fermento riguarda il ruolo del settore privato nel sistema internazionale ed in modo particolare l’impatto delle attività delle *imprese* sui diritti umani con il processo di emersione di standard internazionali volti a disciplinare la condotta delle stesse in funzione di una loro “responsabilizzazione” in materia di diritti umani. Lo strumento internazionale di riferimento in materia è rappresentato dai Principi Guida ONU su imprese e diritti umani adottati nel 2011 dal Consiglio dei diritti umani delle Nazioni Unite⁵. Suddivisi in tre pilastri, il primo incentrato sull’obbligo statale di proteggere i diritti umani dalle violazioni riconducibili alle attività delle imprese, (il c.d. *State duty to protect*), il secondo relativo alla responsabilità delle imprese di rispettare i diritti umani (la c.d. *corporate responsibility to respect*), ed il terzo, infine, concernente il diritto di accesso ai rimedi per le vittime (c.d. *access to remedies*), i Principi Guida costituiscono il primo standard realmente ‘globale’ in materia. Nonostante essi non siano uno strumento vincolante hanno guadagnato un generale ed unanime consenso essendo diventati nel giro di pochi anni il principale standard internazionale in materia e sono stati riconosciuti da Stati, Organizzazioni internazionali, imprese, associazioni di categoria, ordini forensi, società civile e da tutti gli organismi onusiani che operano nel settore dei diritti umani⁶.

Il secondo pilastro dei Principi guida è particolarmente interessante ai fini della nostra analisi. In effetti esso fissa uno ‘standard di condotta attesa’ per le imprese che consiste nella responsabilità di evitare le violazioni dei diritti umani che esse possano *causare o contribuire a causare* e di prevenire l’impatto negativo sui diritti umani che deriva dalle attività di terze parti e che sia direttamente collegato alle loro operazioni, ai loro prodotti o servizi, in ragione di un rapporto commerciale con un

ente terzo⁷. Come è noto, il nucleo centrale di questa responsabilità si fonda su di uno standard di *due diligence* la c.d. *due diligence* aziendale sui diritti umani, che impone di cercare di prevenire l'impatto negativo sui diritti umani che può derivare dalle proprie operazioni economiche attraverso l'utilizzo di idonei processi volti a identificare, prevenire e rendere conto di come tali impatti vengono affrontati, nonché di porre loro rimedio⁸. Si tratta di un meccanismo di *risk-assessment* che si sostanzia in un processo continuativo di gestione del rischio che un'impresa ragionevole e prudente deve intraprendere, alla luce delle sue caratteristiche (settore di attività, contesto operativo, dimensioni e simili fattori) per far fronte alla sua responsabilità di rispettare i diritti umani⁹. Si tratta, insomma, di un approccio definibile come *human rights by design* all'impatto negativo delle attività di impresa sui diritti umani, che è applicabile anche alle imprese che sviluppano e/o utilizzano le moderne tecnologie digitali, basate sul *machine learning*, sull'intelligenza artificiale, ecc. Le imprese del settore tecnologico, infatti, già applicano un meccanismo, analogo ma più circoscritto, di valutazione del rischio di impatto negativo quando integrano le considerazioni in materia di tutela della *privacy* durante le fasi più importanti dello sviluppo di un prodotto (la c.d. *privacy by design*)¹⁰. In altre parole, la *due diligence* sui diritti umani si estende anche alle situazioni relative allo sviluppo e all'impiego di tali tecnologie, con le imprese che sono tenute a dimostrare di aver adottato tutte le misure appropriate per garantire la protezione dei diritti umani che potrebbero essere potenzialmente compromessi, in aggiunta e accanto alle questioni collegate alla tutela della *privacy*.

Se gli standard internazionali in materia di impresa e diritti umani già richiedono alle imprese di effettuare una *due diligence* generale sui diritti umani quando sviluppano e utilizzano tecnologie basate sugli algoritmi, stupisce allora che tale approccio regolamentare basato sull'adozione di misure preventive sia

assente dalla bozza di regolamento della Commissione europea del 2021 volta a fissare delle regole armonizzate in materia di intelligenza artificiale (il c.d. *Artificial intelligence Act*)¹¹. La proposta di regolamento mira a garantire, tra le altre cose, che i sistemi di intelligenza artificiale immessi sul mercato dell'Unione e ivi utilizzati siano *sicuri* e rispettino la normativa vigente in materia di *diritti fondamentali* e i valori dell'Unione, nonché a garantire una migliore *governance* e che le autorità e i tribunali nazionali competenti possano indagare e affrontare più efficacemente eventuali violazioni degli obblighi in materia di diritti fondamentali in presenza di violazioni dei requisiti di sicurezza applicabili ai sistemi di intelligenza artificiale. Purtroppo, la proposta attualmente pendente non include alcun riferimento ai Principi Guida ONU, né all'adozione di una *due diligence* generale in materia di diritti umani per le imprese che si avvalgono di questa tecnologia, né ad altri analoghi standard internazionali in materia di imprese e diritti umani. Non può essere considerato espressione di uno *human rights by design* il riferimento, contenuto nell'articolo 54 della proposta di regolamento, che, in relazione alla raccolta e al trattamento di dati personali nel processo di sperimentazione e utilizzo di sistemi di intelligenza artificiale, rinvia, alla lettera c), alla necessità che esistano effettivi meccanismi di monitoraggio per identificare qualsiasi rischio elevato per i 'diritti fondamentali' delle persone interessate, nonché a meccanismi di 'risposta' (c.d. *response*) per mitigare prontamente tali rischi e, ove necessario, interrompere l'utilizzo di tali sistemi. Tantomeno ciò può valere per la formulazione dell'articolo 67 della proposta di regolamento che prevede che qualora il sistema di intelligenza artificiale presenti un rischio per la salute o la sicurezza delle persone, oppure per la conformità agli obblighi previsti dal diritto dell'Unione, o da quello nazionale, a tutela dei diritti fondamentali o per altri aspetti della tutela dell'interesse pubblico, l'autorità di vigilan-

za del mercato di uno Stato membro può chiedere all'operatore di adottare tutte le misure adeguate a far sì che il sistema in esame, all'atto della sua immissione sul mercato o messa in servizio, non presenti più tale rischio o che sia, a seconda dei casi, ritirato dal mercato o richiamato entro un termine ragionevole, proporzionato alla natura del rischio. In entrambi i casi in effetti, la formulazione della proposta di regolamento non è allineata con le disposizioni del secondo pilastro dei Principi Guida ed il processo di *due diligence* aziendale sui diritti umani ivi disciplinati¹². Siffatta mancanza è ancora più grave ove si consideri che il regolamento persegue l'obiettivo di assicurare la coerenza con il diritto dell'Unione ed in modo particolare con la Carta dei diritti fondamentali dell'UE e con le politiche dell'Unione in materia di dati ed in particolare con il regolamento generale sulla protezione dei dati 2016/679. Nulla si dice, né si rinvia in alcun modo al processo legislativo avviato dal legislatore europeo e destinato all'adozione di una direttiva della Commissione volta ad introdurre un obbligo per il settore privato europeo di *due diligence* in materia di diritti umani ed ambiente applicabile anche lungo le *supply chains* (la c.d. *corporate sustainability due diligence*)¹³. Insomma, armonizzare gli sforzi di questi due processi legislativi sarebbe stato, ed è tutt'ora, auspicabile.

3. Nuove tecnologie, valori ed individuo

Passiamo alla nozione di *valori*. Il *machine learning* e la tecnologia dell'intelligenza artificiale 'toccano' tre valori centrali della sfera personale dell'individuo: a) la formazione del *consenso* individuale e la comunicazione delle idee; b) l'autonomia e la capacità di *autodeterminarsi* dell'individuo; c) l'essenza dell'uomo, la sua *dignità*. Tutti e tre questi aspetti si trovano al centro del sistema di valori su cui si basano gli strumenti internazionali di tutela dei diritti umani.

3.1. L'incidenza sulla formazione del consenso individuale e la comunicazione delle idee

Per quanto riguarda il primo aspetto, le tecnologie in esame pongono complesse sfide alla formazione e alla comunicazione del *consenso individuale*, entrambe indispensabili per la rivendicazione e la protezione di qualsiasi diritto umano, sia esso civile, politico, economico, sociale o culturale. A ben vedere, la distorsione delle informazioni, la mancanza di processi trasparenti, il controllo sulle informazioni personali comportano in misura crescente la diluizione del nostro consenso individuale al punto tale da mettere in pericolo le stesse fondamenta del modo con cui affermiamo i nostri diritti umani e riteniamo che gli altri siano responsabili della loro violazione. Esempio plastico di quanto andiamo dicendo è rappresentato dallo scandalo *Facebook/Cambridge Analytica*. I fatti sono noti. Un ricercatore dell'Università di Cambridge aveva sviluppato un *App* da far girare in Facebook e che attraverso la somministrazione di un sondaggio riusciva a produrre profili psicologici e di previsione del comportamento degli utenti, basandosi sulle attività da questi svolte online. L'*App* fu scaricata da centinaia di migliaia di utenti di Facebook ed essa riuscì maliziosamente a memorizzare dati sensibili di vario tipo di circa 50 milioni di profili Facebook. Il ricercatore condivise (in violazione dei termini d'uso di Facebook) queste informazioni con *Cambridge Analytica* una società specializzata nel raccogliere dai social network dati sui loro utenti per creare profili di ogni utente da utilizzare attraverso un sistema di 'microtargeting comportamentale' sviluppato dall'impresa in questione. Un sistema, insomma, destinato a sviluppare messaggi pubblicitari altamente personalizzati per ogni singola persona ed in grado di far leva non solo sui gusti, ma anche sulle emozioni degli utenti. I dati raccolti erano in grado, pertanto, di creare profili psicologici dei titolari dei dati: questi profili abbinati al sistema di pubblicità

personale sarebbero stati utilizzati a scopi di propaganda politica per condizionare cento campagne elettorali in oltre trenta Stati¹⁴. Lo scandalo *Facebook/Cambridge Analytica*, con i rischi da esso palesati di distorsione dell'informazione di massa, di violazione della *privacy* per milioni di persone in tutto il mondo, mette in discussione il diritto dei cittadini a partecipare liberamente alla gestione degli affari pubblici e a votare in elezioni che garantiscano la libera espressione della volontà degli elettori così come garantito a livello universale dall'art. 25 del Patto sui diritti civili e politici, e a livello regionale europeo dall'art. 3 del Protocollo No. 1 della CEDU¹⁵.

Se le distorsioni dell'informazione, come quelle esaminate in relazione allo scandalo *Facebook/Cambridge Analytica*, mettono in discussione l'autentica natura e l'effettiva portata del consenso prestato dagli individui all'utilizzo di sistemi di *machine learning* e di intelligenza artificiale, l'altro lato della medaglia è rappresentato dal deficit di trasparenza circa come le imprese dell'*High-tech* utilizzano e condividono i dati degli utenti. In effetti nonostante il fatto che la comunicazione volontaria delle politiche in materia di trasparenza sia diventata uno standard del settore tecnologico¹⁶, tuttavia, continua a sussistere una diversità di approcci alla trasparenza in relazione all'utilizzo di algoritmi e di tecnologie di intelligenza artificiale, e continuano a sussistere differenze di tipo regolamentare e giurisdizionale nei diversi ordinamenti nazionali. Resta soprattutto aperta la questione relativa al se gli individui riescano a rilasciare effettivamente e realmente un consenso, consapevole, libero e informato all'utilizzo, condivisione o al trattamento dei loro dati da parte delle imprese del settore tecnologico quando si relazionano con le tecnologie digitali. A questo proposito l'Unione Europea sembra essere sempre più all'avanguardia a livello globale nel cercare di garantire siffatto consenso consapevole, informato e libero. Le *Ethics Guidelines for Trustworthy Artificial Intelligen-*

ce adottate nel 2019 dall'*High-Level Expert Group on Artificial Intelligence*¹⁷, infatti, individuano sette condizioni affinché le tecnologie fondate su algoritmi e simili possano definirsi 'affidabili' (*trustworthy*). Si tratta di assicurare 1) il controllo e supervisione da parte dell'uomo; 2) la solidità tecnica e sicurezza; 3) il rispetto della privacy e della *governance* dei dati; 4) la trasparenza; 5) la salvaguardia della diversità, della non discriminazione e dell'equità; 6) il benessere sociale e ambientale; 7) la responsabilità.

3.2. L'incidenza sull'autonomia e sulla capacità di autodeterminarsi dell'individuo

Per quanto attiene al secondo valore, quello dell'*autonomia* e della *capacità di autodeterminarsi* dell'uomo, tali valori costituiscono come evidenziato, in un recente scritto, dal Presidente della Corte europea dei diritti dell'uomo il "fondamento morale" della stessa nozione di *rule of law* in quanto funzionali all'esclusione di qualsiasi forma di arbitrio da parte dei governi e dei poteri, sia pubblici che privati¹⁸. Ebbene i fenomeni di c.d. *autoritarismo digitale*, in cui le tecnologie algoritmiche e di intelligenza artificiale vengono utilizzate come strumento di controllo sociale e di sorveglianza di polizia, in funzione di un 'rimodellamento delle forme di repressione'¹⁹ non fanno altro che mettere in crisi l'autonomia personale e la capacità di autodeterminarsi dell'individuo e mettono quindi "sotto pressione" il funzionamento dello stesso principio di *rule of law*²⁰. Il riferimento va ai sistemi di riconoscimento facciale, a quelli automatici di riconoscimento delle emozioni, alla sorveglianza digitalizzata, ma anche alle tecniche di disinformazione, all'utilizzo di *fake news*, cui tutti siamo chi in misura maggiore, chi in misura minore, esposti. È una prassi, questa passata in rassegna, che può costituire in assenza di meccanismi di bilanciamento e controllo, un pericoloso e subdolo

meccanismo di interferenza nei diritti fondamentali della persona umana.

È necessario, insomma, che le convenzioni e gli altri strumenti internazionali sui diritti umani – e gli obblighi che derivano da tali strumenti – guidino gli Stati e le loro azioni in materia di cooperazione digitale, e fare in modo che i diritti umani ricevano applicazione per garantire che le tecnologie digitali nuove ed emergenti non causino lacune di tutela. Il punto centrale è: in che modo fare ciò?

Ora, a noi sembra che superato, e da tempo, ogni dubbio relativamente al se il diritto internazionale dei diritti umani possa e debba ricevere applicazione all'era dell'intelligenza artificiale, la risposta alla domanda di cui sopra passa attraverso il riconoscimento che quando governi autocratici violano i diritti civili e politici attraverso misure di repressione digitale, oppure quando violano i diritti economici, sociali e culturali condizionando l'erogazione dei servizi pubblici (che si tratti del diritto al più alto livello raggiungibile di salute fisica e mentale, del diritto alla sicurezza sociale, del diritto all'istruzione, del diritto a partecipare alla vita culturale, del diritto a un adeguato tenore di vita) a meccanismi di controllo sociale non trasparenti e discriminatori, nulla di 'nuovo' emerge rispetto alle forme .. 'più tradizionali' di intrusione nella autonomia personale dell'individuo. Il problema va risolto, allora, nella logica della *responsabilità* dello Stato di *rispettare, proteggere e realizzare* i diritti umani sanciti nelle convenzioni internazionali²¹. Tale responsabilità scaturisce dal dovere degli Stati di regolamentare le attività degli enti economici privati – anche quelli che sviluppano e utilizzano tecnologie digitali – che si trovano sotto il loro controllo e/o giurisdizione anche quando queste attività dispieghino effetti in Paesi terzi. Con riferimento al settore dei diritti economici, sociali e culturali, questa impostazione è stata materialmente applicata dal Comitato per i diritti economici, sociali

e culturali nel Commento generale n. 24 dedicato specificamente agli obblighi che dal Patto del 1966 discendono sugli Stati contraenti in relazione alle attività delle imprese²². Il Comitato, in effetti, ha evidenziato come gli Stati contraenti siano obbligati ad adottare le misure necessarie per regolare le attività delle imprese che possono incidere negativamente sui diritti economici, sociali e culturali, e in particolare per evitare la discriminazione di lavoratori e migranti, quella sessuale, quella religiosa o razziale e le altre forme di discriminazione. Il Comitato ha sottolineato che l'obbligo di *rispettare* i diritti economici, sociali e culturali risulta violato "quando gli Stati parte attribuiscono priorità agli interessi commerciali delle imprese rispetto alle garanzie previste dal Patto senza alcuna giustificazione, o quando perseguono politiche che influiscono negativamente su tali diritti"²³. L'obbligo di *proteggere*, invece, comporta secondo il Comitato che gli Stati contraenti "devono prevenire effettivamente qualsiasi violazione dei diritti economici, sociali e culturali che possa verificarsi nel quadro delle attività commerciali". Secondo il comitato, ciò richiede che gli Stati contraenti "adottino misure legislative, amministrative, educative e altre misure appropriate per garantire un'effettiva protezione contro le violazioni dei diritti del Patto collegate alle attività delle imprese e che forniscano alle vittime di tali violazioni l'accesso a delle vie di rimedio effettive"²⁴. L'obbligo di realizzare, infine, impone agli Stati contraenti di adottare le misure necessarie, "nel massimo delle risorse disponibili, per facilitare e promuovere il godimento dei diritti sanciti dal Patto e, in alcuni casi, per fornire direttamente beni e servizi essenziali a tale godimento"²⁵.

Di particolare rilevanza ai fini della nostra analisi è, inoltre, il fatto che il Comitato non abbia esitato a porre in evidenza come "gli obblighi degli Stati contraenti ai sensi del Patto non si fermano ai loro confini territoriali" e che essi sono tenuti ad "adottare le misure necessarie per prevenire le violazioni dei

diritti umani all'estero da parte di società domiciliate nel loro territorio e/o sottoposte alla loro giurisdizione (sia che sia costituite in base al loro diritto interno, sia che abbiano la loro sede legale, l'amministrazione centrale o il luogo principale di attività sul territorio nazionale), senza violare la sovranità o diminuire gli obblighi degli Stati ospitanti ai sensi del Patto²⁶.

Nonostante questo crescente riconoscimento delle *responsabilità* degli Stati, resta il punto fondamentale di come garantire delle vie di rimedio effettive alle vittime che abbiano visto la propria autonomia personale e la propria capacità di autodeterminarsi essere 'comprese' da parte di regimi autocratici che usano le tecnologie digitali non solo contro i propri cittadini o le persone presenti sul proprio territorio, ma anche contro i presunti nemici dello Stato all'estero. Le vie di rimedio, in effetti, sono pur sempre ancorate all'ordinamento nazionale dello Stato in questione e, anche a causa della reticenza con cui normalmente i vari colossi del settore tecnologico affrontano le questioni di trasparenza ed il confronto con le autorità di regolamentazione di ordinamenti terzi, per le vittime di violazioni dei diritti umani causate dalle forme di repressione basata sull'utilizzo di tecnologie digitali, ottenere un ristoro resta molto spesso una chimera.

3.3. L'incidenza sul valore della dignità umana

Passiamo al terzo valore 'toccato' dal *machine learning* e dalle altre tecnologie digitali, il principio di *dignità umana*, principio considerato, come è noto, la *pietra angolare* della tutela internazionale dei diritti umani. Nella misura in cui l'impiego delle tecnologie digitali diventa un mezzo per *strumentalizzare* l'essere umano, esso rappresenta un'intrusione nel principio di dignità umana, intesa come l'uguale valore morale che deve essere riconosciuto ad *ogni* essere umano. Mi riferisco alla capacità, tipi-

camente inerente a siffatte tecnologie, di rimuovere, in misura più o meno maggiore, un certo grado di potestà decisionale dall'operatore umano, per attività che erano state fino ad oggi interamente realizzate e *controllate* dall'uomo, e a trasferirle a processi autonomizzati che sono in grado di funzionare senza un costante controllo umano²⁷. Questo può rendere ridondanti – se non addirittura irrilevanti – le capacità cognitive e quelle di giudizio intrinsecamente connaturate all'uomo, come apprendere, parlare, valutare, ecc. La prassi ha già messo in luce i pericoli che dal punto di vista della protezione dei diritti umani sono collegati al venire meno delle competenze professionali dei lavoratori in specifici settori caratterizzati da alta automattizzazione (con l'enorme numero di disoccupati che questo processo potrà creare), oppure dall'utilizzo di piattaforme di lavoro digitali basate su algoritmi in grado di riprodurre pregiudizi sociali (con rischio di discriminazioni e *bias*.)²⁸, o, infine, nell'esercizio di funzioni governative come l'amministrazione della giustizia²⁹. Il rischio insomma è che tale processo di strumentalizzazione possa alterare il significato normalmente attribuito alla parola 'umanità' e la stessa valutazione circa il livello di tutela da attribuire alle dimensioni della dignità umana, 'intaccando' il mantra dell'*inviolabilità* di tale principio.

Insomma, ciò che si rende necessario è un approccio cauto al processo di sviluppo e utilizzo delle tecnologie digitali. Sebbene, esse siano in grado di sopravanzare l'effettiva capacità del diritto e delle autorità di regolamentazione di prevedere e anticipare i rischi per i diritti umani (piuttosto costringendo il diritto ad inseguire secondo una logica *reattiva* alla regolamentazione in tali materie), è opportuno, invece, che Stati e legislatori cerchino in via *preventiva* di esercitare le funzioni regolamentari ad essi spettanti mediante la previsione delle esternalità negative, come l'impatto sui diritti umani, che possono scaturire dal *machine learning*, dall'intelligenza artificiale e dalle altre tec-

nologie digitali che si intende disciplinare. Occorre, in altre parole, uno *human rights-based approach* che sia applicato attraverso il diritto in tutte le fasi di sviluppo e utilizzo delle tecnologie. La notizia positiva è che sul punto si sta consolidando, a mio giudizio, un consenso piuttosto diffuso come tra l'altro dimostrato da diversi documenti internazionali ed in modo particolare, con riferimento al contesto europeo, da quelli adottati in ambito di Unione europea³⁰ e di Consiglio d'Europa³¹.

4. Responsabilità e diritti umani nella società degli algoritmi

La terza chiave di lettura, infine, attiene come anticipato poco più sopra all'allargamento dell'istituto della *responsabilità* nel diritto internazionale. Ci riferiamo in modo particolare all'emersione di nuove *forme di responsabilità* dei diversi attori che operano nella contemporanea società degli algoritmi. Si tratta di un tema su cui abbiamo altre volte avuto occasione di soffermarci e che non è possibile per motivi di spazio affrontare in modo approfondito in questa sede³². Basti qui solo sottolineare che l'avvento dei sistemi di *machine learning*, basati sulla tecnologia degli algoritmi e sull'intelligenza artificiale, può contribuire a modificare, e anzi sta già modificando, il modo con cui il diritto si forma, opera e viene applicato. Ciò vale, a nostro avviso, anche in relazione alla nozione di responsabilità applicata nel diritto internazionale, nel senso che, come suggerito dal processo di cristallizzazione di un sistema giuridico internazionale in materia di imprese e diritti umani, il riallineamento degli squilibri di *governance* (i c.d. *governance gaps*) che sempre più caratterizzano il sistema delle relazioni internazionali, non può più passare esclusivamente attraverso l'istituto della responsabilità internazionale dello Stato, ma deve altresì prendere necessariamente in considerazione anche le responsabilità 'complementari' e 'condivise'³³ degli altri attori che partecipano a

tali processi e contribuiscono a condizionare la protezione dei diritti umani, oppure a violarli apertamente. A nostro giudizio, insomma, accanto al regime sulla responsabilità internazionale dello Stato, che deve effettuare le sue scelte di *policy* in materia di tecnologie digitali senza rinunciare ad assicurare la protezione dei diritti umani degli individui sottoposti alla propria giurisdizione (con gli obblighi, collegati a tale responsabilità, di prevenzione, di informazione e di trasparenza), e accanto alla responsabilità dell'individuo applicata nell'ambito del diritto penale internazionale in relazione alle *gross violations* dei diritti umani, ... *tertium datur!* È in via di consolidamento un regime internazionale sulla *responsabilità delle imprese* in materia di diritti umani³⁴ che opera, accanto ai primi due regimi di responsabilità internazionale, e che impone alle imprese, con riferimento specifico alla salvaguardia di tali valori avvertiti come fondamentali per la comunità internazionale, di rispettarli e di adottare a tal fine processi di *due diligence* in materia di diritti umani per individuare, prevenire e mitigare i rischi di un impatto negativo sui diritti umani derivante dalle loro attività. Tale responsabilità delle imprese di rispettare i diritti umani si applica a tutti gli enti del settore privato e, per quanto attiene il tema del presente lavoro, si estende ovviamente anche alle imprese del settore tecnologico le cui operazioni economiche sono dedite allo sviluppo o all'utilizzo delle tecnologie digitali.

5. Conclusioni

L'utilizzo di tecnologie digitali, come l'impiego di algoritmi predittivi, l'intelligenza artificiale, il *machine learning*, le tecniche di riconoscimento facciale, è in costante aumento. La narrativa normalmente associata a questo fenomeno tende a mettere in luce il potenziale di queste tecnologie per la crescita economica, lo sviluppo, il benessere delle comunità di persone, ma non

sempre viene riposta sufficiente enfasi sul potenziale impatto negativo sulla società e sui principi che governano la società come la *rule of law* ed i diritti umani. Solo più recentemente, a causa delle pressioni provenienti da cittadini, dalla società civile e da altri gruppi vulnerabili, istituzioni di governo e Organizzazioni internazionali hanno iniziato a prendere in considerazione le sfide che tali tecnologie pongono per la tutela dei diritti umani. Ciò ha comportato uno spostamento dell'attenzione sulla questione volta a stabilire se e come regolamentarne l'utilizzo, e soprattutto quali attori debbano assumersi relativi doveri e responsabilità. A tal fine un crescente consenso si sta consolidando intorno alla necessità che il quadro normativo di riferimento per le tecnologie digitali richieda uno *human rights-based approach* e debba essere costruito intorno a due principi: quello della *centralità dell'uomo* e quello di *responsabilità*³⁵. Per quanto riguarda il primo principio, la centralità dell'uomo rinvia alla necessità che sia assicurato un *controllo* effettivo sulle potenziali violazioni dei diritti umani derivanti dalle tecnologie digitali, il che implica che il loro utilizzo non deve violare i diritti fondamentali garantiti dalle Costituzioni e dagli standard internazionali. La centralità dell'uomo implica, insomma, che tali tecnologie debbano rimanere sotto il controllo umano, anche nelle circostanze in cui la digitalizzazione della tecnologia consenta di adottare decisioni indipendentemente da uno specifico intervento umano. Il criterio del controllo umano, si traduce pertanto, con riguardo alle imprese che sviluppano le tecnologie digitali oppure che ne fanno uso per i propri scopi commerciali, nella necessità di un approccio proattivo ai potenziali impatti negativi derivanti dall'utilizzo di questa tecnologia volto a prevenire le violazioni che possano scaturirne per la garanzia dei diritti umani. Tale approccio preventivo è perfettamente coerente con l'applicazione di processi di *due diligence* aziendale in materia di diritti umani.

Per quanto riguarda il secondo principio – quello di responsabilità – occorre garantire l'esistenza di sistemi di *accountability* efficaci per monitorare e, ove necessario, affrontare efficacemente qualsiasi impatto negativo sui diritti umani derivanti dalle tecnologie digitali. Ciò porta a considerare come oggigiorno le violazioni dei diritti umani si verificano sempre più frequentemente in un quadro caratterizzato da azioni *congiunte* e *coordinate*, piuttosto che indipendenti, da parte di diversi soggetti – pubblici e privati – che, attraverso i loro comportamenti, contribuiscono in vario modo ad assicurare, o meno, la tutela dei diritti umani. È esattamente in questa prospettiva di analisi che l'avvento della società dell'intelligenza artificiale non ha fatto altro che accelerare ulteriormente un processo già in atto e che sta originando “un cambiamento paradigmatico in cui il potere pubblico non è più l'unica fonte di preoccupazione per il rispetto dei diritti fondamentali e la tutela della democrazia”³⁶.

Note di chiusura

¹ Il presente lavoro è pubblicato grazie al supporto del progetto SERICS (SEcurity and RIghts in the CyberSpace - PE00000014) realizzato nell'ambito del Piano Nazionale di Ripresa e resilienza del MUR, finanziato dal programma NextGenerationEU dell'UE.

² Basti pensare alla letteratura addensatasi negli anni '70 del secolo trascorso intorno ad uno dei primi studi circa i rapporti tra sviluppo scientifico-tecnologico e strutture economico-sociali, il c.d. Rapporto Richta dal nome del suo autore (cfr. R. RICHTA, *Civiltà al bivio: le conseguenze umane e sociali della rivoluzione scientifica e tecnologica*, Milano, 1972). Nella prospettiva dei diritti fondamentali ci limitiamo a segnalare, in una letteratura praticamente sconfinata, M. CARTABIA, *In tema di "nuovi" diritti*, in *Scritti in onore di F. Modugno*, Napoli, 2011, I, 643; S. RODOTÀ, *Il mondo nella rete. Quali diritti, quali vincoli*, Roma-Bari, 2014; O. POLLICINO, *Judicial Protection of Fundamental Rights on the Internet*, Hart Publishing, Oxford, 2021.

³ Cfr. T. Van Ho, *COVID-19 Symposium: A Time to Kill 'Business as Usual' - Centring Human Rights in a Frustrated Economy (Part 1)*, in *Opinio Juris*, 2 aprile 2020.

⁴ Cfr. O. POLLICINO, *Costituzionalismo, privacy e neurodiritti*, in *Medialaws*, 2021, pp. 9-16, in part. p. 11.

⁵ Cfr. Consiglio dei diritti umani, *Report of the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie. Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, UN Doc. A/HRC/17/31 del 21 marzo 2011.

⁶ Non è possibile una analisi puntuale del contenuto dei Principi Guida. Ci limitiamo a rinviare a R. MARES (ed.), *The UN Guiding principles on business and human rights: foundations and implementations*, Leiden, 2012; F. MARRELLA, *I Principi Guida dell'ONU sulle imprese e i diritti umani del 2011 e l'accesso ai rimedi tramite gli strumenti di diritto internazionale privato europeo: una valutazione critica*, in (a cura di) M. CASTELLANETA, F. VESSIA, *La responsabilità sociale d'impresa tra diritto societario e diritto internazionale*, Napoli, 2019, pp. 315-337. Sia consentito anche il rinvio a M. FASCIGLIONE, *I Principi guida ONU su impresa e diritti umani e il consolidamento del regime internazionale in materia di settant'anni dalla Dichiarazione universale*, in (a cura di) G. CATALDI, *I diritti umani a settant'anni dalla Dichiarazione universale delle Nazioni Unite*, Napoli, 2019, pp. 93-128; ID., *Per uno studio dei Principi Guida ONU su imprese e diritti umani*, in (a cura di) M. FASCIGLIONE, *I Principi Guida su Imprese e Diritti Umani*, Roma, 2020, pp. 35-58.

⁷ Cfr. i Principi 13 e 17.

⁸ Cfr. Principio 15.

⁹ Cfr. Alto commissariato sui diritti umani, *The Corporate Responsibility to Respect Human Rights: An Interpretative Guide*, Ginevra, 2012, p. 4.

¹⁰ In Europa, la *privacy by design* e la *privacy by default* sono elementi fondamentali del regime giuridico di protezione dei dati dall'art. 25 del GDPR (Regolamento 2016/679/UE del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE). In base a tale disposizione, i responsabili del trattamento devono mettere in atto misure tecniche e organizzative adeguate e le garanzie necessarie, volte ad attuare i principi di protezione dei dati in modo efficace e a tutelare i diritti e le libertà degli interessati (cfr. anche *European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, adottato il 13 novembre 2019, par. 12 e seguenti). In materia v. A.E. WALDMAN, *Data Protection by Design? A Critique of Article 25 of the GDPR*, in *Cornell International Law Journal*, 2020, Vol. 53, No. 1, p. 147-167.

¹¹ Cfr. Proposta di regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM(2021) 206 final, del 21 aprile 2021.

¹² Abbiamo avuto modo di analizzare maggiormente in dettaglio tale aspetto in M. FASCIGLIONE, *Business and Human Rights in the Age of Artificial Intelligence*, in *Federalismi.it*, 2/2022, pp. 164-183, p. 177 ss.

¹³ Cfr. Commissione europea, *Proposal for a Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937*, COM(2022)71 final, del 23 febbraio 2022.

¹⁴ Cfr. <https://qz.com/1239762/cambridge-analytica-scandal-all-the-countries-where-scl-elections-claims-to-have-worked>.

¹⁵ Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, Roma, 1950. In materia v. M. STARITA, *Art. 3*, in (a cura di) S. BARTOLE, P. DE SENA, V. ZAGREBELSKI, *Commentario breve alla Convenzione europea dei diritti dell'uomo*, Padova, 2012, pp. 832-857.

¹⁶ Ruolo pionieristico è stato svolto da Google quando, nel 2010, essa ha pubblicato il suo *Transparency Report*, in cui ha reso note le sue restrizioni circa i contenuti e le misure relative alla sicurezza e alla privacy (cfr. <https://transparencyreport.google.com/about>).

I diritti umani nell'era degli algoritmi e dell'intelligenza artificiale

¹⁷ Cfr. High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy Artificial Intelligence*, 2019, consultabile al sito <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

¹⁸ R. SPANO, *The rule of law as the lodestar of the European Convention on Human Rights: The Strasbourg Court and the independence of the judiciary*, in *European Law Journal*, 2021.

¹⁹ Cfr. S. FELDSTEIN, *How Artificial Intelligence Is Reshaping Repression*, in *Journal of Democracy*, 2019, Volume 30, n. 1, pp. 40-52.

²⁰ Cfr. O. POLLICINO, *Costituzionalismo, privacy e neurodiritti*, cit., p. 10.

²¹ Come noto la tripartizione degli obblighi scaturenti dalle norme sui diritti umani in obblighi di rispettare, proteggere e realizzare, è stata proposta in dottrina da H. SHUE, *Basic Rights: Subsistence, Affluence, and US Foreign Policy*, Princeton, 1980, p. 52, ripresa da A. EIDE, *The International Human Rights System*, in (Eds) A. Eide et al, *Food as a Human Rights*, Tokyo, 1984, p. 152 ss, e materialmente recepita dal Comitato sui diritti economici, sociali e culturali nella sua, oramai consolidata, prassi.

²² Comitato sui diritti economici, sociali e culturali, *General comment No. 24 (2017) on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities*, UN Doc. E/C.12/GC/24, del 10 agosto 2017.

²³ Comitato sui diritti economici, sociali e culturali, *General comment No. 24 (2017)*, cit. par. 12.

²⁴ Comitato sui diritti economici, sociali e culturali, *General comment No. 24 (2017)*, cit. par. 14.

²⁵ Comitato sui diritti economici, sociali e culturali, *General comment No. 24 (2017)*, cit. par. 23.

²⁶ Comitato sui diritti economici, sociali e culturali, *General comment No. 24 (2017)*, cit. par. 26.

²⁷ Per una analisi in materia sia pure in una prospettiva differente v. P. DE SENA, *Dignità umana in senso oggettivo e diritto internazionale*, in *Dir. um. e dir. int.*, 2017, pp. 573-586, che si sofferma sul ruolo della dignità umana in senso oggettivo come *ratio* dell'indisponibilità del corpo umano, a fini commerciali, in ambito europeo.

²⁸ Si consideri ad esempio il caso dell'algoritmo utilizzato dalla società *Deliveroo Italia* per gestire il sistema di prenotazione digitale delle sessioni di lavoro dei *rider* impiegati dall'azienda. L'algoritmo, infatti, che doveva stabilire

la priorità in base alla quale ai *rider* venivano assegnati i turni di lavoro, era stato concepito in modo da penalizzare i lavoratori che si assentavano ingiustificatamente dalle sessioni di lavoro assegnate, ma non effettuava alcuna differenziazione per le situazioni di astensione legittima, come l'esercizio del diritto di sciopero! Il caso ha originato quindi una vicenda giudiziaria con il Tribunale di Bologna che ha condannato la società per condotta discriminatoria in relazione al funzionamento dell'algoritmo nella piattaforma digitale (cfr. Trib. di Bologna, *Filcams Cgil Bologna, Nidil Cgil Bologna, Filt Cgil Bologna c. Deliveroo Italia S.r.l.*, ord. 31 dicembre 2020).

²⁹ In materia, con riferimento all'indipendenza dei giudici cfr. G.M. RUOTOLO, *The End of Dormancy. Judicial Independence through Data-Driven Knowledge, Open Data and Artificial Intelligence from an International and European Law Perspective*, in (eds.) S. SHETREET, H. CHODOSH, E. HELLAND, *Challenged Justice. In pursuit of Judicial Independence*, Leiden/Boston, 2021, p. 59 ss.

³⁰ Sul punto, si veda, *inter alia*: Consiglio europeo, *Presidency conclusions. The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, del 21 ottobre 2020, par. 10 e ss., che enfatizza la necessità di “[a] fundamental rights-based approach to AI”; Commissione europea, *Libro Bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 final, del 19 febbraio 2020, p. 2, secondo cui “qualsiasi quadro regolamentare per l'IA deve essere fondato sui valori fondamentali dell'Unione” incluso il rispetto per i diritti umani. Il tema è poi ampiamente trattato negli studi compiuti dall'Agenzia per i diritti fondamentali dell'Unione europea (v. FRA, *Getting the future right – Artificial intelligence and fundamental rights*, del 14 dicembre 2020; FRA, *Fundamental Rights Report 2022*, 8 giugno 2022p. 17 e ss.).

³¹ Il tema di uno *human rights-based approach* allo sviluppo e utilizzo delle tecnologie digitali è presente in tutti i documenti prodotti dall'*Ad hoc Committee on Artificial Intelligence* del Consiglio d'Europa e che sono consultabili al sito web www.coe.int/en/web/artificial-intelligence/cahai.

³² V. ad es, M. FASCIGLIONE, *L'emergenza COVID-19 e l'attuazione della responsabilità delle imprese di rispettare i diritti umani nel diritto internazionale*, in *Quaderni di SIDIBlog*, 2020 (2021), pp. 25-45.

³³ Le implicazioni teoriche e pratiche delle *shared responsibilities* di imprese e di Stati nel diritto internazionale sono analizzate da: A. NOLLKAEMPER, D. JACOBS, *Shared Responsibility in International Law: A Conceptual Framework*, in *Michigan Journal of International Law*, 2013, p. 359 ss.; M. KARAVIAS, *Shared Responsibility and Multinational Enterprises*, in *Netherlands International Law Review*, 2015, p. 91 ss.

I diritti umani nell'era degli algoritmi e dell'intelligenza artificiale

³⁴ I segnali del consolidamento di un siffatto regime sono, a nostro giudizio, molteplici. Non si tratta solo dell'affermazione di standard internazionali non vincolanti in materia di imprese e diritti umani, come ad es. i menzionati Principi guida onusiani del 2011, e gli altri standard internazionali esistenti in materia, ma anche del processo di emersione di regimi normativi che, tanto a livello di ordinamenti nazionali degli Stati, quanto a livello di ordinamenti regionali (come quello europeo), sono volti a fissare obblighi di *due diligence* in materia di diritti umani per le imprese.

³⁵ Entrambi i principi sono stati più volte evocati dalle istituzioni internazionali e da altri organismi di regolamentazione. Si veda, tra gli altri, FRA, *Getting the future right*, cit., pp. 8-10.

³⁶ O. POLLICINO, G. DE GREGORIO, *Constitutional Democracy in the Age of Algorithms: The Implications of Digital Private Powers on the Rule of Law in Times of Pandemics*, in *MediaLaws*, 11 novembre 2020.

La valutazione d’impatto sui diritti fondamentali dei minori di età nell’ambiente digitale. Riflessioni a margine della proposta di direttiva relativa alla *due diligence* delle imprese ai fini della sostenibilità e del *Digital Services Act*

ILARIA GARACI

Sommario: 1. L’evoluzione della responsabilità sociale di impresa. Verso la vincolatività della *due diligence* in materia di diritti umani e ambiente. - 2. La *due diligence* nel contesto digitale in base agli standard internazionali sui diritti umani relativi ai minori. - 3. La *due diligence* sui diritti dei minori nell’ambito della nuova strategia europea per il mercato unico digitale. - 3.1. La “dipendenza da videogiochi” e la “dipendenza da Internet” quali minacce ai diritti umani del minore. - 4. I diritti dei minori nell’ambito della proposta di direttiva relativa alla *due diligence* delle imprese ai fini della sostenibilità.

1. L’evoluzione della responsabilità sociale di impresa. Verso la vincolatività della *due diligence* in materia di diritti umani e ambiente.

La crisi economica e sociale e l’aggravarsi dello scenario climatico inducono da tempo riflessioni sulla struttura dell’attuale sistema capitalistico¹, focalizzato sul principio della “massimizzazione del profitto”², verso direzioni in grado di mitigare i crescenti rischi ambientali, eliminare le violazioni dei diritti umani e ridurre le ineguaglianze sociali. Ci si domanda quale sia la funzione della grande impresa azionaria all’interno del mercato e, in particolare, se quest’ultima possa, o piuttosto debba, assume-

re un ruolo sociale più inclusivo e, in applicazione del principio di sussidiarietà “orizzontale”³, farsi carico del perseguimento di scopi sostenibili⁴.

Il tema della responsabilità sociale di impresa (*Corporate Social Responsibility*)⁵ nasce nella prospettiva di una possibile rilevanza degli interessi degli *stakeholders* (dipendenti, consumatori, fornitori, comunità di riferimento, ecc.) nella definizione delle regole di gestione dell'impresa⁶ e si sviluppa attraverso un approccio essenzialmente volontaristico, inizialmente concentrato più sulla promozione di contributi positivi che un'impresa può offrire alla comunità, piuttosto che sulla prevenzione degli effetti negativi delle sue esternalità⁷.

Negli ultimi anni, in considerazione della maggiore consapevolezza delle criticità ambientali, sociali e finanziarie e della crescente rilevanza del principio dello sviluppo sostenibile⁸, sul piano delle politiche dell'Unione europea e internazionale⁹, attraverso la definizione degli SDG (*Sustainable Development Goals*)¹⁰, il dibattito si è arricchito di nuove riflessioni. Si prospetta una concezione rinnovata della *Corporate Social Responsibility* (CSR), cui si affianca o si sostituisce l'acronimo ESG (*Environmental Social Governance*), che si fonda sulla rilevanza dell'interesse economico complessivo dell'impresa e dei soci nel lungo periodo, reso possibile grazie anche alle politiche di sostenibilità sociale e ambientale¹¹, finalizzate essenzialmente a ridurre i rischi di impatto sull'ambiente e sui diritti umani che derivano dall'attività di impresa. Si avverte inoltre l'esigenza di responsabilizzare maggiormente le imprese con strumenti normativi. Di qui le prescrizioni in materia di divulgazione non finanziaria¹², le quali, benché si limitino a prevedere meri obblighi di trasparenza¹³, contribuiscono certamente a creare, in forza del principio del *comply or explain*, una positiva competizione tra le imprese sui temi ESG per attrarre gli interessi degli investitori¹⁴, soprattutto di quelli responsabili, disposti a riconoscere un premio alle aziende maggiormente attente ai temi di sostenibilità sociale ed ambientale. La re-

sponsabilità sociale d'impresa è, tuttavia, ancora caratterizzata da un approccio volontaristico, che trova fondamento nei Principi guida delle Nazioni Unite su imprese e diritti umani (UNGP)¹⁵ e in altri documenti¹⁶, che prevedono obblighi internazionali a protezione dei diritti umani e dell'ambiente, rivolti tuttavia agli Stati e pertanto non vincolanti per le imprese. Tali iniziative hanno certamente indotto molte aziende, nella prassi, ad adottare codici di condotta¹⁷ e ad elaborare politiche e strategie sostenibili di lungo periodo. Al riguardo si sottolinea l'importante ruolo assunto dal diritto contrattuale¹⁸, in considerazione del crescente impiego, negli accordi commerciali internazionali, delle c.d. clausole di sostenibilità¹⁹, con cui le parti assumono reciproci obblighi in relazione agli ESG, richiama, al fine di renderli vincolanti, i codici di condotta, sia pure con il limite della loro non rilevanza esterna²⁰.

L'interrogativo che a questo punto si pone, sotto il profilo di politica legislativa, è se proseguire con l'approccio volontaristico e competitivo delle scelte di responsabilità sociale²¹, lasciando quindi spazio alla discrezionalità dei giudici in caso di condotte abusive delle imprese che impattano sui diritti umani e sull'ambiente²², ovvero seguire la strada dell'azione normativa attraverso l'imposizione degli scopi sostenibili²³, come del resto avvenuto in alcuni Stati membri, attraverso norme in materia di dovuta diligenza²⁴ e in altri paesi, che hanno adottato misure ancora più rigorose²⁵.

L'Unione Europea, nella prospettiva di armonizzare le legislazioni già esistenti, spinta inoltre dall'aggravarsi dello scenario climatico e dalle crescenti preoccupazioni riguardo le violazioni dei diritti umani da parte delle imprese – specialmente quando le catene del valore di alcune di esse si estendono in paesi caratterizzati da sistemi giuridici o meccanismi di applicazione della legge deboli – con la recente proposta di direttiva in materia di sostenibilità²⁶ ha optato per la strada dell'azione normativa al fine di dirigere la condotta d'impresa al rispetto dei diritti umani, internazionalmente riconosciuti, e dell'ambiente. La propo-

sta è volta infatti ad introdurre un obbligo di *due diligence* per le imprese di grandi dimensioni, in relazione ai diritti umani e all'ambiente, non solo all'interno dell'Unione europea, ma anche lungo le catene di approvvigionamento delle imprese europee a livello globale. Le imprese sarebbero pertanto obbligate a compiere un'analisi preventiva dei rischi, adottando misure specifiche, al fine di prevenire o comunque ridurre gli effetti negativi della loro attività sull'ambiente e sui diritti umani, ponendo la loro attenzione sull'intero processo produttivo dell'impresa.

Alla previsione dell'obbligo di compiere la *due diligence* si accompagna un importante sistema di *enforcement*, in chiave preventiva e risarcitoria, che attribuisce una legittimazione ad agire in capo a tutti i titolari di interessi direttamente incisi dalla condotta dell'impresa o che lamentino una potenziale lesione da parte della stessa.

La proposta di direttiva, andrebbe ad integrare, come specificato nelle premesse stessa della proposta, il contesto normativo dell'Unione europea, con la prospettiva di “*delineare un quadro trasparente e prevedibile che aiuti le società dell'UE, in tutti i settori dell'economia, a valutare e a gestire i rischi e gli impatti per la sostenibilità in relazione ai rischi fondamentali per i diritti umani e l'ambiente, anche nelle rispettive catene del valore.*”

Proprio in vista di tale coordinamento si svolgeranno alcune considerazioni, con riguardo alla rilevanza dei diritti dei minori di età nei processi di *due diligence* delle imprese, in particolare in quelle che operano nel contesto digitale.

2. La *due diligence* nel contesto digitale in base agli standard internazionali sui diritti umani relativi ai minori

La necessità di approntare una normativa efficace basata sul diritto e sugli standard internazionali in materia di diritti umani si avverte anche con riguardo all'attività delle imprese tecnologiche

che operano nella realtà digitale. A fronte, infatti, delle molteplici opportunità che lo sviluppo delle nuove tecnologie comporta per le persone e la società in generale, anche nella prospettiva del raggiungimento degli obiettivi di sviluppo sostenibile di cui all'Agenda 2030²⁷, si riscontrano altrettanti rischi per la tutela dei diritti umani che richiedono efficaci misure di protezione. Gli strumenti digitali possono diversamente incidere sul diritto alla privacy e alla sicurezza, sul diritto a non essere discriminati, sulla libertà di espressione, sul diritto alla salute e, in misura certamente maggiore, sono potenzialmente in grado di ledere i diritti dei gruppi vulnerabili (minori, anziani, persone con disabilità, rifugiati, migranti, persone provenienti da contesti socio-economici disagiati, ecc.), i quali, da un lato, sono maggiormente esposti ai pericoli disseminati nella realtà digitale e dall'altro, ora a causa delle scarse competenze digitali o linguistiche, ora per ragioni economiche, ora per mancanza di infrastrutture²⁸, ne rischiano l'esclusione, determinandosi perciò un aumento delle diseguaglianze. I rischi cui in particolare sono esposti i minori di età²⁹ durante la navigazione in Internet sono peraltro molteplici ed in continua evoluzione³⁰ e pertanto richiedono un monitoraggio costante.

A ciò si aggiunge la difficoltà di approntare un adeguato sistema di regole giuridiche, non essendo ancora chiari molti effetti dannosi associati all'uso delle nuove tecnologie, specie nel lungo periodo (si pensi per esempio alle dinamiche dei social network) e tenendo anche conto delle trasformazioni sociali indotte dalle stesse tecnologie³¹.

Gli strumenti e gli standard elaborati a livello internazionale ed europeo stabiliscono obblighi o forniscono parametri di riferimento per gli Stati membri affinché assicurino che le aziende ottemperino alle loro responsabilità rispetto ai diritti umani e alle libertà fondamentali dei minori anche nell'ambiente digitale e vengano ritenuti responsabili in caso di abusi. La necessità che le imprese operanti nel settore digitale effettuino una *due*

diligence generale sui diritti umani, avendo specifico riguardo ai diritti dei minori di età, in quanto soggetti vulnerabili, è stata infatti messa in evidenza nell'ambito di diverse iniziative sovranazionali. Per citarne alcune: il Commento generale n.16 sugli obblighi degli Stati relativamente all'impatto del settore delle imprese sui diritti dell'infanzia, adottato dal Comitato sui diritti dell'infanzia nel 2013, nell'ambito del quale si invitano gli Stati a richiedere alle imprese di sottoporre i diritti dell'infanzia e dell'adolescenza ad una procedura di *due diligence* al fine di prevenire e mitigare il loro impatto sui diritti umani; le Linee Guida per il rispetto, la protezione e l'adempimento dei diritti dei minori nell'ambiente digitale, adottate nell'ambito della raccomandazione del Consiglio d'Europa del 2018³², con cui si invitano gli Stati membri a richiedere alle imprese commerciali di assumersi la responsabilità di rispettare i diritti dei minori nell'ambiente digitale e di adottare le necessarie misure di attuazione, tenendo conto degli standard e delle linee guida internazionali ed europee pertinenti³³; il Commento generale n. 25, adottato nel 2021, dal Comitato delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza nell'ambiente digitale. In tal documento, elaborato al fine di assistere gli Stati membri dell'ONU, le organizzazioni internazionali e le Agenzie specializzate nel conseguire la piena realizzazione dei diritti riconosciuti nella Convenzione dei diritti del fanciullo del 1989 anche nell'ambiente digitale, si richiede agli Stati di “garantire che, in tutte le azioni riguardanti la fornitura, la regolamentazione, la progettazione, la gestione e l'uso dell'ambiente digitale, l'interesse superiore di ogni bambino abbia una considerazione primaria” e quindi a tale fine “di intraprendere una procedura di *due diligence* relativamente ai diritti dei minorenni, in particolare per effettuare valutazioni di impatto sui loro diritti e renderle pubbliche, con particolare attenzione agli impatti differenziati e, a volte, gravi dell'ambiente digitale sui minorenni”.

Conformemente ai diritti e ai principi contemplati nella Convenzione ONU sui diritti del fanciullo si è inoltre acquisita la consapevolezza della necessità di garantire e rafforzare l'autonomia del minore anche nell'ambiente digitale. Nella nuova strategia per un Internet migliore per i ragazzi (Bik+)³⁴, e nella dichiarazione europea dei principi e diritti digitali per il decennio digitale si sottolinea la necessità di conferire maggiore autonomia e responsabilità digitali al minore affinché sia in grado di compiere scelte consapevoli e sicure. A tal fine si prevedono azioni per garantire l'educazione digitale su larga scala (attraverso campagne di alfabetizzazione digitale rivolte ai diversi attori educativi quali la famiglia, la scuola, i servizi socio-educativi di sostegno genitoriale, ecc.), con una particolare attenzione ai minori con bisogni speciali o specifici, o provenienti da contesti svantaggiati o di vulnerabilità, nonché favorire la partecipazione attiva dei minori nell'ambiente digitale, affinché sviluppino e pratichino le competenze di cittadinanza nei dibattiti pubblici sulle politiche e le strategie, ed esercitino il diritto di riunione e associazione attraverso le piattaforme sociali online.

3. La *due diligence* sui diritti dei minori nell'ambito della nuova strategia europea per il mercato unico digitale

L'Unione europea sta mostrando una crescente consapevolezza delle problematiche connesse allo sviluppo delle nuove tecnologie digitali, sempre più ispirate alla logica del "capitalismo della sorveglianza"³⁵, e della necessità di predisporre strumenti di natura preventiva orientati a responsabilizzare maggiormente le imprese che sviluppano e diffondono prodotti e servizi digitali in relazione al rispetto dei diritti fondamentali delle persone e, in particolare, dei diritti dei minori di età. In questa prospettiva si colloca il Regolamento 679/2016/UE³⁶ (detto an-

che GDPR) che, sia pure soltanto in relazione agli aspetti legati alla *privacy*, si fonda sul meccanismo del *risk-assessment*, basato sul principio della responsabilizzazione del titolare e del responsabile del trattamento (*accountability*)³⁷, chiamati a svolgere una valutazione preventiva dei rischi derivanti dall'attività di impresa al fine di eliminarli o ridurli con misure adeguate e proporzionate³⁸.

Lo stesso approccio, in termini più generali, caratterizza la nuova strategia europea per il mercato unico digitale³⁹. La direttiva 2018/1808/UE sui servizi di media audiovisivi prevede l'estensione degli obblighi intesi a proteggere i minori da contenuti dannosi che possono nuocere al loro sviluppo fisico, mentale e morale e da contenuti illegali alle piattaforme per la condivisione di video. Il recente Regolamento sui servizi digitali (*Digital Services Act* o DSA)⁴⁰, al fine di assicurare una maggiore tutela dei diritti fondamentali degli utenti nella rete, stabilisce, fra le altre cose, specifici obblighi per i prestatori di servizi intermediari (ed obblighi supplementari per le piattaforme di dimensioni molto grandi) al fine di contrastare i contenuti illegali, la disinformazione online, di garantire maggiore trasparenza delle tecniche di comunicazione commerciale e dei sistemi di raccomandazione e in generale gestire altri rischi per la società. Il DSA dedica, in generale, particolare rilievo all'interesse del minore: nel considerando 89 appare il riferimento esplicito al principio del "*best interest of the child*", che, in particolare, i fornitori di piattaforme digitali (e i motori di ricerca) di grandi dimensioni devono tenere sempre presente nell'adattamento del *design* dei loro servizi e interfacce online, soprattutto quando i servizi sono rivolti ai minori o sono utilizzati prevalentemente da questi ultimi⁴¹. Alle piattaforme *online* è fatto inoltre divieto di presentare pubblicità ai minori sulla base della profilazione (art. 28)⁴² e alle piattaforme *online* (e motori di ricerca) di dimensioni molto grandi è richiesto di compiere una valutazione

d’impatto degli eventuali rischi sistemici che possono sorgere, in relazione alla progettazione di interfacce online che sfruttano, intenzionalmente o meno, le debolezze e l’inesperienza dei minori o che possono causare comportamenti di dipendenza e in generale qualsiasi effetto negativo concreto o prevedibile sulla tutela della salute pubblica e dei minori, nonché sul benessere fisico e mentale della persona (art. 34). Si coglie, peraltro, una prospettiva diversa, rispetto a quella, individualistica, accolta dal GDPR⁴³. Il modello di analisi del rischio su cui si fonda il DSA prende in considerazione sia le implicazioni negative (effettive e) “prevedibili” (che potrebbero verificarsi – ma anche non verificarsi – nel medio lungo periodo), sia le conseguenze etico-sociali (di natura quindi collettiva e non solo individuale), riconducibili all’uso di certe nuove tecnologie, anche a prescindere dal fatto che queste conseguenze producano nell’immediato e in concreto un pregiudizio dei diritti e delle libertà fondamentali individuali. Si tratta di un passaggio importante di prospettiva, prevalentemente informata al principio di precauzione, in ragione proprio dell’incertezza del rischio di danno correlato all’uso di certe nuove tecnologie, in attesa di ottenere ulteriori risultati dalla ricerca scientifica. Si pensi alle diverse strategie di marketing fondate sulla profilazione degli utenti (targeting commerciale, pubblicità gamificata, ecc.), ai sistemi di raccomandazione e alla gerarchia dei contenuti decisi dall’algoritmo⁴⁴, al potere selettivo dell’indicizzazione, alle diverse forme di processo decisionale automatizzato che riguardano i minori e agli effetti discriminatori che comportano; sono alcuni esempi di come le nuove tecnologie siano potenzialmente in grado di incidere sulla vita privata delle persone, sul loro sviluppo, sulla loro libertà di pensiero e di scelta; di condizionare, inoltre, l’opinione pubblica, agevolare la manipolazione e la discriminazione⁴⁵, sebbene non sia al momento possibile identificare, né, tantomeno, misurare, non solo i pregiudizi concreti

alla sfera personale delle persone nel lungo periodo, in particolare quando tali persone si trovino in una condizione pregressa di vulnerabilità (dovuta per esempio all'età, alla malattia, al disagio socio-economico o ad altri specifici, anche contingenti, fattori), ma anche l'impatto sulla società in generale. Ne discende la necessità di un monitoraggio costante unitamente al coinvolgimento continuo degli *stakeholders*, con i quali le aziende operanti nel mercato dei servizi digitali possono mappare le tematiche di sostenibilità più rilevanti per dimostrare il loro approccio responsabile verso i diritti dei gruppi più vulnerabili, quali sono anche i minori di età. Ciò è effettivamente messo ben in evidenza nel considerando 90 del DSA dove si richiedono, nei processi di *due diligence*, adeguate forme di partecipazione dei soggetti destinatari dei servizi e dei gruppi potenzialmente impattati dagli stessi, attraverso il coinvolgimento dei loro rappresentanti, di esperti indipendenti e delle organizzazioni della società civile.

3.1. La “dipendenza da videogiochi” e la “dipendenza da Internet” quali minacce ai diritti umani del minore

Studi scientifici mostrano un notevole incremento di patologie e disturbi legati all'uso improprio dei prodotti e dei servizi digitali da parte in particolare dei bambini e degli adolescenti. Per citarne alcuni: irritabilità, perdita del sonno, aumento del peso per scarsa mobilità, insorgenza di comportamenti aggressivi, ansia, depressione, disturbi dell'attenzione. Si è inoltre rilevato come l'uso eccessivo dei nuovi strumenti di comunicazione digitale e dei videogiochi possa portare a sintomi analoghi a quelli tradizionalmente associati all'uso di sostanze che creano dipendenza⁴⁶.

L'Organizzazione mondiale della Sanità del resto ha riconosciuto ufficialmente la “dipendenza da videogiochi” (o *gaming disorder*), includendola nell'Icd (*International Classification of Dise-*

ases)⁴⁷. Una decisione importante che può, peraltro, dare fondamento ad azioni legali⁴⁸, nonché alla predisposizione di misure più significative, quali limiti di utilizzo per i minorenni.

Diversi studi riconoscono inoltre la “dipendenza da Internet” come una patologia, un disturbo ossessivo/compulsivo, che spinge una persona ad un uso eccessivo dello strumento tecnologico e comprende una grande varietà di comportamenti e problemi di controllo degli impulsi⁴⁹. Oltre alla sindrome di Hikikomori⁵⁰, considerata una delle forme più gravi di dipendenza, si sono rilevati, soprattutto negli adolescenti, una serie di stati emotivi e comportamenti problematici⁵¹, che inducono il soggetto a forme comportamentali compulsive che nel tempo possono dare luogo a dipendenza⁵². I prodotti tecnologici sono infatti progettati e programmati per attirare in modo crescente l’attenzione dell’utente (design persuasivo) e consentire lo sviluppo di tecniche in grado di sfruttare la fragilità di quest’ultimo, orientandolo verso comportamenti, finalizzati esclusivamente a potenziare il “mercato dei dati” e che possono avere significativi impatti sulla salute psichica e fisica dei bambini e degli adolescenti⁵³.

In termini di diritti umani tale rischio riguarda certamente il diritto alla salute, ma può riguardare anche il diritto a non essere discriminati sulla base della diagnosi della dipendenza da Internet. In ogni caso riguarda i diritti di specifici gruppi vulnerabili, quali appunto i minori di età. Nel DSA il legislatore mostra di aver raggiunto tale consapevolezza laddove richiede espressamente agli operatori digitali di compiere la valutazione d’impatto anche dei rischi sistemici che possono sorgere, in relazione alla progettazione di interfacce online che sfruttano, intenzionalmente o meno, le debolezze e l’inesperienza dei minori o che possono causare comportamenti di dipendenza e in generale qualsiasi effetto negativo concreto o prevedibile sulla tutela della salute pubblica e dei minori, nonché sul benessere fisico e mentale della persona (cons. 83 e art. 34 DSA).

4. I diritti dei minori correlati all'uso delle nuove tecnologie nella proposta di direttiva relativa alla *due diligence* delle imprese ai fini della sostenibilità

La proposta di direttiva in materia di sostenibilità di impresa, benché presenti molti aspetti problematici, rappresenta certamente una tappa importante nel processo di responsabilizzazione delle imprese in relazione all'impatto della loro attività sull'ambiente e sui diritti umani e segnatamente nel processo di realizzazione degli obiettivi di sviluppo sostenibile, fin'ora ritenuti perseguibili attraverso la pressione del mercato o i rimedi indiretti.

Non è questa la sede per analizzare le diverse critiche rivolte alla proposta di direttiva sotto i più vari profili, compresi quelli che riguardano il merito della scelta di normativizzare la responsabilità di impresa⁵⁴; ci si limita però a svolgere alcune considerazioni sulla portata applicativa della proposta, con particolare riferimento al tema della tutela dei gruppi vulnerabili in relazione allo sviluppo delle nuove tecnologie, muovendo da alcune critiche che hanno riguardato il ristretto ambito di applicazione della futura direttiva, in particolare sotto il profilo oggettivo⁵⁵.

Il testo della proposta non appare infatti sotto questo aspetto chiaro: per ritenere la futura direttiva applicabile a tutte le possibili violazioni dei diritti umani, e non solo a quelle specificamente indicate, occorre una particolare operazione ermeneutica, attraverso una clausola di salvaguardia dal contenuto non facilmente comprensibile⁵⁶. Il rischio che si corre è che le imprese concentrino i propri sforzi solo sulle questioni oggetto degli specifici obblighi, quali in particolare quelli indicati nella Sezione 2 dell'Allegato alla proposta di direttiva, trascurando le altre questioni fondamentali. Peraltro si mette in evidenza come alcuni strumenti internazionali non siano indicati, fra questi la Convenzione europea dei diritti dell'uomo e la Carta dei diritti fondamentali dell'Unione europea⁵⁷.

Affinché la futura direttiva possa incidere effettivamente sulla promozione e la protezione dei diritti umani e dell'ambiente in modo conforme agli standard internazionali⁵⁸ si ritiene opportuno un più diffuso riferimento ai gruppi vulnerabili e pertanto una maggiore considerazione dell'interesse (superiore) del minore, quale soggetto vulnerabile su cui più frequentemente impatta l'attività di impresa. Tale esplicitazione renderebbe più facile desumere l'applicabilità della direttiva ai casi di violazione dei diritti fondamentali dei minori correlati all'uso delle nuove tecnologie, considerato che i servizi digitali sviluppati all'interno dell'Unione europea e in generale i beni o servizi frutto delle nuove tecnologie, possono essere immessi, o comunque avere un impatto, anche fuori dal mercato dell'Unione europea. Ciò significa che nella valutazione d'impatto dei rischi correlati allo sviluppo e all'impiego delle nuove tecnologie le imprese debbano tenere conto di specifici fattori, quali, per limitarci ad alcuni esempi, le diversità culturali, il minor grado di alfabetizzazione culturale e digitale raggiunto nei paesi in cui impatta la tecnologia.

Il testo proposto dal Parlamento europeo con la Risoluzione del 10 marzo 2021⁵⁹, richiamando una serie di documenti internazionali⁶⁰ che fanno riferimento agli obblighi di *due diligence* in materia di diritti dei minori avrebbe probabilmente facilitato, sotto tale profilo, una lettura più inclusiva della proposta di direttiva⁶¹.

In altre parole è auspicabile un più esplicito coordinamento con la normativa esistente e *in fieri* nell'Unione europea. A questo ultimo riguardo, peraltro, si è fatto notare⁶² come la bozza di regolamento della Commissione europea del 2021 sull'intelligenza artificiale (il c.d. *Artificial intelligence Act*)⁶³ non faccia alcun riferimento ai Principi guida ONU, né all'esigenza di una *due diligence* in materia di diritti umani per le imprese che si avvalgono di questa tecnologia, né ad altri analoghi standard internazionali in materia di imprese e diritti umani.

La valutazione d'impatto sui diritti fondamentali

Note di chiusura

¹ M.MELI, *I nuovi principi costituzionali in materia di ambiente e sostenibilità*, in *Riv. giur. Ambiente e diritto*, 2022, p.1 ss.

² Secondo la teoria dello *shareholder value*, per la quale la funzione dell'impresa è esclusivamente quella di aumentare i profitti agli azionisti (M. FRIEDMAN, *The Social Responsibility of Business Is to Increase Its Profits*, pubblicato sul *The New York Times Magazine*, il 13 settembre 1970).

³ In base al quale principio si legittima, ai sensi dell'art. 118, comma 4, Cost., «l'autonoma iniziativa dei cittadini, singoli e associati, per lo svolgimento di attività di interesse generale». Cfr. P. PERLINGIERI, *La sussidiarietà nel diritto privato*, in *Rass. dir. civ.*, 2016, p. 687 ss..

⁴ U. TOMBARI, *Corporate purpose e diritto societario: dalla "supremazia degli interessi dei soci" alla libertà di scelta dello "scopo sociale"?*, in *Riv. soc.*, 2021, pp. 3,10.

⁵ C. ANGELICI, *Responsabilità sociale dell'impresa, codici etici, autodisciplina*, in *Giur. comm.* 2011, p. 163.

⁶ Ivi, p.162.

⁷ M.E. COENRAADS- J.E.S. HAMSTER, *Corporate social responsibility: from soft law to hard obligations*, in *ijdschrift voor de Ondernemingsrechtpraktijk*, 2019, p. 21.

⁸ La nozione di sviluppo sostenibile appare per la prima volta nel 1987, nel "Burtland Report" (*Report of the World Commission on Environment and Development: Our Common Future*) dove si legge: "Humanity has the ability to make development sustainable to ensure that it meets the needs of the present without compromising the ability of future generations to meet their own needs".

⁹ Sul piano nazionale le sollecitazioni provenienti dalle fonti sovranazionali hanno trovato un primo accoglimento nella recente riforma costituzionale degli art. 9 e 41 Cost. (legge cost. n. 1 dell'11 febbraio 2022).

¹⁰ Cfr. l'Agenda 2030, adottata a New York, il 25 settembre 2015, in cui sono elencati i 17 obiettivi di sostenibilità. (Per una ricostruzione delle tappe che hanno segnato l'ascesa dello sviluppo sostenibile nel diritto internazionale, europeo e nazionale si veda D. IMBRUGLIA, *Mercato unico sostenibile e diritto dei consumatori*, in *Persona e mercato*, 2021, p. 495 ss.).

¹¹ U.TOMBARI, *Corporate Social Responsibility (CSR), Environmental Social Governance (ESG) e scopo della società*, in *Riv. dir comm.*, 2021, pp. 226-227.

¹² La rendicontazione non finanziaria è stata introdotta dalla Direttiva 2014/95/UE e recepita in Italia con il d.lgs. 254/2016. L'obbligo, in base a tale normativa, ricade solo a carico delle grandi società quotate e delle grandi banche e assicurazioni, quotate e non, con più di 500 lavoratori, ma si consideri che il 16 dicembre 2022 è stata pubblicata nella Gazzetta Ufficiale dell'Unione europea la nuova Direttiva “*Corporate Sustainability Reporting Directive (CSRD)*”, che andrà a modificare la precedente, prevedendo un allargamento dei soggetti interessati (l'obbligo ricadrà anche sulle piccole e medie imprese quotate e non quotate).

¹³ Sul ruolo della trasparenza nella promozione della responsabilità sociale si veda L. MARCHEGANI, *Riflessioni su informazione non finanziaria, comunicazione di impresa e fiducia degli stakeholders*, in *Osservatorio del diritto civile e commerciale*, 2021, disponibile su: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3847034.

¹⁴ R. ROLLI, *L'impatto dei fattori ESG sull'impresa. Modelli di governance e nuove responsabilità*, Bologna, il Mulino, 2020, p. 51.

¹⁵ I «Principi guida su imprese e diritti umani», approvati nel 2011 dal Consiglio dei diritti umani delle Nazioni Unite, hanno introdotto a livello mondiale la norma sulla «dovuta diligenza» e fornito un quadro non vincolante per le imprese in relazione alle loro responsabilità riguardo al rispetto dei diritti umani.

¹⁶ Fra questi: le linee guida dell'OCSE per le imprese multinazionali (che sono state riviste nel 2011), la dichiarazione tripartita dell'ILO sui principi riguardanti le imprese multinazionali e la politica sociale (rivista nel 2017), l'Agenda 2030, adottata a New York nel 2015, dove sono tipizzati i 17 obiettivi della sostenibilità, l'Accordo di Parigi del 2015, concluso tra gli Stati membri della Convenzione quadro delle Nazioni Unite sul clima del 1992.

¹⁷ L'autodisciplina svolge un ruolo centrale nello sviluppo sostenibile della gestione aziendale. Il nuovo Codice di Autodisciplina delle società quotate sul Mercato Telematico Azionario (“MTA”) gestito da Borsa Italiana, (“Codice di Corporate Governance”), approvato nel gennaio 2020, rappresenta un importante strumento di stimolo per il rafforzamento della corporate governance attraverso la valutazione del mercato. Cfr. P. MONTALENTI, *Il nuovo Codice di Corporate Governance*, in *Corporate Governance*, fasc. 1., 2021

¹⁸ Favorendo la lettura ecologica del contratto (vedi M. PENNASILICO, *Sviluppo sostenibile e «contratto ecologico»: un altro modo di soddisfare i bisogni*, in *Rass. dir. civ.*, 2016, 1291 ss.) e in generale gli studi sulla “conformazione ecologica” dell'autonomia negoziale che portano a considerare l'interesse ambientale

“un vincolo positivo e intrinseco all'attività di operatori pubblici e privati” (M. PENNASILICO, *Dal “controllo” alla “conformazione” dei contratti: itinerari della meritevolezza*, in *Contr. impr.*, 2020, p. 823 ss.).

¹⁹ Sul punto si veda S. LANDINI, *Sostenibilità e diritto dei privati. Il caso dei contratti sostenibili nel settore turistico*, in questo volume.

²⁰ Fra i problemi che pone la dimensione volontaristica della responsabilità sociale d'impresa vi è quello della individuazione dei beneficiari delle scelte aziendali sostenibili e dei relativi strumenti di tutela in caso di inadempimento. Cfr. C. PONCIBÒ, *The Contract Governance Of Sustainable Development*, in *Isaidat Law Review*, 2022, p. 4.

²¹ U. TOMBARI, *Corporate purpose e diritto societario: dalla “supremazia degli interessi dei soci” alla libertà di scelta dello “scopo sociale”?* cit., p.10.

²² Sia con riguardo alle questioni di giurisdizione (per una rassegna dei casi in cui i tribunali europei hanno riconosciuto la propria giurisdizione anche nei casi di condotte abusive dell'impresa che producono effetti in luoghi diversi rispetto a quelli in cui ha la sede legale si veda M. V. ZAMMITTI, *L'impresa socialmente responsabile: un primo itinerario di giurisprudenza, anche in prospettiva comparata*, in *Le società*, 2021, p. 1018 ss.), sia con riguardo alla individuazione del concreto standard di diligenza. Al riguardo si segnala la innovativa, ma contestata, decisione del Tribunale dell'Aia del 27 maggio 2021, con la quale la società olandese Royal Dutch Shell è stata condannata a ridurre le proprie emissioni di CO2 del 45% entro il 2030, in linea con gli obiettivi stabiliti con l'Accordo di Parigi, da cui si è ricavato il concreto standard di diligenza (duty of care) richiesto alle imprese del settore. La portata della sentenza si coglie propria nella rilevanza diretta che la Corte ha inteso dare nella specie agli strumenti di *soft law*.

²³ U. TOMBARI, *Corporate purpose e diritto societario: dalla “supremazia degli interessi dei soci” alla libertà di scelta dello “scopo sociale”?* cit., p. 10.

²⁴ Così per esempio: nei Paesi Bassi, la legge sulla dovuta diligenza in materia di lavoro minorile impone alle imprese che operano sul mercato olandese di indagare se vi sia il ragionevole sospetto che i beni o i servizi forniti siano stati prodotti ricorrendo al lavoro minorile e, in caso affermativo, di adottare e attuare un piano d'azione. In Francia, la legge relativa al dovere di diligenza delle imprese madri e appaltatrici (c.d. Loi Pacte del 2019) impone ad alcune società di grandi dimensioni l'adozione, la pubblicazione e l'attuazione di un piano di dovuta diligenza per identificare e prevenire i rischi per i diritti umani, la salute, la sicurezza e l'ambiente causati dall'impresa, dalle sue controllate, dai suoi subappaltatori o dai suoi fornitori. La legge francese introduce una

responsabilità amministrativa in caso di inosservanza dei requisiti in materia di dovuta diligenza e prevede l'obbligo per l'impresa di risarcire il danno provocato.

²⁵ Negli Stati Uniti l'*Uyghur Forced Labor Prevention Act* (2021) vieta l'importazione di tutti i beni estratti, prodotti, o fabbricati, in tutto o in parte, nella regione cinese dello Xinjiang o da determinati soggetti cinesi, in quanto si presume che siano effettuati con il lavoro forzato degli Uiguri, facendo tuttavia salva la prova contraria.

²⁶ *Proposal for a Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937, COM(2022)71 final*, del 23.2.2022, disponibile su: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0071>.

²⁷ Si pensi, per esempio, a come le tecnologie assistite dall'intelligenza artificiale contribuiscano, nel settore medico sanitario (dalla telemedicina all'assistenza robotica durante le operazioni chirurgiche), a salvare vite umane, nel settore del trasporto, a ridurre gli incidenti stradali, nell'istruzione a ridurre le disuguaglianze garantendo l'accesso ad una più ampia platea di studenti che altrimenti ne rimarrebbero esclusi, nel lavoro, attraverso lo smart-working, a ridurre le emissioni inquinanti, ecc.

²⁸ Il *digital divide*, ossia il divario esistente fra i soggetti che hanno effettivo accesso alle moderne tecnologie informatiche e i soggetti che non ne hanno, incide sui diritti umani dal momento che l'accesso a Internet deve ritenersi un prerequisito per l'esercizio degli altri diritti, quali per esempio il diritto all'istruzione, il diritto al lavoro.

²⁹ Vedi A. CORRENTI, *Piattaforme tecnologiche: protezione ed educazione dell'utente all'utilizzo delle infrastrutture informatiche nei mercati a concorrenza imperfetta*, in questo volume.

³⁰ Per tale ragione l'OCSE (nel rapporto *Children in the digital environment. Revised typology of risks*, del 2021) ha ritenuto di effettuare una revisione rispetto alle categorie individuate nel rapporto del 2019, individuando quattro grandi categorie di rischi: i rischi di contenuto (di esposizione a contenuti nocivi, illegali, di incitamento all'odio, di disinformazione), i rischi di condotta (di contribuire alla creazione di contenuti o di contatti digitali rischiosi), i rischi di contatto (sexting, sextortion, cyberbullismo) e i rischi per consumatori (frodi online, tecniche di marketing nocive o comunque invasive). A questi rischi si aggiungono quelli trasversali che impattano in generale sul benessere dei minori, come i rischi per la privacy, quelli legati alle tecnologie avanzate e quelli per la salute. Dal gioco interattivo alla visualizzazione di un video o

dal semplice uso di smart toys o di altri dispositivi IoT (Internet of Things), le aziende sono in grado di inferire informazioni, anche sensibili, preziosissime che non si limitano alle sole caratteristiche, abitudini e preferenze dell'utente, ma includono anche le sue condizioni di salute, le sue abilità cognitive, i suoi stati d'animo, le sue vulnerabilità, consentendo quindi, grazie alle tecniche analitiche e predittive, la realizzazione di profili accurati relativi ai singoli consumatori minorenni, verso i quali indirizzare pubblicità mirate e personalizzate, servendosi, peraltro, di tecniche particolarmente persuasive, come l'influencer marketing e la pubblicità c.d. gamificata al fine di orientarne i comportamenti. Ne discende una considerevole limitazione della libertà di autodeterminazione dell'utente minorenne in grado di estendersi ben oltre la sfera economica e che né lo strumento del consenso (cfr. A.M. GAMBINO, *Big data e fairness. Il ruolo delle authorities*, in *Nuovo dir. civ.*, 2020, p. 298), né la trasparenza formale del trattamento dei dati sono, in ogni caso, in grado di escludere.

³¹ G.M.FLICK- C.FLICK, *L'algoritmo d'oro e la torre di Babele*, Milano, 2022, p.87

³² Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment.

³³ La Raccomandazione fa esplicito riferimento ad una serie di documenti internazionali nei quali è affermata la responsabilità delle imprese di rispettare i diritti umani, compresi i diritti dei minori, in particolare: la Raccomandazione CM/Rec(2016)3 del Comitato dei Ministri agli Stati membri sui diritti umani e le imprese, il Commento generale del Comitato delle Nazioni Unite sui diritti dell'infanzia n. 16 (2013) sugli obblighi degli Stati per quanto riguarda l'impatto del settore commerciale sui diritti dei bambini, i Principi guida delle Nazioni Unite su imprese e diritti umani (2011), le Linee guida del Consiglio d'Europa per la cooperazione tra le forze dell'ordine e i fornitori di servizi Internet contro la criminalità informatica (2008), le Linee guida sui diritti umani per i fornitori di servizi Internet (Consiglio d'Europa ed EuroISPA) (2008), le Linee guida sui diritti umani per i fornitori di giochi online (Consiglio d'Europa ed Euro ISFE) (2008) e i Principi sui diritti dei bambini e le imprese (2012) elaborati dall'UNICEF, dal Global Compact delle Nazioni Unite e dall'ONG Save the Children.

³⁴ *A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK)* Bruxelles, 11.5.2022 COM(2022) 212 final.

³⁵ Lo sviluppo della tecnologia ha determinato infatti l'insorgere di nuovi poteri economici che, sfruttando l'enorme patrimonio informativo acquisito

nell'attività di raccolta dei dati personali, in una logica di mera massimizzazione del profitto, sono sempre più in grado di "sorvegliare" i comportamenti delle persone al fine di creare prodotti predittivi sempre più sofisticati, in grado di orientare, ai fini commerciali (ma non solo) i comportamenti delle persone attraverso pratiche invasive e lesive dei loro diritti fondamentali. (S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*. Roma, 2019, p. 22). Come inoltre messo in luce nell'ultimo rapporto del Consiglio dei diritti umani delle Nazioni Unite sul diritto alla privacy nell'era digitale (A/HRC/48/31), il rischio che si creino sistemi di sorveglianza e controllo sempre più invasivi in grado di pregiudicare i diritti umani è diventato concreto e reale.

³⁶ Regolamento UE 2016/679 del 27 aprile 2016 del Parlamento europeo e del Consiglio, relativo "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva n. 95/46/CE.

³⁷ Il principio dell'*accountability* rappresenta una delle principali novità del regolamento che, diversamente dalla direttiva 95/46/CE, abrogata, è prevalentemente incentrato sulla valutazione dei rischi e delle relative attività e sulle misure di sicurezza, tecniche ed organizzative da adottare. Cfr. R. D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in V. CUFFARO, R. D'ORAZIO - V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, 2019, Torino, p. 65; G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, 1, p. 1 ss.

³⁸ L'art.25 del GDPR prevede in capo al titolare e al responsabile del trattamento dei dati personali l'obbligo di adottare misure tecniche e organizzative in grado di garantire la riservatezza dell'utente finale e dei suoi dati personali fin dalla fase della progettazione dei prodotti e dei servizi (c.d. *privacy by design* e *by default*)

³⁹ Nonché la strategia europea per lo sviluppo dell'intelligenza artificiale. Cfr. Proposta di Regolamento per la introduzione di regole armonizzate sull'intelligenza artificiale elaborata dalla Commissione e sottoposta al Parlamento e al Consiglio il 21 aprile 2021 [COM (2021) 206 final] (*Intelligence Artificial Act*)

⁴⁰ Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) che sarà applicato in tutti gli Stati membri a partire dal 17 febbraio 2024.

⁴¹ Sotto tale profilo quindi il regolamento sui servizi digitali recepisce le indicazioni contenute nel *General Comment* n. 25, del 2 marzo 2021, del Comita-

to Onu alla Convenzione di New York del 1989 sui diritti dell'infanzia e dell'adolescenza, che indica le modalità con cui i diritti dei minori, affermati nella Convenzione, debbano essere applicati nell'ambiente digitale. In questo documento, infatti, si fa riferimento ai rischi che sorgono in relazione alle nuove forme di pubblicità commerciale e alle strategie di design persuasivo correlate ai prodotti e ai servizi digitali. Si legge, in particolare, come gli Stati parte dovrebbero garantire che le imprese non si rivolgano ai minorenni "utilizzando tecniche progettate per dare priorità agli interessi commerciali rispetto a quelli del minore".

⁴² Questione che era stata lasciata aperta dal GDPR

⁴³ Sui limiti del modello individualistico adottato nel GDPR si vedano le considerazioni di A. MANTELERO, *Responsabilità e rischio nel Reg UE 2016/679*, in *Nuove Leggi civ. comm.*, 2017, p. 164.

⁴⁴ R. MONTINARO, *I sistemi di raccomandazione nelle interazioni tra professionisti e consumatori: il punto di vista del diritto dei consumi (e non solo)*, in *Persona e Mercato*, 2022, p..368 ss..

⁴⁵ Cfr. A. JABŁONOWSKA, MACIEJ KUZIEMSKI, A M., NOWAK, H.W. MICKLITZ, P. PAŁKA, G. SARTOR, *Consumer law and artificial intelligence Challenges to the EU consumer law and policy stemming from the business' use of artificial intelligence*, EUI Working Paper LAW 2018/11, p. 48.

⁴⁶ Cfr. T. CANTELMÌ, C. DEL MIGLIO E A. GAMBA, *Contributo allo studio di variabili psicopatologiche correlate all'uso-abuso di Internet*, in *Journal of Psychopathology*, 2002, consultabile all'indirizzo <https://www.jpsychopathol.it/article/contributo-allo-studio-di-variabili-psicopatologiche-correlate-allusoabuso-di-internet/>.

⁴⁷ Tale classificazione è diventata effettiva a partire dal 1 gennaio 2022

⁴⁸ Al riguardo si consideri la decisione della Corte suprema del Quebec del 7 dicembre 2022 con cui è stata accolta l'azione di classe promossa da alcuni genitori nei confronti dell'azienda produttrice del videogioco "Fortnite" ritenuto pericoloso per la dipendenza che crea nei giocatori, associata a danni psicologici e fisici. Nella specie vengono lamentati emicrania, dolori alla schiena e al collo, disturbo del sonno e problemi sociali significativi. Particolare interesse suscitano le questioni di fatto e di diritto che dovranno essere successivamente valutate nel merito al fine di riconoscere una responsabilità del produttore dei videogiochi. Così, in particolare, si dovrà verificare se nella specie a) sia stato sviluppato, prodotto, pubblicato, commercializzato e venduto un prodotto pericoloso e dannoso per la salute dei membri della classe; b) si presuma che i convenuti fossero consapevoli dei rischi e dei pericoli associati all'uso del videogioco in questione; c) i convenuti abbiano omesso o

trascurato di rivelare ai membri i rischi e i pericoli associati al videogioco; d) i membri della classe fossero a conoscenza, o fossero in grado di conoscere, i rischi e i pericoli associati all'uso del gioco; e) i convenuti abbiano fornito ai membri tutte le informazioni necessarie per proteggerli dai rischi e dai pericoli associati all'uso del videogioco; f) non avendo menzionato i rischi e i pericoli associati all'uso del videogioco, i convenuti abbiano commesso una pratica vietata ai sensi dell'articolo 215 del Consumer Protection Act; g) i convenuti, attraverso la loro strategia di marketing e pubblicità, abbiano tentato di banalizzare o negare i rischi e i pericoli associati all'uso del videogioco; h) i convenuti abbiano violato i diritti alla vita, alla sicurezza e all'integrità dei membri ai sensi della *Charte des droits et libertés de la personne*, del Quebec i) i ricorrenti e i membri della classe abbiano diritto ai danni punitivi ai sensi della *Charte* o della LCP (la legge sulla protezione del consumatore).

⁴⁹ F. SALICETIA, *Internet Addiction Disorder, in Procedia - Social and Behavioral Sciences*, 2015, 191, p. 1372 ss..

⁵⁰ Questo tipo di sindrome porta il giovane ad isolarsi e ad abbandonare gli studi e la frequentazione di amici. Cfr. T.A. KATO, S. KANBA e A.R. TEO, *Hikikomori: Multidimensional understanding, assessment, and future international perspectives, in Psychiatry and Clinical Neurosciences*, 2019, 73, pp. 427-448.

⁵¹ Così la c.d. "Fear of missing out", con cui si indica la preoccupazione ossessiva di perdere un evento postato in rete, o comunque di essere "essere tagliati fuori" dalle esperienze vissute dagli amici; la "no mobile phone phobia", ossia la paura di rimanere senza il proprio cellulare da cui può derivare uno stato di ansia molto forte.

⁵² M.D. GRIFFITHS -D.J. KUSS, *Adolescent social media addiction (revisited), in Education and Health*, 2017, 35, n. 3, p. 49 ss..

⁵³ Si pensi, per citare alcuni esempi, alle tecniche volte a confrontare (soprattutto) le adolescenti con standard di bellezza irrealistici (per esempio le applicazioni che consentono di ritoccare i lineamenti del viso rendendo spesso l'immagine della persona molto distante da quella reale); al meccanismo dei "like" che può contribuire anche a distruggere l'autostima dei giovani utenti, sottoposti ad un'approvazione sociale costante e da parte di un esteso numero di persone.

⁵⁴ Si è per esempio evidenziato il rischio di una eccessiva burocratizzazione che finirebbe per intralciare lo stesso sviluppo sostenibile delle imprese (Cfr. G.D. MOSCO, R. FELICETTI, *Fin troppa diligenza sulla sostenibilità delle società, in Imprese Unione Europea*, 19.7.22, disponibile su: <https://www.lavoce.info/archives/96293/fin-troppa-diligenza-sulla-sostenibilita-delle-societa>). Si è da

altri sottolineata l'inutilità e l'inidoneità della direttiva a “modificare realmente i canoni deontici dell'azione gestoria (E. BARCELONA, *La sustainable corporate governance nelle proposte di riforma del diritto europeo: a proposito dei limiti strutturali del c.d. stakeholderism*, in Riv. soc., 2022,p. 32).

⁵⁵ Le critiche hanno riguardato anche il ristretto ambito soggettivo della futura direttiva e in particolare i criteri individuati per circoscriverlo, quello della dimensione (vedi art. 2, § 1 lett. a) e del fatturato (vedi art. 2, §1 lett. b), non ritenendosi tali elementi indicatori affidabili a valutare gli impatti negativi che un'impresa può originare sulla sua catena del valore e portando poi ad escludere dall'ambito di applicazione le piccole e medie imprese (PMI), le quali possono invece avere impatti importanti sui diritti umani (M. FASCIGLIONE, *Luci ed ombre della proposta di direttiva europea sull'obbligo di due diligence d'impresa in materia di diritti umani ed ambiente*, in Sidiblog, 26 maggio 2022, disponibile all'indirizzo : <http://www.sidiblog.org/2022/05/26/luci-ed-ombre-della-proposta-di-direttiva-europea-sullobligo-di-due-diligence-dimpresa-in-materia-di-diritti-umani-e-ambiente/>). Si evidenzia peraltro come sotto questo profilo la proposta di direttiva non risulti in linea con i Principi Guida ONU, in particolare con il Principio 14 in base al quale “la responsabilità delle imprese di rispettare i diritti umani si applica a tutte le imprese indipendentemente dalla loro dimensione, dal settore, dal contesto operativo, dell'assetto proprietario e dalla loro struttura. Nondimeno, la portata e la complessità degli strumenti con cui le imprese assolvono tale responsabilità possono variare in base ai summenzionati fattori e al livello di gravità degli impatti negativi dell'impresa sui diritti umani”.

⁵⁶ L'art. 3 lett. b) e c) della bozza di proposta di direttiva, al fine di definire i comportamenti che determinano un impatto negativo sull'ambiente e sui diritti rinvia alle violazioni dei divieti e degli obblighi derivanti dalle convenzioni e strumenti internazionali elencati nelle Parti II e I dell'Allegato alla proposta di direttiva. E' presente tuttavia, nello stesso Allegato (ma vedi anche il considerando 25) una clausola di salvaguardia che prevede l'applicabilità della proposta anche alle violazioni di un divieto o di un diritto non contemplati nell'Allegato, ma inclusi negli accordi sui diritti umani elencati nella sezione 2 dell'allegato, che pregiudica direttamente un interesse giuridico tutelato in tali accordi, a condizione che l'impresa interessata possa ragionevolmente stabilire il rischio di tale pregiudizio e le misure appropriate da adottare per conformarsi agli obblighi di cui all'articolo 4 della direttiva, tenendo conto di tutte le circostanze pertinenti delle proprie operazioni, come il settore e il contesto operativo. Fra questi strumenti internazionali compare in ogni caso la Convenzione Onu sui diritti del fanciullo.

⁵⁷ Come messo in evidenza nei commenti alla proposta di direttiva di UNICEF (*An EU Corporate Sustainability Due Diligence Directive that Works for Children*, UNICEF comments on the European Commission proposal [COM(2022) 71 final], disponibile all'indirizzo: <https://www.unicef.org/eu/documents/eu-corporate-sustainability-due-diligence-directive-works-children>) e di Save the Children (Vedi la dichiarazione congiunta di Save the Children e della Commissione internazionale dei giuristi, maggio 2022, *Advancing child rights in the proposed EU Corporate Sustainability Due Diligence Directive* disponibile all'indirizzo: <https://www.icj.org/joint-position-paper-advancing-child-rights-in-the-proposed-eu-corporate-sustainability-due-diligence-directive/>).

⁵⁸ In particolare si considerino gli obblighi degli Stati ai sensi della Convenzione ONU sui diritti dell'infanzia, alla luce anche del Commento generale n. 25 sui diritti dei minori in relazione all'ambiente digitale.

⁵⁹ Risoluzione del Parlamento europeo del 10 marzo 2021 recante raccomandazioni alla Commissione sulla diligenza e la responsabilità delle imprese (2020/2129(INL)), disponibile al seguente indirizzo: <https://eur-lex.europa.eu/legalcontent/IT/TXT/PDF/?uri=CELEX:52021IP0073&from=EN>

⁶⁰ Quali il Global Compact delle Nazioni Unite del 2012 e l'iniziativa sui diritti dei minori e i principi delle imprese elaborata dall'Unicef e Save the Children, il commento generale n. 16 del Comitato delle Nazioni Unite per i diritti del fanciullo del 2013 che individua una serie di obblighi per gli Stati riguardanti l'impatto delle imprese sui diritti dei minori, tra cui la possibilità che gli Stati impongano alle imprese di adottare misure di dovuta diligenza in materia di diritti dei minori

⁶¹ Nelle raccomandazioni alla commissione (al punto 21) si richiedeva di includere nell'Allegato "gli impatti negativi sui diritti umani espressi nelle convenzioni internazionali in materia di diritti umani che sono vincolanti per l'Unione europea o per i suoi Stati membri, nella Carta internazionale dei diritti dell'uomo, nel diritto internazionale umanitario, negli strumenti delle Nazioni Unite in materia di diritti umani sui diritti delle persone appartenenti a gruppi o comunità particolarmente vulnerabili, e nei principi relativi ai diritti fondamentali enunciati nella Dichiarazione dell'OIL sui principi e i diritti fondamentali nel lavoro, così come quelli riconosciuti nella Convenzione dell'OIL sulla libertà di associazione e il riconoscimento effettivo del diritto di contrattazione collettiva, nella Convenzione dell'OIL sull'eliminazione di ogni forma di lavoro forzato o obbligatorio, nella Convenzione dell'OIL sull'effettiva abolizione del lavoro minorile e nella Convenzione dell'OIL sull'eliminazione della discriminazione in materia di impiego e professione. Tra tali impatti

figurano anche, ma non solo, gli impatti negativi in relazione ad altri diritti riconosciuti dalla Dichiarazione tripartita di principi sulle imprese multinazionali e la politica sociale (dichiarazione MNE) e da una serie di convenzioni dell'OIL, quali la libertà di associazione, la contrattazione collettiva, l'età minima, la salute e la sicurezza sul lavoro, la parità di retribuzione, nonché i diritti riconosciuti dalla Convenzione sui diritti del fanciullo, dalla Carta africana dei diritti dell'uomo e dei popoli, dalla Convenzione americana sui diritti dell'uomo, dalla Convenzione europea dei diritti dell'uomo, dalla Carta sociale europea, dalla Carta dei diritti fondamentali dell'Unione europea e dalle costituzioni e legislazioni nazionali che riconoscono o attuano i diritti umani".

⁶² Vedi M. FASCIGLIONE, *I diritti umani nell'era degli algoritmi e dell'intelligenza artificiale*, in questo volume.

⁶³ Cfr. Proposta di regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM(2021) 206 final, del 21 aprile 2021.

Rischio e responsabilità nei sistemi dell'*Internet of Things**

FRANCESCO MEZZANOTTE

Sommario: 1. Introduzione. - 2. Il campo di analisi: i danni attesi nell'ambiente IoT. - 3. Il contesto normativo e i principali regimi di responsabilità potenzialmente rilevanti. - 3.1. L'inadeguatezza dei comuni regimi di responsabilità civile. - 3.2. La responsabilità da prodotto difettoso quale modello di riferimento. - 4. La responsabilità da prodotto e i rischi di danno negli ambienti IoT. - 4.1. La nozione di produttore. - 4.2. La nozione di prodotto. - 4.3. La nozione di difetto. - 4.4. La nozione di difetto. - 5. Violazione dei dati personali: interazione con il regime di responsabilità nel GDPR. - 6. La causalità nell'ambiente IoT. - 7. Conclusioni.

1. Introduzione

Fin dalla sua originaria presentazione da parte della Commissione Europea nel 2015, la 'Strategia per il mercato unico digitale in Europa' ha perseguito, quale fine principale, quello di 'massimizzare il potenziale di crescita dell'economia digitale europea'. A tale obiettivo sono da subito risultate strumentali tre azioni complementari: l'aumento della competitività grazie all'interoperabilità e alla standardizzazione dei sistemi; la promozione di una società digitale inclusiva; la costruzione di un'economia fondata sui dati (*data economy*)¹. Nel quadro di quest'ultima linea di intervento, le problematiche relative all'allocazione dei nuovi rischi di danno derivanti dall'evoluto contesto tecnologico si sono imposte come una delle tematiche più stimolanti, per via della forte pressione esercitata sui tradizionali regimi della responsabilità contrattuale ed extracontrattuale da parte dei più innovativi prodotti e servizi propri dell'economia degli *intangible assets*².

A queste apicali questioni ha dapprima fornito risposta la Comunicazione 'Costruire un'economia dei dati europea' del 2017, con la quale la Commissione ha riconosciuto che tali innovazioni sono in grado di migliorare la sicurezza e la qualità della vita, ma che esse, allo stesso tempo, sono inevitabilmente soggette alla possibilità di errori di progettazione, cattivo funzionamento o manipolazione dei dispositivi, decretando dunque la fondamentale importanza delle modalità con cui dare certezza sia agli utilizzatori sia ai produttori dei dispositivi in relazione alla loro potenziale responsabilità³.

L'aspirazione ad un più coerente sistema di principi e regole che governino il regime della responsabilità con riferimento alle tecnologie emergenti, concepito quale vera preconditione di ogni futuro sviluppo, ha poi ricevuto ulteriore impulso con la Comunicazione del 25 aprile 2018 'L'intelligenza artificiale per l'Europa'. Con tale documento la Commissione Europea ha presentato una serie di iniziative dirette alla realizzazione di un quadro normativo adeguato al rinnovato contesto tecnologico, con il fine ultimo di far sì che le attività economiche europee possano beneficiare della rivoluzione digitale continuando a garantire, al contempo, un alto livello di fiducia e di protezione dei consumatori⁴. Si legge in quel documento che i robot avanzati e i prodotti dell'internet delle cose possono agire in modi che non erano stati previsti quando il sistema è stato messo in funzione per la prima volta: cresce dunque la consapevolezza dell'esigenza di verificare se le criticità derivanti dall'innovazione possano essere adeguatamente affrontate facendo ricorso ai regimi di responsabilità attualmente vigenti a livello europeo e nazionale⁵.

È sulla base di tali premesse che lo Staff Working Document allegato alla Comunicazione del 2017 si concentrava su talune possibili misure legislative dirette a prevenire le conseguenze negative di vuoti normativi, con specifico riguardo al settore dell'*Internet of Things* (IoT)⁶. Le soluzioni proposte hanno preso

le mosse dalla considerazione di come la moderna industria tecnologica si basi sulla complessa interazione, sul mercato, di operatori differenti e di come, conseguentemente, un'equa ripartizione dei costi degli incidenti attesi in tale settore risulti incompatibile con regole di responsabilità basate sulla colpa. Regimi di responsabilità oggettiva sono quindi stati presentati quale necessario punto di partenza per un'analisi che ha visto poi l'individuazione di alcuni possibili criteri di imputazione di allocazione dei costi attesi dei danni. Più specificamente, tra le opzioni normative prese in considerazione figurano: (i) un approccio basato sulla 'produzione del rischio', volto a porre la responsabilità in capo all'operatore di mercato che incrementa maggiormente la probabilità di verificazione di eventi infausti⁷; (ii) un approccio basato sulla 'gestione del rischio', in forza del quale è riconosciuto responsabile l'operatore di mercato che si trovi nella situazione migliore per minimizzare o evitare il prodursi del danno o, ancora, per neutralizzare i costi da esso generati⁸; (iii) un sistema di assicurazione volontaria o obbligatoria, diretto a garantire ai soggetti danneggiati il completo risarcimento del pregiudizio subito, strutturato in modo tale da essere finanziato dai contributi dei produttori, degli sviluppatori di *software*, nonché degli altri attori dell'economia digitale⁹.

Sebbene negli anni più recenti non siano mancati ulteriori e relevantissimi interventi delle istituzioni europee nel settore della responsabilità nell'economia digitale, questi non hanno più direttamente interessato lo specifico settore dell'IoT, e l'analisi delle peculiari problematiche che esso pone è sembrato rifluire nel più ampio dibattito sulle sfide poste dall'intelligenza artificiale e sulle decisioni algoritmiche¹⁰. Lo scritto intende riprendere specificamente ad esame il dibattito sulle iniziative regolatorie sino ad oggi discusse in questo peculiare campo.

L'analisi si svilupperà come segue: si fornisce dapprima un'essenziale ricognizione del settore, individuando i rischi di

danno che ad esso precipuamente si connettono (n. 2); concentrandosi, quindi, sulla pertinenza al tema delle regole armonizzate a livello europeo sulla responsabilità da prodotto difettoso, oggi al centro di un vivo dibattito sulle relative esigenze di riforma, proprio alla luce del mutato quadro tecnologico di riferimento (n. 3). Proprio a tal fine, ci si interroga sul raffronto tra le condizioni necessarie per il sorgere della responsabilità da prodotto difettoso e gli specifici rischi di danno connessi al funzionamento degli ambienti IoT. Ciò al fine di mostrare fin dove adattamenti opportuni possono essere perseguiti attraverso idonee correzioni interpretative, ovvero quali siano le aree che più impellentemente richiedano correttivi da adottare in via legislativa (n. 4). Tra i profili maggiormente problematici, emerge quello relativo a quel particolare elemento di fattispecie delle tutele risarcitorie rappresentato dal nesso causale: a questo dovrà essere dedicata una particolare attenzione, viste le peculiarità che esso pone nel settore dell'IoT (n. 5).

2. Il campo di analisi: i danni attesi nell'ambiente IoT

I recenti progressi tecnologici hanno dato spazio a nuovi rischi di danno, e così a nuove possibili fonti di responsabilità per gli imprenditori e le imprese nell'ambito dei rapporti con la clientela e con altri soggetti interessati: i settori a cui è stata rivolta maggior attenzione, secondo un primo inquadramento desumibile dalla lettura dei documenti ufficiali UE, sono quelli dell'IoT, da una parte, e dell'Intelligenza Artificiale ('IA'), dall'altra¹¹. Mentre quest'ultimo settore abbraccia una pluralità di sistemi di natura eterogenea, accomunati dalla loro capacità, fondata sul funzionamento di meccanismi algoritmici, di 'comprendere' ed 'interpretare' le informazioni provenienti dall'ambiente circostante, e dunque di 'apprendere' e 'reagire' in modo non prevedibile – e quindi effettivamente autonomo – (*e.g.* robot, droni,

veicoli a guida autonoma, ecc.)¹², la tecnologia IoT opera ad oggi in modo maggiormente deterministico¹³.

Più in particolare, l'IoT può essere descritto come un ecosistema cyber-fisico di sensori e azionatori, che rende possibili e supporta processi decisionali per mezzo di un *software* integrato e della connessione assicurata da sistemi di *cloud computing*, i quali permettono la raccolta, l'analisi, la condivisione e il (ri)utilizzo dei dati, registrati e scambiati da (e attraverso) diversi dispositivi (attraverso una comunicazione c.d. *Machine to Machine*: 'M-M')¹⁴. Sulla base di quanto detto, l'IoT si sostanzia dunque in un'architettura di sistemi e apparecchi in grado di 'percepire' ciò che li circonda, di 'elaborare' le informazioni rilevanti e di 'reagire' di conseguenza, modificando o adattando l'assetto dei dispositivi interconnessi.¹⁵ Si possono immaginare diverse applicazioni di questo sistema, ciascuna caratterizzata da un differente livello di complessità e esplicantesi in varie dimensioni: a partire da basilari accessori (*wearables*) – i quali inviano segnali a chi li utilizza in funzione delle informazioni raccolte sulla base delle attività svolte o dei valori corporei (*body measurements*)¹⁶ – fino a giungere a più articolati sistemi di strumenti e macchinari utilizzati per organizzare il funzionamento di reti complesse (quali, per esempio, distretti industriali, imprese agricole, centri e servizi ospedalieri, ecc.), o per fornire supporto alle attività di amministrazione e gestione dei pubblici spazi (e.g., sistemi di trasporto – strade, ferrovie – *smart cities*, ecc.)¹⁷.

Come emerge da questa prima ricognizione, una delle caratteristiche distintive degli ambienti IoT è costituita dal fatto che il relativo funzionamento non sarebbe possibile in assenza di un ampio numero di attori presenti sul mercato, ciascuno dei quali è chiamato a fornire uno o più dei componenti essenziali di tale complesso ecosistema¹⁸. Volendosi limitare ad elencare solo alcune tra le più rilevanti componenti di un ambiente IoT, vengono in rilievo: (i) i dispositivi materiali e i loro componenti interni; (ii) i

sensori in essi integrati; (iii) il *software* che rende operativo l'apparecchio interconnesso; (iv) la trasmissione, l'elaborazione e l'utilizzo dei dati da parte dei dispositivi e dei programmi; (v) i servizi che garantiscono la connessione; (vi) la presenza di infrastrutture digitali e di servizi di manutenzione del *cloud*, ecc.¹⁹.

Sebbene ad oggi il settore IoT non sia ancora stabile oggetto di contenzioso²⁰, il processo tramite cui esso tende a pervadere in modo sempre più capillare le attività della vita quotidiana lascia preconizzare l'emergenza, nel prossimo futuro, di una serie di rischi di danno concreti e di natura standardizzata, in grado di sollevare problematiche in materia di responsabilità civile la cui rilevanza sarà direttamente proporzionale al livello di sviluppo tecnologico²¹.

Quale punto di riferimento dell'analisi condotta nel presente articolo sia concesso prendere le mosse da alcuni semplici casi di studio.

Si prenda come primo esempio un ambiente domotico (*smart home*) dotato dei tipici oggetti di arredamento e servizi (acqua, riscaldamento, servizi di telecomunicazione, sistemi *home-video* e di allarme), i quali siano però in grado di registrare i dati e le informazioni che ad essi pervengono dall'esterno attraverso diversi strumenti di misurazione (termostati, timer, rilevatori di fumo e di suoni, sensori, ecc.) e di funzionare rimanendo, in maniera costante, reciprocamente interconnessi tramite la rete internet²². Si supponga, allora, un'anomalia nell'ordinario funzionamento dell'ambiente automatizzato dalla quale sia in qualche modo discesa un'alterazione nell'alimentazione elettrica del frigocongelatore, il suo surriscaldamento e, quindi, un'esplosione che distrugge l'intera abitazione, favorita anche dall'assenza dei proprietari al momento del fatto (*Caso A*)²³.

Come secondo esempio, si prenda a riferimento la peculiare applicazione del meccanismo IoT nel settore dei trattamenti sanitari, e si immagini che una cartella clinica sia gestita con un

sistema di interconnessione di dati che consenta al paziente e al suo medico curante di raccogliere simultaneamente tutte le informazioni provenienti dai diversi specialisti che lo hanno in cura, così come quelle attinenti allo stato fisico dell'interessato (es. battito cardiaco, temperatura, pressione, ecc.), e che sia programmato per rilevare e segnalare incompatibilità o necessari adattamenti tra diversi trattamenti farmacologici, prescrivendo i dovuti correttivi. Si supponga allora che l'apparecchiatura di un simile sistema IoT sia soggetta ad un attacco hacker, che ne alteri l'operatività, pregiudichi il *software*, e cagioni una dispersione dei dati personali del titolare, compromettendo le decisioni sanitarie suggerite dal sistema e/o, su sua consultazione, dal medico responsabile (*Caso B*). Ovvero, quale rilevante variante al caso, si immagini che il medesimo risultato pregiudizievole derivi dalle modalità, rivelatesi erronee, con cui l'algoritmo della cartella clinica intelligente ha processato le diverse informazioni ricevute (*Caso B'*).

I principali rischi di danno connessi a tali modelli sono evidenti, e vanno dalla mancata possibilità di far uso dell'impianto e dal materiale deterioramento dei locali e dei dispositivi interessati (*Caso A*), o dalla fuga e perdita di dati personali fino ai potenziali rischi per l'integrità fisica delle persone coinvolte (*Caso B*). Dal punto di vista giuridico quanto detto fin ora solleva una fondamentale questione: su chi dovrebbero gravare i costi attesi dei danni derivanti da questo tipo di eventi lesivi?

3. Il contesto normativo e i principali regimi di responsabilità potenzialmente rilevanti

Giova sottolineare, prima di procedere nell'analisi, come qualsiasi regime di responsabilità diretto a regolare l'economia digitale non possa essere concepito come un insieme di regole e principi destinati ad operare *in vitro*²⁴. Come risulta in modo

sempre più evidente, la regolamentazione di mercati in evoluzione, caratterizzati da rilevanti investimenti nell'innovazione, involge questioni di interesse pubblico e di sicurezza generale, e ciò sollecita inevitabilmente numerosi interventi del legislatore, diretti a garantire un livello costante di fiducia e affidabilità delle attività di produzione e distribuzione dei prodotti e dei servizi²⁵. In tal senso, i tradizionali regimi di responsabilità civile di diritto privato possono essere coerentemente intesi quali strumenti complementari rispetto ai più generali modelli normativi di diritto pubblico, basati su una serie di prescrizioni settoriali (ad esempio nel settore dei prodotti alimentari, dei prodotti farmaceutici e dei dispositivi medici)²⁶ e, in via residuale, di standard di sicurezza aventi efficacia orizzontale come quelli oggi armonizzati su scala europea per effetto della Direttiva sulla sicurezza generale dei prodotti²⁷ e dalle relative misure di attuazione²⁸. Proprio in questa profonda complementarità tra le politiche di intervento di diritto pubblico e privato può rinvenirsi il tratto caratterizzante del diritto privato regolatorio²⁹ – o, secondo una prospettiva parzialmente differente, di quel *supervision private law*³⁰ – di recente oggetto delle crescenti attenzioni nella dottrina europea³¹.

Nel settore oggetto d'esame diversi atti legislativi dell'UE in materia di sicurezza affrontano questioni di rilievo in tema, validi per un'ampia gamma di apparecchiature e macchinari: basti pensare alla Direttiva 2006/42/CE relativa alle macchine (contenente gli standard di sicurezza rilevanti per i robot)³², alla Direttiva 2014/53/CE sulle apparecchiature radio³³, e alla più risalente Direttiva del Consiglio 89/391/CEE sulla sicurezza dei lavoratori³⁴. Pur nella piena consapevolezza delle rilevantissime interazioni che simili tecniche di regolazione possono assumere rispetto alla materia oggetto d'analisi³⁵, l'indagine condotta in queste pagine si concentrerà, più specificamente, sui tipici rimedi di diritto privato³⁶.

A tal riguardo, il dibattito accademico e istituzionale ha già posto in rilievo la sostanziale inadeguatezza dei regimi di responsabilità civile attualmente in uso per affrontare efficacemente il complesso coacervo di rischi connessi all'ordinario funzionamento delle nuove tecnologie digitali³⁷. Non rientra nell'ambito della presente analisi un esame approfondito di tutte le pretese potenzialmente azionabili da parte del soggetto danneggiato, siano esse basate sulle norme vigenti in materia contrattuale o extracontrattuale di diritto interno o su atti legislativi dell'UE. Diversamente, a seguito di un'essenziale ricognizione dei principali limiti e problemi che sembrano incidere negativamente sull'efficacia dei tradizionali regimi di responsabilità, l'accento verrà posto sulla disciplina dedicata al prodotto difettoso, generalmente considerata come il modello maggiormente pertinente alla tutela di interessi come quelli coinvolti negli scenari ipotetici a cui si è fatto riferimento³⁸.

3.1. L'inadeguatezza dei comuni regimi di responsabilità civile

I principi generali della responsabilità civile – di natura contrattuale o extracontrattuale – così come applicati negli ordinamenti della tradizione giuridica occidentale, sono chiaramente inadatti ad individuare e gestire i rischi di danno prodotti dalle nuove infrastrutture tecnologiche dell'IoT.

In linea di principio, il fornitore di un dispositivo o di un servizio che si riveli difettoso, causando così un danno alla controparte contrattuale, dovrebbe essere giudicato responsabile del prodursi delle conseguenze lesive del malfunzionamento dell'IoT. A titolo di esempio, se si caratterizza ulteriormente il *Caso A* e si suppone provato il fatto che l'incendio sia stato causato da un'interruzione nel servizio di connessione internet, la quale abbia dunque impedito il corretto flusso di informazioni tra i vari sensori della *smart home*, risulta difficilmente conte-

stabile la pretesa del cliente che domandi alla controparte contrattuale la totalità dei danni che siano diretta conseguenza dell'inesatta esecuzione dell'accordo, secondo quanto previsto in via generale dalle norme in materia di inadempimento delle prestazioni dedotte in contratto³⁹. Nonostante ciò, non appena le premesse fondamentali a cui si è fatto riferimento risultino meno lineari, sembra assai più complicato ritenere configurate le condizioni per il sorgere, in modo sì certo, di una responsabilità contrattuale. In primo luogo, il principio della relatività degli effetti del contratto (*privacy of contract*) può di per sé escludere l'esperibilità di molte azioni nei confronti dei fornitori dell'ecosistema IoT: questo è chiaramente il caso ogniqualvolta un problema nel funzionamento possa essere ricondotto ai produttori o ai fabbricanti con i quali il consumatore finale non abbia stipulato alcun accordo in via diretta. Inoltre, l'ecosistema IoT potrebbe richiedere la stipula di contratti di varia natura (quali contratti di acquisto degli *hardware*, contratti di licenza d'uso di *software*, contratti per servizi di connettività o di manutenzione, ecc.): il sovrapporsi di tali previsioni contrattuali può creare delle complicazioni per la parte lesa, non solo per via dell'esigenza di coordinare l'eterogeneo contenuto dei termini e delle condizioni proposti da ciascun fornitore, ma anche perché potrebbe risultare estremamente oneroso identificare quale sia, tra tutte, l'esatta prestazione la cui mancata esecuzione abbia determinato il malfunzionamento del sistema⁴⁰.

Tali considerazioni rimangono valide – ed anzi assumono, se possibile, valenza ancor maggiore – se si entra nel campo della responsabilità extracontrattuale. Nel suo tipico modello basato sulla colpa, che rappresenta il regime generale nelle giurisdizioni riconducibili alla tradizione giuridica europea⁴¹, il sistema della responsabilità per atto illecito garantisce al soggetto vittima del pregiudizio scarse possibilità di ottenere un risarcimento del danno derivante dal funzionamento di sistemi complessi

come quelli emergenti oggi nell'ambito digitale⁴². È invero storicamente assai complicato per il soggetto danneggiato, collocato a valle di lunghe e complesse catene commerciali, fornire la prova dei requisiti fondanti la responsabilità delle imprese impegnate nella produzione, fornitura e distribuzione di prodotti e servizi standardizzati⁴³. Tale onere probatorio appare ancor più difficile da assolvere se si volge lo sguardo alle controversie che possono sorgere in contesti altamente tecnologici, governati da interazioni M-M, ove è assai difficile considerare la reazione automatizzata ad un input informatico da parte di uno dei dispositivi interconnessi quale una violazione di un dovere di diligenza per il quale ritenere imputabile un operatore che fornisce un semplice elemento del complessivo ecosistema IoT⁴⁴.

3.2. La responsabilità da prodotto difettoso quale modello di riferimento

Date le considerazioni fin ora esposte, non dovrebbe sorprendere la ricerca di nuovi regimi di responsabilità, i quali potrebbero dimostrarsi maggiormente capaci di assicurare una corretta allocazione dei nuovi rischi di danno connessi agli ambienti digitali innovativi. Nel quadro di questo dibattito, gran parte delle attenzioni, sia con riguardo agli approcci accademici che a quelli di natura istituzionale⁴⁵, sono stati rivolti alla disciplina del risarcimento dei danni causati da prodotti difettosi armonizzata in Europa dalla Direttiva 85/374/CEE⁴⁶. A tutta prima, il tentativo di affrontare le problematiche sollevate dalle moderne tecnologie traendo diretta ispirazione dal più risalente atto legislativo emanato dalle istituzioni europee nel settore della responsabilità extra-contrattuale potrebbe apparire singolare, e probabilmente destinato a produrre risultati di livello insoddisfacente⁴⁷. A fronte di un'analisi più approfondita, seppur non senza talune necessarie specificazioni, questo tipo di sforzo in-

tellettuale sembra essere, tuttavia, degno di maggior credito. Trattandosi del più ragguardevole esempio di armonizzazione giuridica realizzata nel campo del diritto della responsabilità per atto illecito⁴⁸, la disciplina sui prodotti difettosi potrebbe rappresentare una valida opzione per orientare le future discussioni sull'economia digitale.

Non a caso, come si dirà, nelle più recenti proposte di revisione della normativa europea sul punto si rinvengono, significativamente, stimoli alla riconsiderazione delle ragioni che hanno visto progressivamente evolvere un regime di illecito sviluppatosi per affrontare le criticità generate dal progresso tecnologico, e quindi articolatosi, anche attraverso la sua applicazione giurisprudenziale, secondo peculiarità tali da renderlo oggi un autonomo sotto-settore della responsabilità civile, governato dai propri principi, concetti e, soprattutto, da soluzioni operazionali affatto peculiari⁴⁹.

Proprio in quest'ottica, merita sottolineare la notevole affinità tra le premesse legislative in base alle quali la responsabilità da prodotto fu elaborata ed introdotta in Europa e le opzioni regolamentari oggetto del più recente dibattito sul tema dell'economia digitale. Quale intervento normativo guidato dalle concorrenti istanze di protezione del consumatore e di promozione del mercato interno⁵⁰, le finalità ispiratrici della Direttiva 85/374/CEE sono chiaramente illustrate nei suoi *considerando* introduttivi, dai quali emerge con chiarezza come il legislatore dell'epoca avesse individuato in un regime di responsabilità *no-fault* del produttore la premessa imprescindibile per offrire un'adeguata soluzione al problema di una giusta attribuzione dei rischi inerenti alla produzione tecnica standardizzata⁵¹.

Dopo più di tre decenni di progresso scientifico, l'UE continua a mostrarsi in linea con le proprie posizioni di partenza, ritenendo giusto assumere che un numero sempre maggiore di utenti finali farà uso prodotti di natura relativamente comples-

sa, il cui funzionamento implica necessariamente interazioni complesse con terze parti: oggi – così come ieri – è dunque avvertito come necessario un intervento del legislatore che promuova un regime di responsabilità capace di evitare che gli utilizzatori di queste nuove tecnologie possano versare in situazioni di incertezza nel domandare il risarcimento del danno e sviluppare così una mancanza di fiducia⁵². Come da ultimo può leggersi nel Libro bianco della Commissione sull'intelligenza artificiale, '[l]e caratteristiche delle tecnologie digitali emergenti, come l'IA, l'Internet delle cose e la robotica, possono mettere in discussione alcuni aspetti dei quadri giuridici relativi alla responsabilità e renderli meno efficaci. Alcune di queste caratteristiche potrebbero rendere difficile far risalire il danno alla condotta di una persona, condizione indispensabile per invocare la responsabilità per colpa conformemente alla maggior parte delle norme nazionali in materia. Ne deriva la possibilità che i costi per le vittime aumentino in maniera significativa, e la potenziale difficoltà di avviare azioni per responsabilità nei confronti di soggetti diversi dal produttore e di ottenere elementi di prova a sostegno di tali azioni'⁵³.

Sebbene queste analogie di fondo rendano in qualche modo ammissibile considerare il regime dei prodotti difettosi quale valido punto di riferimento nel quadro della tematica in esame, questa osservazione non implica di certo che si debba applicare meccanicamente (e sotto alcuni aspetti acriticamente) un corpo di regole elaborato in un contesto tecnologico profondamente diverso rispetto a nuovi operatori di mercato e nuovi scenari industriali. Come è stato correttamente posto in evidenza, risulta difficile riadattare alle nuove sfide poste dagli ambienti IoT molte delle condizioni essenziali su cui la Direttiva 85/374/CEE fonda la responsabilità del produttore nei confronti dell'utilizzatore danneggiato⁵⁴. Ciò risulta in modo ancor più chiaro se si considera il livello di armonizzazione massima oggi

indiscutibilmente da riconoscere alla disciplina UE sulla responsabilità da prodotto difettoso, da cui consegue un vincolo per i legislatori nazionali e per gli interpreti a rafforzarne o ampliarne le prescrizioni interpretando estensivamente le misure di tutela formalmente contenute nei testi normativi europei⁵⁵.

A partire da queste considerazioni, la restante parte dell'articolo si concentrerà su alcune delle caratteristiche fondamentali del regime della responsabilità da prodotto difettoso che, *de lege data*, appaiono più problematiche in funzione di una loro possibile applicazione ai rischi propri degli ambienti IoT. In taluni casi si terrà conto delle possibili sovrapposizioni con altri regimi di responsabilità (in particolare, con quanto previsto dalle norme in materia di protezione dei dati). L'indagine vuole costituire un punto di partenza per la futura elaborazione di proposte più dettagliate in una prospettiva *de lege ferenda*.

4. La responsabilità da prodotto e i rischi di danno negli ambienti IoT

Tra le iniziative promosse nel quadro della Strategia del mercato unico digitale in Europa, la Commissione UE ha effettuato un'approfondita valutazione della Direttiva 85/374/CEE, focalizzando l'attenzione specificamente sul modo in cui essa ha continuato a spiegare i propri effetti nel tempo e sulla sua rilevanza con riguardo alle emergenti tecnologie digitali. Le preliminari indicazioni risultanti da questo controllo di adeguatezza, così come pubblicate nella Relazione ufficiale dell'8 maggio 2018⁵⁶, sembrano in linea con le fondamentali conclusioni a cui sono pervenuti alcuni studiosi recentemente impegnati nel tentativo di inquadrare i nuovi rischi di danno connessi all'utilizzo dei prodotti e dei servizi dell'Industria 4.0 entro gli schemi della responsabilità da prodotto⁵⁷.

Ai sensi dell'art. 1 della Direttiva 85/374/CEE 'il produttore è responsabile del danno causato da un difetto del suo prodotto'.

Nell'analisi che segue saranno dunque oggetto di specifico esame i rapporti intercorrenti tra l'ambiente IoT e l'esatta portata di nozioni legislative come quelle di: (i) produttore; (ii) prodotto; (iii) difetto; (iv) danno. Un'analisi specifica sarà poi dedicata al concetto di causalità che, come si avrà modo di osservare, rappresenta un elemento di rilevanza essenziale allo scopo di edificare un efficace sistema di allocazione dei costi attesi dei danni tra i diversi livelli dell'architettura IoT.

4.1. La nozione di produttore

La Direttiva 85/374/CEE prevede una lista di soggetti potenzialmente responsabili, con il chiaro scopo di permettere alla vittima della lesione di individuare in modo semplice un convenuto dal quale pretendere il risarcimento⁵⁸. Al contempo, in quanto misura di massima armonizzazione, la Direttiva è stata costantemente interpretata dalla Corte di giustizia come una disciplina che individua in modo esaustivo le categorie di soggetti destinatari del peculiare regime di 'responsabilità oggettiva' valido per i casi di prodotti difettosi⁵⁹. In conseguenza di ciò possono essere giudicati responsabili ai sensi di quanto previsto dalla Direttiva il solo produttore (o colui che è considerato come tale)⁶⁰, l'importatore⁶¹ e, in presenza di talune condizioni, il fornitore del prodotto⁶², mentre ciò non è possibile con riferimento ad ogni altra tipologia di imprenditore coinvolto⁶³. Se applicato ad entrambi i *Casi* in esame (A, B), un tale stato dell'arte potrebbe tradursi nella radicale esclusione dell'applicabilità del sistema di responsabilità in commento con riguardo a tutti quei fornitori di *servizi* che, sebbene non incorporati in beni tangibili, costituiscono cionondimeno essenziali elementi dell'ecosistema IoT.

Un'opinione ormai consolidata, invero, esclude l'applicazione del regime della responsabilità da prodotto difettoso nei confronti degli operatori di mercato che offrano un semplice

‘servizio’: anche se la loro prestazione è adempiuta in un contesto in cui è stato utilizzato un prodotto difettoso, la posizione di tali soggetti è giudicata diversamente rispetto a quella di un fornitore, pur sempre considerabile come un operatore della filiera di produzione e commercializzazione del prodotto⁶⁴. Fino ad oggi la Direttiva è stata ritenuta applicabile ai fornitori di servizi solo in presenza di situazioni ove il medesimo soggetto poteva essere altresì considerato quale produttore di un bene utilizzato per la fornitura del servizio⁶⁵. Nel quadro del diritto UE risulta dunque ancora inesausta la questione sul se possa farsi applicazione della direttiva nei casi di responsabilità di un prestatore di servizi che faccia uso di un prodotto difettoso del quale non sia anche produttore⁶⁶.

Questo profilo merita oggi di essere ulteriormente approfondito nel contesto dell’IoT, ove potrebbe essere necessaria un’interpretazione teleologica della Direttiva, ispirata dall’obiettivo di assicurare un’equa ripartizione del rischio tra tutti gli operatori di mercato che possano essere parte di un rapporto giuridico con un utente finale danneggiato, allo scopo di evitare lacune normative e di promuovere un effettivo riparto della responsabilità⁶⁷.

Problemi di questo tipo si sono con maggior frequenza presentati, negli ultimi anni, nell’ambito del dibattito che, specie oltreoceano, si incentra sulla possibile estensione della disciplina da prodotto difettoso ai nuovi operatori della *platform economy*⁶⁸. Si pensi, per tutti (e pur nel quadro di un’evoluzione senz’altro frastagliata)⁶⁹, ad un caso come quello deciso in *Oberdorf v. Amazon.com Inc*, nel quale le corti hanno aperto all’idea che il noto portale telematico sia in una posizione di controllo sulla complessiva operazione commerciale che attraverso il *virtual marketplace* professionalmente organizzato si conclude, tale da equipararlo al produttore/venditore del bene di consumo difettoso acquistato dal consumatore finale⁷⁰.

4.2. La nozione di prodotto

Ad un più attento esame, le precedenti argomentazioni risultano strettamente connesse alla necessità di una revisione dell'estensione del concetto di 'prodotto' e all'esigenza di adottare un approccio evolutivo guidato dal nuovo contesto digitale, che sia in grado di superare la legalistica distinzione tra la vendita di beni e la prestazione di servizi nei mercati digitali⁷¹.

In chiara connessione con lo scenario tecnologico presente quasi quarant'anni fa, la Direttiva si concentra sui danni prodotti da beni mobili, inclusa l'elettricità (ma con l'eccezione dei prodotti della coltivazione diretta e del bestiame), anche quando essi siano incorporati in altri beni mobili o immobili. Non vi è dubbio sul fatto che tale clausola di 'incorporazione' sia stata prevista per affrontare i rischi di danno derivanti da fondamentali componenti di prodotti altamente sofisticati, come veicoli o farmaci⁷². Oggi tale regola, mentre potrebbe risultare idonea a disciplinare i casi in cui si riscontri la presenza di 'difetti' in componenti materiali dei dispositivi IoT interconnessi (quali sensori, antenne trasmettenti, ecc.), solleva interrogativi assai più ardui da risolvere se si ha riguardo agli elementi immateriali, i quali parimenti costituiscono parte fondamentale di tale ecosistema⁷³. In particolare, questo tema assume rilevanza cruciale per quanto riguarda la qualificazione giuridica della fornitura di *software*⁷⁴. In attesa di un già previsto formale chiarimento per via legislativa da parte delle istituzioni UE⁷⁵, sembra comunque esserci spazio per dei possibili adeguamenti in via ermeneutica.

Mentre non si riscontrano particolari problemi con riferimento ai *software* conservati in un supporto materiale (CD, supporti di memoria, ecc.), costantemente trattati alla stregua di prodotti nel contesto giuridico europeo⁷⁶, tale conclusione diviene assai più incerta quando il *software* non viene fornito per

il tramite di supporti tangibili (per esempio, attraverso un trasferimento *online* o per mezzo di *download* e aggiornamenti automatici di sistema). Con riferimento a tale ultimo gruppo di ipotesi sarebbe oggi auspicabile l'applicazione del regime della responsabilità da prodotto difettoso, in quanto esso risulta del tutto in linea con le scelte che in origine ispirarono la sua introduzione e che ancora oggi orientano l'attività legislativa delle istituzioni europee⁷⁷.

In dottrina, è stata proposta una convincente distinzione tra *software* in grado di intraprendere azioni in modo autonomo, da un lato, e *software* che più semplicemente mettono a disposizione informazioni aventi carattere strumentale rispetto alle decisioni e alle attività successivamente svolte dai singoli individui⁷⁸. Mentre non si ritiene che questi ultimi casi debbano essere soggetti al regime di 'responsabilità oggettiva' dettato dalla Direttiva (per esempio, allorché un sistema GPS fornisca indicazioni errate in merito alle condizioni della strada, poi utilizzate dal conducente), diversa è la conclusione a cui si perviene con riguardo ai primi, che comprendono una serie di ipotesi estremamente rilevanti nell'ambito dell'ambiente IoT (come quelle rappresentate dai *Casi A, B*). In queste situazioni l'impiego del *software* è essenziale per il funzionamento di uno o più dispositivi materiali e per la realizzazione della sua/loro funzione nel più ampio sistema interconnesso per il quale essi sono concepiti. Alla luce di questo inestricabile legame, operativo e funzionale, una radicale esclusione della protezione garantita dal regime della responsabilità da prodotto difettoso per i casi in cui ad essere interessata dal malfunzionamento sia la componente di programma sembrerebbe essere soluzione ermeneutica incompatibile con il dichiarato fine normativo di un'equa ripartizione dei rischi nella moderna industria tecnologica⁷⁹.

Queste indicazioni sembrano del resto essere alla base delle più recenti linee di riforma promosse dalle istituzioni europee.

In particolare, come si legge nella recente relazione della Commissione sulle implicazioni operative dei sistemi IoT in materia di responsabilità civile, '[n]onostante l'ampiezza della definizione di prodotto fornita dalla direttiva sulla responsabilità per danno da prodotti difettosi, il suo ambito di applicazione andrebbe ulteriormente chiarito per rispecchiare meglio la complessità delle tecnologie emergenti e garantire che il risarcimento sia sempre possibile per i danni causati da prodotti difettosi a causa del *software* o di altre caratteristiche digitali. Si consentirebbe in tal modo agli operatori economici, quali gli sviluppatori di *software*, di valutare se possono essere considerati produttori ai sensi della direttiva sulla responsabilità per danno da prodotti difettosi'⁸⁰.

4.3. La nozione di difetto

La nozione di 'difetto' rappresenta, tradizionalmente, il tema più controverso nel quadro della concretizzazione del regime della responsabilità da prodotto. Come noto, la Direttiva europea si limita a prevedere formalmente un test genericamente basato sull'aspettativa del consumatore (*consumer-expectation test*), il quale determina il sorgere della responsabilità ogniqualvolta il prodotto non offre la sicurezza che ci si può legittimamente attendere tenuto conto di tutte le circostanze⁸¹. Nella sua messa in pratica, ciò si traduce in uno standard normativo che opera oggettivamente (ovvero sulla base del ragionevole livello di comprensione del grande pubblico, tralasciando invece le aspettative o condizioni facenti specificamente capo al soggetto leso) e tenendo conto del contesto nel quale al prodotto si fa ricorso⁸².

Sebbene il dettato della Direttiva 85/374/CEE non riproduca formalmente la categorizzazione elaborata nel modello statunitense, le corti e gli studiosi appartenenti alla tradizione giuridica continentale sembrano nondimeno adusi alla formale distin-

zione tra: (a) difetti di fabbricazione (*manufacturing defects*); (b) difetti di progettazione (*design defects*); (c) difetti nelle istruzioni o negli avvisi (*warning defects*)⁸³.

In termini operativi, fatta eccezione per quanto attiene il primo gruppo di casi (basato sull'oggettivo rilevamento di uno specifico difetto del prodotto), gli altri elementi di valutazione sembrano avvicinarsi al test dell'aspettativa, che si mostra in concreto assai prossima all'analisi rischi-benefici tipica del contesto giuridico nord-americano⁸⁴. In particolare, per quanto attiene alla portata normativa del *consumer expectation test*, non è irrilevante la tendenza giurisprudenziale a confrontare gli investimenti in progettazione o nella fornitura delle informazioni a favore dell'utente con quelli che sarebbe legittimo aspettarsi in un modello oggettivo di corretta organizzazione industriale, in linea con gli standard di sicurezza del mercato. Questo tipo di approccio implica, il più delle volte, una valutazione che si rivela equivalente, in termini funzionali, ad un test di ragionevolezza⁸⁵.

In presenza di tale scenario viene spontaneo domandarsi, in prospettiva critica, come inquadrare in questa nozione di 'difetto': (a) la reazione automatica indesiderata di uno o più dispositivi dell'architettura IoT ad un impulso derivante dall'ambiente interconnesso (*Caso A*); o (b) l'insufficiente livello di sicurezza opposto ai tentativi di intrusione da parte di soggetti terzi (*hackers*), con la conseguente incapacità di proteggere le informazioni (di carattere personale) attraverso le quali opera il sistema *data-driven*, o comunque l'indesiderabile esito del processo decisionale sviluppatosi a partire dalle indicazioni provenienti dalla progettazione del *software* (*Caso B', B''*).

Tali questioni risultano ancor più problematiche se si considera che, secondo quanto previsto dalle norme in materia di responsabilità da prodotto, le legittime aspettative del consumatore in termini di sicurezza devono essere valutate facendo riferimento al momento in cui il bene viene immesso in circola-

zione⁸⁶. Tale principio rischia di collidere con uno scenario tecnologico caratterizzato da un costante livello di innovazione e da cambiamenti continui, in grado di rendere un sistema IoT (originariamente) sicuro in breve tempo obsoleto, e dunque non più al riparo dai nuovi rischi di malfunzionamento e da cyberattacchi.

Nell'esperienza nordamericana l'insorgenza di danni causati da difetti apparsi a seguito dell'avvenuta messa in commercio del prodotto è stata affrontata attraverso la previsione generalizzata, per mezzo di interventi legislativi, di un dovere di protezione gravante in capo al produttore⁸⁷, che ha in seguito trovato formale riconoscimento nel più recente (Terzo) *Restatement of Tort: Products Liability* ('post sale failure to warn')⁸⁸. Anche in Europa, seppur in un settore diverso qual'è quello della protezione dei dati personali, il legislatore ha formalmente riconosciuto l'esigenza di un'efficace gestione dei nuovi rischi di danno propri degli ambienti altamente tecnologici e la necessità delle modifiche da questi ultimi imposte sulle misure tecniche e organizzative adottate dai titolari e dai responsabili del trattamento dei dati per realizzare l'obiettivo della sicurezza⁸⁹. Trasposti nel contesto IoT, tali principi e regole potrebbero rivelarsi valide soluzioni in grado di incoraggiare i produttori e gli sviluppatori di *software* ad internalizzare una significativa porzione dei costi attesi connessi alle loro attività, incentivando così un controllo costante e un obbligatorio incremento del livello di sicurezza nel funzionamento degli ecosistemi interconnessi (come quelli presenti in una *smart home*)⁹⁰.

A prescindere tuttavia da questi ultimi rilievi, va osservato come sia in chiave più generale lo stesso concetto di 'difetto', per come più tradizionalmente concretizzato nei giudizi civili, ad essere posto in crisi nei contesti di responsabilità algoritmica, digitale e nei sistemi di IA⁹¹. Ciò conduce parte della dottrina alla ricerca di nuove soluzioni ermeneutiche attraverso le quali

valutare la sussistenza di un prodotto progettato o fabbricato in modo tale da poter legittimare pretese risarcitorie da parte di un consumatore pregiudicato nella propria sfera personale o patrimoniale. Tra queste, si segnalano le proposte che aprono ad innovativi criteri di individuazione della difettosità del prodotto dell'Industria 4.0, le quali, allontanandosi da un'analisi volta alla ricerca di uno specifico malfunzionamento *interno* al sistema, suggeriscono l'elaborazione di raffronti dinamici con apparecchi comparabili, vuoi propri dell'ambiente analogico (*i.e.*, si confrontano gli esiti dell'impiego del prodotto oggetto di giudizio con la comune operatività di più tradizionali beni di consumo), vuoi desumendo, specie in prospettiva futura, uno standard ipotetico di *performance* attesa nel mercato dei prodotti di ultima generazione⁹².

4.4. La nozione di danno

Le voci di danno alla base del regime di responsabilità oggettiva introdotto dalla Direttiva 85/374/CEE sono espressamente elencate dall'art. 9 e comprendono, da un lato, la morte o le lesioni personali e, dall'altro, il danno o la distruzione di un bene normalmente destinato all'uso o al consumo privato (ed effettivamente utilizzato come tale dalla parte lesa)⁹³. Qualsiasi altra tipologia di lesione – tra cui, segnatamente, quella di 'danni immateriali' come quelli meramente patrimoniali – dovrebbe ritenersi non rientrante nello speciale regime di responsabilità riservato ai prodotti difettosi, e dunque lasciata al regime prescelto dai legislatori nazionali⁹⁴. Mentre la semplice applicazione di tali previsioni risulta di per sé sufficiente a coprire i principali danni rilevanti nel *Caso A*, è meno certo che un'interpretazione letterale del dettato della Direttiva possa garantire una tutela effettiva contro i – difficilmente prevedibili – rischi di danno propri degli ambienti IoT, come quelli ipotizzati nel

Caso B (quali le perdite derivanti da attività di *hacking* e dalla violazione dei dati, con i conseguenti pregiudizi anche di carattere non patrimoniale). Per affrontare correttamente il problema occorre considerare, in via preliminare, il modo in cui la concreta interpretazione della direttiva, così come storicamente elaborata dalla Corte di giustizia UE, ha influito sulla messa in atto delle regole ricavate dal testo legislativo.

Ciò vale, anzitutto, per quanto attiene l'esatta perimetrazione della figura dei 'danni immateriali'. È evidente, ad un primo sguardo rivolto ai *considerando* della Direttiva, che l'originale intenzione degli estensori fosse quella di far riferimento ai soli patemi 'animo (*pretium doloris*) e, più in generale, agli essenziali interessi di natura non patrimoniale delle persone fisiche⁹⁵. Allo stesso tempo, l'esigenza di applicare a vicende concrete le rigide voci di danno previste dalla lettera della Direttiva ha portato ad una interpretazione più sfumata del regime di responsabilità oggettiva lì descritto, emersa in particolare nella decisione emessa dalla Corte di giustizia all'esito del caso *Veedfald*⁹⁶. In tale occasione i giudici del Lussemburgo, pur non essendo di fronte ad un tipo di danno formalmente riconducibile alla lista contenuta nell'art. 9 (si trattava, in particolare, della perdita della possibilità per un paziente di essere curato attraverso un trapianto di fegato, divenuto impossibile a causa della difettosità del fluido con cui l'organo era stato trattato prima dell'operazione), adottò un approccio complesso.

Da un lato, questa affermò che la Direttiva individua in modo esaustivo le voci di danno in grado di ammettere l'applicazione della disciplina dei prodotti difettosi; dall'altro, essa chiarì, tuttavia, che un giudice nazionale non può rifiutarsi di riconoscere alcun risarcimento a favore della parte attrice sulla base del fatto che, pur in presenza tutti gli altri elementi richiesti ai fini del sorgere della responsabilità, il danno non sia riconducibile ad alcuna delle predette voci⁹⁷. La decisione ha portato ad un concreto

ampliamento dell'ambito materiale della Direttiva, oggi esteso a tal punto da comprendere i danni derivanti da perdita delle aspettative, e delle *chance* e tale, secondo taluni commentatori, da includere la più ampia area delle 'pure perdite economiche' (anche in contrasto con l'intenzione del legislatore storico)⁹⁸.

Un altro rilevante aspetto dell'evoluzione giurisprudenziale ha riguardato il concetto di 'lesioni personali', così come interpretato, in particolare, nella famosa pronuncia della Corte di giustizia nel caso *Boston Scientific Medizintechnik GmbH*. La controversia è sorta a fronte dell'utilizzo di una serie di *pacemakers* difettosi da parte di una clinica, la quale si era impegnata con i suoi pazienti a sostituirli in via preventiva. Questo impegno ha sollevato la questione se i costi delle operazioni di rimozione e sostituzione del prodotto costituissero un tipo di danno causato da lesioni personali ai sensi della direttiva 85/374/CEE. In tale frangente, considerato il bisogno di tutela effettiva della salute e della sicurezza del consumatore, il dettato legislativo fu oggetto di un'interpretazione estensiva, secondo cui i costi dell'operazione chirurgica finalizzata alla sostituzione di un prodotto difettoso costituiscono un 'danno causato da morte o lesioni personali' di cui il produttore è responsabile se tale operazione è necessaria per ovviare a tale specifico difetto.⁹⁹ Com'è evidente, un tale approccio ermeneutico ha l'effetto di sfumare la linea di demarcazione tra il risarcimento del danno e la sua prevenzione attraverso la riparazione del prodotto¹⁰⁰.

È alla luce di simili considerazioni che pare opportuno esaminare perdite dovute a cyber-attacchi perpetrati contro le reti e i dispositivi IoT (quali quelli esplicitati nel *Caso B*). Come in precedenza accennato, una questione di carattere decisivo è rappresentata, in queste ipotesi, dalla (quantomeno apparente) natura prettamente economica del danno derivante dall'inutilizzabilità dei sistemi interconnessi e dai malfunzionamenti dovuti ai tentativi di intrusione nelle reti e nei dispositivi dell'ambiente domotico.

In diversi casi ciò che potrebbe apparire come un semplice impoverimento di natura finanziaria trova la sua origine in un danno materiale ad una o più componenti dell'ecosistema IoT. I rapporti tecnici dimostrano come, invero, in media: (a) più del cinquanta per cento dei cyberattacchi rende necessario la sostituzione dell'*hardware* o di un *software* o la rimozione da questi ultimi di un *malware* installatovi; (b) in quasi il venti per cento dei casi ha luogo una sottrazione di una proprietà intellettuale; (c) nel trentatré per cento dei casi l'intrusione *hacker* determina una perdita di dati¹⁰¹. Quanto ai danni *sub* (a) e (b), un ampliamento della portata della clausola dei 'danni immateriali' o, in modo probabilmente più efficace, un'interpretazione dei 'danni alle cose' analoga a quella in precedenza elaborata con riferimento alla nozione di 'lesioni personali' sarebbero in grado di meglio realizzare il fine di un'effettiva tutela risarcitoria dell'utente danneggiato. In particolare, seguendo quest'ultimo approccio, la pretesa dell'attore potrebbe comprendere il valore monetario necessario per eliminare le conseguenze dannose del cyberattacco e ripristinare il livello di sicurezza che è lecito attendersi nell'utilizzo di un'architettura IoT.

Con più specifico riguardo ai casi di violazione dei dati (c), l'analisi del regime della responsabilità da prodotto, qui presentata quale modello normativo utile a disciplinare le ipotesi di responsabilità caratteristiche degli ambienti IoT, deve essere affiancata dai principi e dalle regole uniformi introdotte in Europa dal Regolamento generale sulla protezione dei dati (GDPR)¹⁰².

5. Violazione dei dati personali: interazione con il regime di responsabilità nel GDPR

Pur costituendo una misura di massima armonizzazione, la Direttiva 85/374/CEE non mira(va) ad individuare in modo esaustivo ciascuna delle ipotesi di responsabilità connesse alla mes-

sa in circolazione di un prodotto difettoso: di conseguenza, in presenza di tipologie di danno non espressamente previste dal testo legislativo, ai legislatori e agli interpreti è riconosciuta la possibilità di formulare regole diverse o di individuare altri rimedi riparatori attingendo dal bacino dei principi generali dell'ordinamento¹⁰³. Occorre, dunque, debitamente considerare i concreti effetti della natura di 'massima armonizzazione' della Direttiva come emerge dai suoi *considerando* ed in modo ancor più incisivo dalla lettera dell'art. 13¹⁰⁴: il regime di responsabilità ivi previsto costituisce un ravvicinamento 'pieno' ma, al contempo, non 'esaustivo' della disciplina europea sulla responsabilità originata dal malfunzionamento dei prodotti¹⁰⁵. Da ciò deriva, in definitiva, che ogniqualvolta un danno non rientri nell'ambito di applicazione della Direttiva possono assumere rilevanza altre discipline, fonti di responsabilità¹⁰⁶.

È questo il caso, nello specifico, dei danni derivanti dall'identificazione di informazioni personali, dalla profilazione e, più in generale, dalle violazioni e perdite di dati causati da malfunzionamenti di un sistema IoT¹⁰⁷. Tali tipologie di danno non rientrano nell'ambito applicativo della disciplina della responsabilità da prodotto difettoso, mentre ad esse fa oggi specifico riferimento il GDPR, ai sensi del quale 'chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento' (Art. 82, par. 1). A tale riguardo, il GDPR introduce un'ampia nozione di 'danno' che non solo abbraccia ogni tipo di lesione di natura patrimoniale o non patrimoniale, ma che può altresì sommarsi alle 'azioni di risarcimento di danni derivanti dalla violazione di altre norme del diritto dell'Unione o degli Stati membri'¹⁰⁸. Si tratta di un regime di responsabilità che si inserisce in un più ampio sistema di protezione ispirato dal diritto fondamentale all'effettività della tutela giurisdizionale¹⁰⁹, che deve essere concretamente ga-

rantito ogniqualvolta una persona subisca un pregiudizio a causa di un trattamento dei suoi dati personali avvenuto in violazione delle previsioni del Regolamento¹¹⁰.

Soggetti destinatari dello speciale regime di responsabilità per violazione dei dati personali sono non solo i ‘titolari del trattamento’ (coloro che determinano le finalità e i mezzi del trattamento dei dati personali)¹¹¹, ma anche tutti i ‘responsabili del trattamento’ (ovvero ciascun soggetto impegnato in ‘qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione’)¹¹².

Tale responsabilità ‘cumulativa’ in capo ai titolari e ai responsabili del trattamento costituisce una rilevante innovazione rispetto alle precedenti norme della Direttiva 95/46/CE¹¹³ (esclusivamente dirette ai titolari)¹¹⁴: se trasposta nell’ecosistema IoT, essa dovrebbe consentire una più semplice allocazione dei rischi di violazione dei dati tra i diversi attori del mercato che forniscono le componenti essenziali dell’architettura interconnessa.¹¹⁵ Segnatamente, mentre i ‘titolari del trattamento’ sono in linea di principio responsabili per tutte le attività in cui sono coinvolti e che infrangono le previsioni del GDPR, la responsabilità può gravare in capo ai ‘responsabili’ solo nelle ipotesi in cui questi non abbiano adempiuto agli obblighi loro imposti dal Regolamento o qualora abbiano agito al di fuori o contrariamente alle legittime direttive del titolare¹¹⁶. Tra le obbligazioni gravanti in capo ai titolari e ai responsabili del trattamento dei dati (e fonti di responsabilità in caso di inadempimento), l’art. 32, par. 1, GDPR prevede la messa in atto di misure tecniche e organizzative idonee a ga-

rantire un livello di sicurezza adeguato al rischio di perdita dei dati, 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 per i diritti e le libertà delle persone fisiche¹¹⁷. Al fine di concretizzare questo obbligo normativo, il GDPR individua alcuni esempi di misure di sicurezza considerabili 'adeguate al rischio'. Circoscrivendo l'indagine a quanto appare più rilevante con riferimento agli ambienti IoT, possono menzionarsi: 'la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento'¹¹⁸ e 'una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento'¹¹⁹.

In modo analogo a quanto si è avuto occasione di rilevare con riguardo al regime di responsabilità da prodotto difettoso, la responsabilità scaturente dal mancato adempimento degli obblighi previsti dal GDPR opera in maniera indipendente dalla colpa¹²⁰. Non grava dunque sul soggetto danneggiato l'onere di provare alcuna forma di negligenza in capo ai titolari e ai responsabili del trattamento, mentre questi ultimi possono essere esonerati dalla responsabilità solo qualora dimostrino 'che l'evento dannoso non gli è in alcun modo imputabile'¹²¹. Tale formula rimanda a quella già contenuta nell'art. 23, par. 2, della Direttiva 95/46/EC¹²², espressamente volta ad operare nelle ipotesi di 'errore della persona interessata o di forza maggiore'¹²³. Data l'ulteriore enfasi posta dall'attuale versione della norma sull'assenza di alcun profilo di responsabilità in capo ai titolari e ai responsabili del trattamento ('in alcun modo'), sembra possibile dedurre che la clausola di salvaguardia faccia ancora riferimento ad eventi 'assolutamente al di fuori della sfera di controllo' della persona ritenuta oggettivamente responsabile¹²⁴.

Un ultimo profilo merita di essere evidenziato: l'art. 2, par. 4, GDPR precisa che il Regolamento 'non pregiudica l'applicazione

della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva'. Sebbene tale previsione implichi che lo speciale insieme di regole di esonero di responsabilità ivi contenute continui ad operare in favore degli intermediari di internet, gli effetti di questa conclusione dovrebbero essere circoscritti al più specifico settore dell'attività meramente passiva e neutrale, non estendendosi invece a quelle operazioni ulteriori in grado di qualificare tali soggetti quali titolari e responsabili del trattamento dei dati, secondo la tutt'oggi valida motivazione del caso *Google Spain*¹²⁵.

6. La causalità nell'ambiente IoT

Caratteristica comune dei diversi regimi normativi fin ora oggetto di esame è il loro fondarsi su criteri di allocazione di responsabilità indipendenti dalla colpa. Se si considerano questi insiemi di regole quali possibili dirette fonti di regolazione dello scenario IoT (o, quantomeno, quali 'modelli' in grado di ispirare le opzioni riforma legislativa della materia), tale constatazione risulta in linea con la tradizionale idea che vede nella responsabilità oggettiva un mezzo in grado di garantire un'efficace ripartizione del rischio tra i soggetti coinvolti in organizzazioni e attività di natura complessa, soprattutto quando queste siano influenzate dall'evoluzione tecnologica¹²⁶.

Dovrebbe essere chiaro, al contempo, che il livello di *oggettività* di un sistema di responsabilità civile non può esser definito in astratto, ma dipende unicamente dalle regole che, operazionalmente, ne ispirano la concreta applicazione nella prassi¹²⁷.

Se si è concordi nel rinvenire uno dei principi fondanti la responsabilità oggettiva nell'idea che un individuo non debba in alcun caso sopportare i costi derivanti da eventi dannosi per lui del tutto inevitabili, allora il principale banco di prova per la

realizzazione di tale obiettivo concerne i criteri normativi applicati nella valutazione dell'elemento della causalità e della ripartizione dell'onere della prova tra le parti potenzialmente coinvolte in un contenzioso sul danno IoT¹²⁸.

In presenza di un sistema di responsabilità (oggettiva) come quello introdotto dalla Direttiva 85/374/CEE, all'attore viene richiesta la (sola) 'prova del danno, il difetto e la connessione causale tra difetto e danno' (art. 4). La disciplina europea non specifica cosa debba intendersi per 'connessione causale', lasciando dunque spazio a differenti concretizzazioni della norma a livello nazionale¹²⁹. Indipendentemente dal significato ascrivito al nesso di causalità in ciascuno stato membro (per esempio, in ossequio alla teoria della causalità adeguata; all'approccio *but for*; in considerazione della possibile rilevanza accordata a profili ulteriori quali l'immediatezza, la prevedibilità, la non improbabilità del danno, ecc.), la recente indagine promossa dalle istituzioni dell'Unione sull'applicazione della Direttiva mostra che le questioni relative alla mancanza di sufficienti prove della connessione tra il difetto e il danno rappresentano, in giudizio, una delle principali cause di rigetto delle domande di risarcimento (costituendo, nel loro insieme, il 53% della somma totale dei dinieghi di tutela)¹³⁰.

Tali informazioni lasciano ritenere che una diretta applicazione della disciplina della responsabilità da prodotto difettoso agli scenari IoT comporterebbe il rischio di una sterilizzazione ancor più radicale dell'efficacia di qualsiasi rimedio risarcitorio a cui poter fare astrattamente ricorso in tale settore. Invero, come in precedenza sottolineato, una delle più rilevanti problematiche poste in luce dagli ecosistemi IoT è legata all'ampio numero di operatori necessariamente coinvolti dal loro funzionamento, ognuno fornitore di una componente essenziale dell'architettura complessa.

Muovendo da queste premesse, torniamo ancora al Caso A: si immagini il proprietario della *smart home* gravato dall'onere di

provare il nesso causale intercorrente tra il danno materiale al suo immobile e un qualche ‘malfunzionamento’ del sistema domotico. Supponendo che all’origine dell’evento dannoso vi sia effettivamente stato un problema tecnico, sul piano più strettamente operativo questo può derivare da uno o più di numerosi fattori: un difetto in un singolo componente materiale; un errore nella programmazione del *software* integrato; un non corretto funzionamento di uno o più sensori interconnessi; un’interruzione nei servizi di connessione o nei sistemi di scambio dati tra le varie componenti dell’*hardware*, e via dicendo¹³¹.

In assenza di un intervento normativo a supporto della posizione del soggetto leso, qualsiasi domanda giudiziale di risarcimento si troverà onerata da un carico probatorio concernente l’esatta individuazione della fonte del danno che, pur senza necessariamente sconfinare in una *probatio diabolica*, potrà senza dubbio ridurre notevolmente il numero dei casi destinati a concludersi con un accoglimento della domanda risarcitoria¹³².

Tale considerazione consente di individuare la peculiare natura giuridica del danno prodotto nell’ambiente IoT, il quale, quantomeno in termini fattuali, risulta ‘indivisibile’, in quanto il pregiudizio subito dall’utente finale potrebbe essere stato causato da una pluralità di soggetti, il cui specifico contributo non può essere facilmente qualificato (e quantificato) dall’attore per via dell’inestricabile rete di interazioni instaurate tra i diversi livelli tecnologicamente interconnessi¹³³. In particolare, questa situazione risulta legata a quella che è stata tecnicamente definita una situazione di ‘indeterminatezza del convenuto’, che viene in essere quando: (i) l’attore risulta, secondo le previsioni normative in materia di prova, aver subito un danno a seguito di una condotta illecita; (ii) si è in presenza di una pluralità di soggetti, ognuno dei quali, indipendentemente dagli altri, ha agito in modo tale da essere causa del danno subito dalla parte attrice; ma (iii) risulta impossibile determinare, nel rispetto della disci-

plina dell'onere della prova, quale tra le condotta di tali soggetti costituisca la causa del pregiudizio subito dalla parte attrice, sebbene sia certo che almeno una di esse lo sia¹³⁴.

Come mostrato dagli studi di matrice comparatistica e giur-economica, se l'obiettivo di politica del diritto è quello di garantire, in tali tipologie di contenzioso, la piena reintegrazione del pregiudizio subito dal soggetto leso, i relativi procedimenti giudiziali dovrebbero essere disciplinati da norme che, quantomeno a livello settoriale, si discostino dal tipico sistema di distribuzione dell'onere della prova riferito al nesso di causalità¹³⁵.

Ciò è anzitutto dimostrato dall'univoco andamento storico che ha caratterizzato gli ordinamenti della tradizione giuridica occidentale, chiaramente orientato verso un progressivo aumento dell'attenzione rivolta al problema della causalità ipotetica, affrontato in modo tale da concedere via via più ampie possibilità di risarcimento in situazioni caratterizzate dalla presenza di una pluralità di soggetti responsabili¹³⁶. Una trattazione approfondita della questione andrebbe oltre l'ambito della presente indagine: limitandosi dunque ai soli casi più rilevanti, può farsi menzione della dottrina nordamericana della 'causalità alternativa', elaborata a seguito della decisione della Corte Suprema della California nel caso *Summer v. Tice*¹³⁷; o alla peculiare disciplina che codificazioni civili quali il BGB tedesco¹³⁸ o, più di recente, il BW olandese, riservano al problema in questione¹³⁹. Esempio forse ancor più significativo è quello rappresentato dal sistema francese: nonostante la completa assenza di una espressa disposizione contenuta nel *Code civil* del 1804, i giudici francesi hanno nel tempo affrontato più volte la questione dell'insufficienza dei risarcimenti, elaborando per le ipotesi di indeterminatezza del convenuto norme eccezionali in favore della parte lesa, sulla base di regimi di responsabilità solidale o inversioni dell'onere della prova circa la sussistenza del nesso di causalità¹⁴⁰.

Gli esiti delle indagini comparatistiche non testimoniano soltanto la diffusa presenza di norme dirette a disciplinare i casi di ‘indeterminatezza del convenuto’ (dirette dunque ad ascrivere la responsabilità in capo ad un gruppo di potenziali danneggianti anche qualora non sia possibile provare *quale*, tra di essi, abbia effettivamente cagionato il danno), ma mostrano altresì che l’applicazione di tali soluzioni normative è generalmente estesa ai giudizi vertenti su fattispecie di responsabilità oggettiva, ove la pretesa di risarcimento non risulta fondata necessariamente su una particolare condotta illecita, ovvero anche se nessun convenuto abbia agito negligenzemente nei confronti dell’attore¹⁴¹.

Alla luce di quanto emerso fin ora sembra possibile sostenere che, affinché possa essere efficace, un regime di responsabilità destinato agli ambienti IoT debba impernarsi su un qualche alleggerimento dell’onere probatorio concernente l’esatto processo causativo del danno, operante in favore del soggetto leso, rendendolo in grado di vincolare, potenzialmente, tutti gli operatori di mercato considerabili fornitori di un prodotto o di un servizio essenziale all’organizzazione o al funzionamento di ciascuno dei diversi livelli dello ‘*smart environment*’¹⁴². In termini generali, il fondamento di un simile regime di responsabilità potrebbe essere rinvenuto in argomenti, già accolti in dottrina, ed impernati sul concetto di ‘(in)giustizia relativa’, secondo i quali risulta ‘più ingiusto’ lasciare l’attore privo del risarcimento di un danno che ha *certamente* subito, piuttosto che riconoscere come responsabili soggetti che *potrebbero* aver contribuito al prodursi dell’evento dannoso¹⁴³.

Questa argomentazione risulta ancor più convincente nel settore IoT, ove la sua concretizzazione in una disciplina di dettaglio può essere funzionale alla realizzazione di obiettivi esplicitamente presi di mira negli indirizzi europei sul futuro dell’economia digitale: in particolare, al fine di costruire un sistema

di norme in grado di garantire certezza relativamente all'affidamento riposto dagli utilizzatori nella sicurezza delle moderne tecnologie, favorendo così lo sviluppo di un clima di fiducia tra tutti i soggetti coinvolti nelle nuove relazioni del mercato della tecnologia¹⁴⁴. Proprio nel quadro del diritto dell'Unione, del resto, si danno già oggi rilevanti esempi di interventi di armonizzazione di interi settori della responsabilità civile ispirati, proprio in punto di prova del danno, da regole assai peculiari, la cui eccentricità rispetto ai principi del diritto comune risulta giustificata da null'altro se non dagli espliciti obiettivi di politica legislativa volti a promuovere l'effettività della tutela risarcitoria, e con essa, l'attivismo dei centri del *private enforcement*¹⁴⁵.

Ove le argomentazioni sin qui esposte siano considerate sufficienti a giustificare l'introduzione di norme peculiari in tema di (prova del) nesso di causalità, è tuttavia opportuno, al fine di meglio articolare tale regime, tenere in debita considerazione alcuni ulteriori elementi tipici dell'ambiente IoT. In particolare, è noto che in situazioni caratterizzate dalla presenza di più soggetti responsabili dell'illecito una fondamentale alternativa, in termini normativi, è quella che risiede tra sistemi di responsabilità solidale (comune e gravante in capo a ciascun potenziale danneggiante per l'intero ammontare, e poi suscettibile di regresso nel rapporto interno tra i coobbligati) e parziale¹⁴⁶. Quanto alla presente analisi, la prima opzione sembra preferibile non solo in quanto essa costituisce una di quelle più frequentemente applicate negli ordinamenti della tradizione giuridica occidentale¹⁴⁷, ma soprattutto perché risulta tecnicamente adeguata alla tipologia di danni che si verificano tipicamente negli ambienti IoT. Sebbene siano di fatto 'indivisibili', i danni insorgenti in contesti IoT possono, ciò nonostante, risultare '(ri)allocabili' secondo la gravità delle colpe o la contribuzione all'illecito tra i vari (cor)responsabili.

Più specificamente, i criteri per la redistribuzione interna del danno potrebbero basarsi in primo luogo su una rigorosa

individuazione, tra i diversi fornitori e produttori, dell'esatta causa del danno cagionato all'utente. Tali parametri di regresso si fondano sul presupposto, apparentemente ragionevole, per cui ciascuno degli attori di mercato operanti nel settore dell'economia digitale si trovi in una posizione migliore rispetto a quella propria della vittima nel fornire effettiva prova di quali siano l'esatta natura e le cause dei difetti o dei malfunzionamenti emersi nel complesso sistema IoT. In ogni caso, quale criterio residuale di redistribuzione interna dei costi dell'evento lesivo, è possibile fare riferimento – seppur con i dovuti adeguamenti – alle indicazioni di politica normativa già prospettate dalla Commissione europea, favorendo così una riallocazione interna del peso economico del danno tra i più potenziali soggetti responsabili in base a criteri di creazione o di efficiente gestione del rischio¹⁴⁸.

7. Conclusioni

L'eterogenea serie di istanze e di potenziali conflitti di interessi immaginabili nell'ambito del moderno ambiente digitale è estremamente difficile da ricondurre all'interno delle categorie tradizionali della responsabilità civile. Se si concentra l'attenzione, più specificamente, sui regimi applicabili nel contesto IoT, occorre tenere in debita considerazione un elemento di portata decisiva: il notevole divario che divide le delicate questioni teoriche che minano, astrattamente, le più consolidate dottrine privatistiche, da un lato, e la sostanziale assenza di concreti casi di contenzioso, dall'altro.

Sebbene tale osservazione dovrebbe sconsigliare l'introduzione (o anche solo la discussione) di puntuali interventi legislativi in assenza di una più concreta evidenza di problemi della vita reale, essa costituisce nondimeno uno stimolo per indagini volte ad individuare le principali problematiche connesse all'al-

locazione, tra i più soggetti coinvolti, dei più concreti rischi di danno insiti nell'utilizzo di architetture digitali sofisticate. In queste pagine, muovendo da discipline 'modello' come quelle relative alla responsabilità da prodotto difettoso o alla protezione dei dati personali, si è inteso fornire alcuni spunti per orientamenti evolutivi che potrebbero, nel prossimo futuro, fungere da base per sforzi ermeneutici e legislativi che siano in grado di garantire un'efficace regolazione di diritto privato dell'ecosistema IoT.

In particolare, una volta preso atto che l'obiettivo delle politiche promosse dalle istituzioni europee muove dalla riconosciuta esigenza di una ripartizione dei nuovi rischi di danno tra tutti gli operatori del mercato digitale, emerge chiara l'esigenza di meglio articolare la (tradizionale) soluzione consistente nell'introduzione di un sistema di responsabilità oggettiva. Tra le questioni considerate, un profilo di rilevanza cruciale nell'elaborazione di un futuro regime di responsabilità applicabile nel settore IoT risulta legato all'inestricabilità della rete di prodotti e servizi su cui si basa il funzionamento di tale ambiente tecnologico. Dal concreto punto di vista dell'utente danneggiato, tale situazione può comportare gravi problemi di indeterminatezza del convenuto, con il rischio di privare di ogni effetto risarcitorio o deterrente qualunque regime di responsabilità che venga adottato in tale settore. Come dimostrano indagini guidate dal metodo storico-comparatistico o gius-economico, si tratta di questioni tutt'altro che nuove, la cui soluzione richiede anzitutto una revisione delle norme generali che, in materia di illecito, disciplinano il nesso di causalità e le relative modalità di ripartizione dell'onere probatorio tra i potenziali attori e convenuti nei contesti di contenzioso oggetto d'attenzione.

Note di chiusura

* Si tratta della relazione, corredata dell'apparato bibliografico, tenuta il 7.6.2021 nella *summer school* su "Digital innovation and sustainability" organizzata presso l'Università degli Studi di Napoli "L'Orientale" (Jean Monnet Module Digital Citizenship in the European Union – DiCit). Il saggio, aggiornato a quella data, non tiene conto delle più recenti evoluzioni della disciplina, e in particolare del dibattito sulle proposte di riforma, nel diritto UE, della responsabilità da prodotto difettoso e all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (formalizzate dalla Commissione UE nelle due distinte proposte di direttiva del 28.9.2022, COM(2022)495final e COM(2022)496final).

¹ Commissione Europea, *Strategia per il mercato unico digitale in Europa*, COM (2015) 192 final.

² Cfr. TEUBNER, *Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten*, in 218 *AcP* (2018), p. 156 ss.; WEBER, STEIGER, *New Liability Patterns in the Digital Era*, in SYNODINOU et al. (eds.), *EU Internet Law Regulation and Enforcement*, Cham, 2017, 201 ss.; PALMERINI, BERTOLINI, *Liability and Risk Management in Robotics*, in SCHULZE, STAUDENMAYER (eds.), *Digital Revolution: Challenges for Contract Law in Practice*, Baden-Baden, 2016, 225 ss.; PAGALLO, *The Law of Robots*, Cham, 2013, 115.

³ Commissione Europea, *Costruire un'economia dei dati europea*, COM (2017) 9 final, 14.

⁴ Commissione Europea, *L'intelligenza artificiale per l'Europa*, COM (2018) 237 final.

⁵ Cfr. per un ragguaglio MILLARD, KUAN HON, SINGH, *Internet of Things Ecosystems: Unpacking Legal Relationships and Liabilities*, in *IEEE* 2017, 286 ss.

⁶ Commissione Europea, *Staff Working Document, on the free flow of data and emerging issues of the European data economy*, SWD(2017) 2 final, 32 s.

⁷ Secondo un basilare approccio di analisi economica del diritto: cfr. LANDES, POSNER, *The Economic Structure of Tort Law*, Cambridge (Mass.), 1987, 4-5, 54; POSNER, *Strict Liability: A Comment*, in 2 *Journ. Legal Stud.* (1973), 205.

⁸ Chiaro il richiamo alla nozione di 'Cheapest Costs Avoider', per la cui compiuta elaborazione v. ovviamente CALABRESI, *The Costs of Accidents. A Legal and Economic Analysis*, New Haven-London, 1970, 135.

⁹ Proposta, questa, evidentemente ispirata a modelli c.d. 'no-fault': per una basilare introduzione, v. KEETON, O'CONNELL, *After Cars crash: The need for legal and insurance reform*, Irwin, 1967.

¹⁰ V. in primis, Commissione Europea, *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, COM(2021) 206 final; e v. pure la *Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL))*.

¹¹ Commissione Europea, *L'intelligenza artificiale per l'Europa*, cit., 22 s.

¹² Cfr. GEISTFELD, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, in 105 *Calif. Law Rev.* (2018), 1611 ss.; e nel dibattito europeo, EIDENMÜLLER, *The Rise of Robots and the Law of Humans*, in *ZEuP*, 2017, 765 ss.; WAGNER, *Produkthaftung für autonome Systeme*, in 217 *AcP* (2017), 707 ss.

¹³ Sul punto, v. PAPAPOPOULOS et al, *Leapfrog collaboration: Toward determinism and predictability in industrial-IoT applications*, in *IEEE SAC Symposium Internet of Things*, 2017, 1 ss.

¹⁴ Per ulteriori tentativi di definizione, v. la ricostruzione compiuta da NOTO LA DIEGA, *Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom*, in *Journ. Law & Econ. Reg.*, 2016, 69 ss., spec. 71 ss.

¹⁵ V. in dettaglio, MACAULAY, *RIoT Control: Understanding and Managing Risks and the Internet of Things*, Cambridge (Mass.), 2016, 5.

¹⁶ Sulle problematiche che anche a questo livello di dettaglio la tecnologia può porre, v. BUSCH, *Does the Amazon Dash Button Violate EU Consumer Law? Balancing Consumer Protection and Technological Innovation in the Internet of Things*, in *EuCML*, 2018, 78 ss.; THIERER, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, in *Rich. Journ. Law & Tech.*, 2015, 6.

¹⁷ Cfr. i saggi raccolti in NAKASHIMA, AGHAJAN (eds.), *Handbook of Ambient Intelligence and Smart Environments*, Cham, 2009; e l'ampia analisi contenuta nel report OCSE, *Data-Driven Innovation Big Data for Growth and Well-Being* disponibile all'indirizzo <http://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm/>.

¹⁸ WAGNER, *Robot Liability*, in LOHSSE, SCHULZE, STAUDENMAYER (eds.), *Liability for Artificial Intelligence and the Internet of Things*, Baden-Baden, 2019, 27 ss, spec. 47, discorre di 'unbundled products'; v. pure WEBER, *Liability in the Internet of Things*, in *EuCML*, 2017, 207 ss., a 208.

¹⁹ In una 'simplified view of the IoT stakeholders', MACAULAY, *RIoT Control: Understanding and Managing Risks and the Internet of Things*, cit., 11 ss., elenca: (i)

'users'; (ii) 'application service providers'; (iii) 'manufacturers'; (iv) 'network operators'; (v) 'data centers operators'; (vi) 'regulators'; (vii) 'independent third parties'.

²⁰ Ma per la testimonianza di una progressiva emersione di controversie, specie nell'ambiente nordamericano, v. l'ampia indagine comparatistica condotta da INFANTINO, WANG, *Algorithmic Torts: A Prospective Comparative Overview*, in 28 *Transn. Law & Cont. Probl.* (2019), 280 ss.

²¹ Cfr. TRAUTMAN, ORMEROD, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, in 72 *Univ. Miami Law Rev.* (2018), 761 ss.

²² Sull'applicazione alla domotica della tecnologia IoT ancora valida è l'illustrazione fornita nel volume CARBOU *et al* (eds), *Digital Home Networking*, London, 2013.

²³ Il caso ipotetico trae ispirazione dalla vicenda della causa, giudicata nell'ordinamento inglese, *Hufford v Samsung Electronics (UK) Ltd.*, [148 2014] EWHC 2956 (TCC).

²⁴ Per un analogo approccio metodologico, cfr. ADAR, SIRENA, *Principles and Rules in the Evolving European Law of Contract: From the PECL to the SECL, and Beyond*, in *Eur. Rev. Contr. Law*, 2013, 1 ss.

²⁵ Cfr. HODGES, *European regulation of consumer product safety*, Oxford, 2005, 21.

²⁶ Cfr. PURNHAGEN, *The Politics of Systematization in EU Product Safety Regulation: Market, State, Collectivity, and Integration*, Cham, 2013, 1 ss.

²⁷ Direttiva 2001/95/CE del Parlamento europeo e del Consiglio, del 3 dicembre 2001, relativa alla sicurezza generale dei prodotti.

²⁸ Oggi estese ai prodotti commercializzati online: v. *Comunicazione della Commissione sulla vigilanza del mercato dei prodotti venduti online* (2017/C 2501/01).

²⁹ MICKLITZ, *The Visible Hand of European Regulatory Private Law. The Transformation of European Private Law from Autonomy to Functionalism in Competition and Regulation*, in *Yearbook Eur. Law*, 2009, 3 ss.; e poi ID., *The Internal versus the External Dimension of European Private Law. A Conceptual Design and Research Agenda*, in CREMONA, MICKLITZ (eds.), *Private Law in the External Relations of the EU*, Oxford, 2016, 9 ss.

³⁰ CHEREDNYCHENKO, *Public Supervision over Private Relationships: Towards European Supervision Private Law?*, in *Eur. Rev. Priv. Law*, 2014, 38 ss.

³¹ V. per una recente panoramica, ZOPPINI, *Il diritto privato e i suoi confini*, Bologna, 2021, p. 239 ss.

³² Direttiva 2006/42/CE del Parlamento europeo e del Consiglio del 17 maggio 2006 relativa alle macchine e che modifica la direttiva 95/16/CE (rifusione).

³³ Direttiva 2014/53/UE del Parlamento europeo e del Consiglio del 16 aprile 2014 concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE.

³⁴ Direttiva 89/391/CEE del Consiglio, del 12 giugno 1989, concernente l'attuazione di misure volte a promuovere il miglioramento della sicurezza e della salute dei lavoratori durante il lavoro.

³⁵ CAFAGGI, *A Coordinated Approach to Regulation and Civil Liability in European Law: Rethinking Institutional Complementarities*, in ID. (ed.), *The Institutional Framework of European Private Law*, Oxford, 2006, 191.

³⁶ Sull'impossibilità di isolare le problematiche di responsabilità civile dai più tradizionali approcci di regolazione, cfr. RIZZI, *Non-Measurable Negotiations. The EU between Transnational Regulation of Pharmaceuticals and Private Law*, in CREMONA, MIKHLITZ (eds.), *Private Law in the External Relations of the EU*, cit., 273 ss., spec. 290 ss.

³⁷ V. WEBER, STEIGER, *New Liability Patterns in the Digital Era*, cit., 205.

³⁸ Cfr. SCOTT, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, in 67 *Md. Law Rev.* (2008), 425 ss., a 457.

³⁹ Cfr. ZENO-ZENCOVICH, GIANNONE CODIGLIONE, *Ten Legal Perspectives on the "Big Data Revolution"*, in *Concorrenza e Mercato* 2016, 23 ss., in part. 46 s.

⁴⁰ Cfr. NOTO LA DIEGA, WALDEN, *Contracting for the 'Internet of Things': Looking into the Nest*, in 7 *Eur. Journ. Law Tech*, 2016.

⁴¹ Per una panoramica, VAN DAMM, *European Tort Law*, Oxford, 2006, 184 ss.

⁴² Per l'interazione tra lo sviluppo di innovazioni tecnologiche e l'emersione di questioni connesse alla responsabilità degli operatori, cfr. già in passato NYCUM, *Liability for malfunction of a computer program*, in 7 *Rutgers Journ. Comp. Tech. & Law* (1979), 1 ss.; CRONIN, *Consumer Remedies for Defective Computer Software*, in 28 *Wash. Univ. Journ. Urb. & Contemp. Law* (1985), 273 ss.

⁴³ Cfr. BRÜGGERMEIER, *Tort Law in the European Union*, Alphen aan den Rijn, 2015, 166.

⁴⁴ WEBER, *Liability in the Internet of Things*, cit., 210; MILLARD, KUAN HON, SINGH, *Internet of Things Ecosystems: Unpacking Legal Relationships and Liabilities*, cit., 280.

⁴⁵ Cfr. MACHNIKOWSKY, *Introduction*, in ID. (ed.), *European Product Liability. An Analysis of the State of the Art in the Era of New Technologies*, Cambridge-Anтверp-Portland, 2016, 1 ss., spec. 8 ss.

⁴⁶ Direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi.

⁴⁷ Cfr. WHITTAKER, *Introduction to fault in product liability*, in ID. (ed.), *The development of product liability*, Cambridge, 2010, 1 ss., spec. 20 ss.

⁴⁸ V. HOWELLS, *Product liability: A History of Harmonisation*, in HARTKAMP et al (eds), *Towards a European Civil Code*, Alphen aan den Rijn, 2011, 889 ss., a 894 ss.

⁴⁹ Per un'esemplificazione di questo approccio culturale, v. REIMANN, *Product liability*, in BUSSANI, SEBOK (eds.), *Comparative Tort Law*, Cheltenham, 2015, 250 s., 263; e in chiave maggiormente operativa, sull'influenza effettivamente esercitata dalle regole proprie di questo peculiare settore sul complessivo sistema della responsabilità civile, ID., *Product Liability in a Global Context: the Holow Victory of the European Model*, in *Eur. Rev. Priv. Law*, 2003, 128 ss., a 153 s.

⁵⁰ V. Direttiva 85/374/CEE, considerando 1: 'il ravvicinamento delle legislazioni nazionali in materia di responsabilità del produttore per i danni causati dal carattere difettoso dei suoi prodotti è necessario perché le disparità esistenti fra tali legislazioni possono falsare il gioco della concorrenza e pregiudicare la libera circolazione delle merci all'interno del mercato comune determinando disparità nel grado di protezione del consumatore contro i danni causati alla sua salute e ai suoi beni da un prodotto difettoso'. In dottrina, v. HODGES, *Approaches to product liability in the EU and Member States*, in FAIRGRIEVE (ed.), *Product liability in comparative perspective*, 2005, 192, 195 ('[t]he area of product liability has been something of an ideological battleground between what might be briefly described as supporters of consumer protection and of commercial continuity').

⁵¹ V. Direttiva 85/374/CEE, considerando 2.

⁵² Commissione Europea, *Staff Working Document, on the free flow of data and emerging issues of the European data economy*, cit., 32 s.

⁵³ Commissione Europea, *Libro bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*, COM (2020) 65 final, 17.

⁵⁴ V. per una panoramica di temi rilevanti, MONTINARO, *Responsabilità da prodotto difettoso e tecnologie digitali tra soft law e hard law*, in *Persona e merc.*, 2020, 349 ss.

⁵⁵ Pur nel silenzio della Direttiva sul punto, l'interpretazione datane dalla Corte di giustizia è sempre stata nel senso di un provvedimento che 'non può essere inteso come diretto a lasciare agli Stati membri la possibilità di mantenere un regime generale di responsabilità per danno da prodotti difettosi che

differisca da quello previsto dalla direttiva': v. Corte giust., 25 aprile 2002, C-52/00, *Commissione delle Comunità europee c. Repubblica francese*, § 21; Corte giust., 25 aprile 2002, C-154/00, *Commissione delle Comunità europee c. Repubblica ellenica*; Corte giust., 25 aprile 2002, C-183/00, *Sánchez c. Medicina Asturiana SA*. Sui persistenti margini di discrezionalità degli Stati membri, v. WHITE, *Directive 85/374/EEC concerning liability for defective products: in the name of harmonisation, the internal market and consumer protection*, in GILIKER (ed), *Research Handbook on EU Tort Law*, Cheltenham, 2017, 128 ss., in part. 136 ss.

⁵⁶ Relazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo sull'applicazione della direttiva del Consiglio relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi (direttiva 85/374/CEE), COM(2018) 246 final.

⁵⁷ Per un'essenziale rassegna, v. WAGNER, *Robot Liability*, cit., 41 ss.; WEBER, *Liability in the Internet of Things*, cit., 210.

⁵⁸ Cfr. HOWELLS, *Comparative product liability*, Aldershot, 1993, 30.

⁵⁹ Corte giust., 10 gennaio 2006, C-402/03, *Skov Æg c. Bilka Lavprisvarehus A/S*.

⁶⁰ Direttiva 85/374/CEE, Art. 3, par. 1: 'Il termine «produttore» designa il fabbricante di un prodotto finito, il produttore di una materia prima o il fabbricante di una parte componente, nonché ogni persona che, apponendo il proprio nome, marchi marchio o altro segno distintivo sul prodotto, si presenta come produttore dello stesso'.

⁶¹ Direttiva 85/374/CEE, Art. 3, par. 2: 'Senza pregiudizio della responsabilità del produttore, chiunque importi un prodotto nella Comunità europea ai fini della vendita, della locazione, del «leasing» o di qualsiasi altra forma di distribuzione nell'ambito della sua attività commerciale, è considerato produttore del medesimo ai sensi della presente direttiva ed è responsabile allo stesso titolo del produttore'.

⁶² Direttiva 85/374/CEE, Art. 3, par. 3: 'Quando non può essere individuato il produttore del prodotto si considera tale ogni fornitore a meno che quest'ultimo comunicati al danneggiato, entro un termine ragionevole, l'identità del produttore o della persona che gli ha fornito il prodotto. Le stesse disposizioni si applicano ad un prodotto importato, qualora questo non rechi il nome dell'importatore di cui al paragrafo 2, anche se è indicato il nome del produttore'.

⁶³ Cfr. WHITTAKER, *The EEC Directive on product liability*, in *Yearbook Eur. Law* 1985, 233 ss., spec. 269.

⁶⁴ Corte giust., 21 dicembre 2011, C-495/10, *Centre hospitalier universitaire de Besançon c. Thomas Dutruieux and Caisse primaire d'assurance maladie du Jura*, § 28.

⁶⁵ Corte giust., 10 maggio 2001, C-203/99, *Henning Vedfeld c. Århus Amtskommune*.

⁶⁶ Cfr. FAIRGRIEVE *et al*, *Product Liability Directive*, in MACHNIKOWSKY (ed), *European Product Liability. An Analysis of the State of the Art in the Era of New Technologies*, cit., 17 ss., a 35. Per il rilievo di come l'approccio adottato dalla Corte di giustizia per stabilire se l'evento dannoso possa essere ricondotto al prodotto o al servizio finisca per dipendere dall'esame del caso concreto, v. WUYTS, *The product liability directive - more than two decades of defective products in Europe*, in *Journ. Eur. Tort Law* 2014, 1 ss., 6.

⁶⁷ Cfr. LICHTMAN, E.P. POSNER, *Holding Internet Service Providers Accountable*, in *Sup. Ct. Econ. Rev.*, 2006, 221 ss., 233 ss.

⁶⁸ C. BUSCH, *Rethinking Product Liability Rules for Online Marketplaces: A Comparative Perspective*, in *49th Annual Research Conference on Communications, Information, and Internet Policy*, Washington, DC, September 22-24, 2021 (disponibile su ssrn.com).

⁶⁹ V. R. PETRUSIO- G. SMORTO, *Trasformazione della filiera distributiva e responsabilità delle piattaforme del commercio elettronico nella proposta di direttiva "sulla responsabilità per danno da prodotti difettosi"* in questo volume.

⁷⁰ V. Oberdorf *c. Amazon.com, Inc.*, 936 F.3d 182, (3d Cir. 2019).

⁷¹ WEBER, STEIGER, *New Liability Patterns in the Digital Era*, cit., 203 s.

⁷² Direttiva 85/374/CEE, Art. 2, par. 1; e v. BRÜGGERMEIER, *Tort Law in the European Union*, cit., 176, il quale, anche alla luce della regola di esclusione di cui all'Art. 7(c), considera la più appropriata definizione di 'prodotto' come 'any professional and for economic purpose manufactured movable thing'.

⁷³ Sul tema, v. RUSTAD, KOENIG, *The Tort of Negligent Enablement of Cybercrime*, in *20 Berkeley Tech. Law Journ.* (2005), 1553 ss., in part. 1577; e tra i primi commentatori della Direttiva, WHITTAKER, *European Product Liability and Intellectual Products*, in *105 Law Quarterly Review* (1989), 125 ss.

⁷⁴ Cfr. BUTLER, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, in *50 Univ. Mich. Journ. Law Reform* (2017), 913 ss., 926; GEISTFELD, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, cit.; WAGNER, *Produkthaftung für autonome Systeme*, cit., 707 ss.

⁷⁵ Sul punto, significative sono apparse le conclusioni del documento Commission Staff Working Document SWD(2018) 157 final, *Evaluation of Coun-*

Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. Accompanying the Report COM(2018) 246 final, 24, 23 s.: 'A clarification of the concept "product", e.g., with regards to software, may therefore contribute to improving effectiveness'.

⁷⁶ Commissione Europea, *Interrogazione scritta con risposta n. 706/88 dell'on. Gijs de Vries* [1989], in *Gazz. uff.*, 8.3.1989, 42.

⁷⁷ Si pone in tal senso l'attività svolta presso i gruppi di lavoro attivi sul tema presso l'European Law Institute: v. negli ultimi anni, E.L.I., *Guiding Principles for Updating the Product Liability Directive for the Digital Age*, prepared by Professor Christian Twigg-Flesner, 5 s.; e poi E.L.I., *Public Consultation on Civil Liability Adapting liability rules to the digital age and artificial intelligence*, 2022, 9 ss.

⁷⁸ V. in particolare HOWELLS, TWIGG-FLESNER, WILLETT, *Product Liability and Digital Products*, in SYNODINOU *et al* (eds), *EU Internet Law Regulation and Enforcement*, cit., 191: 'The crucial policy decision should therefore be to class as a product software that is a final product and causes material damage or is a component of the product that makes it function autonomously to cause damage, but to exclude information in written or digital form from the strict product liability regime'.

⁷⁹ Nello stesso senso, FAIRGRIEVE *et al*, *Product Liability Directive*, cit., 46 s.

⁸⁰ Così, Commissione Europea, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*, COM(2020) 64 final, 15.

⁸¹ Direttiva 85/374/CEE, Art. 6, par. 1.

⁸² BRÜGGERMEIER, *Tort Law in the European Union*, cit., 176 ss.

⁸³ Si propone il testo del *U.S. Restatement of Tort (Third): Products Liability*, § 2. *Categories of Product Defect*: 'A product is defective when, at the time of the sale or distribution, it contains a manufacturing defect, is defective in design, or is defective because of inadequate instructions or warnings. A product: (a) contains a manufacturing defect when the product departs from its intended design even though all possible care was exercised in the preparation and marketing of the product; (b) is defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the alternative design renders the product not reasonably safe; (c) is defective because of inadequate instructions or warnings when the foreseeable risks of

harm posed by the product could have been reduced or avoided by the provision of reasonable instructions or warnings by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the instructions or warnings renders the product not reasonably safe’.

⁸⁴ VAN DAMM, *European Tort Law*, cit., 377.

⁸⁵ Sebbene in diversi contesti argomentativi, sia BRÜGGERMEIER, *Tort Law in the European Union*, cit., 181, che BUTLER, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, cit., 917, concordano sul fatto che il test *risk-utility* finisca operativamente per introdurre uno standard di diligenza in un regime di responsabilità che dovrebbe essere invece oggettivo.

⁸⁶ Direttiva 85/374/CEE, Art. 2, par. 1.

⁸⁷ Cfr. WIEBER LENS, *Warning: A Post-Sale Duty to Warn Targets Small Manufacturers*, in *Utah Law Rev.* (2014), 1013 ss.; ROSS, PRINCE, *Post-Sale Duties. The Most Expansive Theory in Products Liability*, in *74 Brooklyn Law Rev.* (2009), 963 ss.

⁸⁸ *U.S. Restatement of Tort (Third): Products Liability*, § 10.

⁸⁹ Cfr. *infra*, § 6.

⁹⁰ In tal senso BUTLER, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, cit., 918 s.; e v. pure LICHTMAN, E.P. POSNER, *Holding Internet Service Providers Accountable*, cit., 223.

⁹¹ Per una rassegna di temi problematici, v. F.P. PATTI, *The European Road to Autonomous Vehicles*, in *43 Fordham Int’l Law Journ.* (2019), 125 ss., a 137 ss.

⁹² Cfr. sul punto, BORGHETTI, *How can Artificial Intelligence be Defective?*, in LOHSSE, SCHULZE, STAUDENMAYER (eds.), *Liability for Artificial Intelligence and the Internet of Things*, cit., 63 ss., in part. 67 s.

⁹³ Direttiva 85/374/CEE, Art. 9, par. 1.

⁹⁴ Direttiva 85/374/CEE, Art. 9, par. 2.

⁹⁵ Direttiva 85/374/CEE, considerando 9; WHITTAKER, *Liability for products. English law, French law, and European harmonisation*, Oxford, 2005, 507 s.

⁹⁶ Corte giust., *Henning Vedfald c. Århus Amtskommune*, cit., § 32 s.

⁹⁷ Cfr. FAIRGRIEVE *et al*, *Product Liability Directive*, cit., 82, concludendo nel senso che ‘the exhaustive enumeration contained in art 9 consists not only in the listing therein of all heads of damage and others not eligible for recovery on the basis of the Directive, but that all of the heads of damage listed therein must be eligible for recovery on the basis of domestic law’.

⁹⁸ Cfr. BORGHETTI, *Heads of Damages. Comments*, in TERRY, STRAETMANS, COLAERT (eds.), *Landmark Cases of EU Consumer Law. In Honour of Jules Stuyck*, Cambridge-Antwerp-Portland, 2013, 317 ss., a 321.

⁹⁹ Corte giust., 5 marzo 2015, C-503-504/13, *Boston Scientific Medizintechnik GmbH c. AOK Sachsen-Anhalt e Betriebskrankenkasse RWE*.

¹⁰⁰ Cfr. ancora FAIRGRIEVE *et al*, *Product Liability Directive*, cit., 85.

¹⁰¹ Sono i dati riportati da BUTLER, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, cit., 921.

¹⁰² Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR).

¹⁰³ Esplicitamente Corte giust., 4 giugno 2009, C-285/08, *Société Moteurs Le-roy Somer c. Société Dalkia France, Société Ace Europe*, § 25.

¹⁰⁴ Cfr. WHITE, *Directive 85/374/EEC concerning liability for defective products: in the name of harmonisation, the internal market and consumer protection*, cit., 136 s.

¹⁰⁵ Cfr. HOWELLS, *Product liability: A History of Harmonisation*, cit., 894.

¹⁰⁶ Cfr. BORGHETTI, *Heads of Damages. Comments*, cit., 323.

¹⁰⁷ FABIANO, *Internet of Things and the Legal Issues related to the Data Protection Law according to the new European General Data Protection Regulation*, in *Athens Journ. Law*, 2017, 201 ss., spec. 203 s.

¹⁰⁸ Regolamento (UE) 2016/679, considerando 146.

¹⁰⁹ Carta dei diritti fondamentali dell'Unione Europea, Art. 47. Cfr. REICH, *The Principle of Effectiveness and EU Contract Law*, in RUTGERS, SIRENA (eds.), *Rules and Principles in European Contract Law*, Cambridge-Antwerp-Portland, 2015, 46; e in un particolare settore, F.P. PATTI, *The Effectiveness of Consumer Protection in Sales Contracts. Some Observations from Recent European Case Law*, in *EuCML*, 2015, 179 ss.

¹¹⁰ Regolamento (UE) 2016/679, Art. 79, par. 1; in tema, VAN DER SLOOT, *Where is the Harm in a Privacy Violation? Calculating the Damages Afforded in Privacy Cases by the European Court of Human Rights*, in *JIPITEC*, 2017, 322 ss.

¹¹¹ Regolamento (UE) 2016/679, Art. 4(7).

¹¹² Regolamento (UE) 2016/679, Art. 4(2).

¹¹³ Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, Art. 23, par. 1.

¹¹⁴ Cfr. SCHUMACHER, *Risks of Liability for breaches of data protection law*, in RÜCKER, KUGLER (eds.), *New European General Data Protection Regulation. A Practitioner's Guide*, München, 2018, 186 ss., 192.

¹¹⁵ STUDER, DE WERRA, *Regulating cybersecurity. What civil liability in case of cyber-attacks?*, in *Expert Focus*, 2017, 511 ss., 513 s.

¹¹⁶ Regolamento (UE) 2016/679, Art. 82, par. 2.

¹¹⁷ Cfr. RÜCKER, *Scope of Application of the GDPR*, in RÜCKER, KUGLER (eds.), *New European General Data Protection Regulation. A Practitioner's Guide*, cit., 9 ss., 34.

¹¹⁸ Regolamento (UE) 2016/679, Art. 32, par. 1(b).

¹¹⁹ Regolamento (UE) 2016/679, Art. 32, par. 1(d).

¹²⁰ VAN ALSENOY, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, in *JIPITEC* 2016, 271 ss., 282; STUDER, DE WERRA, *Regulating cybersecurity*, cit., 514.

¹²¹ Regolamento (UE) 2016/679, Art. 82, par. 3.

¹²² Direttiva 95/46/CE, Art. 23, par. 2: 'il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità se prova che l'evento dannoso non gli è imputabile'.

¹²³ Direttiva 95/46/CE, considerando 55: 'considerando che, in caso di violazione dei diritti delle persone interessate da parte del responsabile del trattamento, le legislazioni nazionali devono prevedere vie di ricorso giurisdizionale; che i danni cagionati alle persone per effetto di un trattamento illecito devono essere riparati dal responsabile del trattamento, il quale può essere esonerato dalla propria responsabilità se prova che l'evento dannoso non gli è imputabile, segnatamente quando dimostra l'esistenza di un errore della persona interessata o un caso di forza maggiore'.

¹²⁴ VAN ALSENOY, *Liability under EU Data Protection Law*, cit., 283.

¹²⁵ Corte giust., 13 maggio 2014, C-131/12, *Google Spain SL and Google Inc. c. Agencia Española de Protección de Datos (AEPD)*, § 38: 'nella misura in cui l'attività di un motore di ricerca può incidere, in modo significativo e in aggiunta all'attività degli editori di siti web, sui diritti fondamentali alla vita privata e alla protezione dei dati personali, il gestore di tale motore di ricerca quale soggetto che determina le finalità e gli strumenti di questa attività deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che detta attività soddisfi le prescrizioni della direttiva 95/46, affinché le garanzie previste da quest'ultima possano sviluppare pienamente i loro effetti e possa essere effettivamente realizzata una tutela efficace e completa delle

persone interessate, in particolare del loro diritto al rispetto della loro vita privata⁷.

¹²⁶ Per uno sguardo comparative sulle funzioni della responsabilità oggettiva, nel panorama europeo, v. OERTEL, *Objective Haftung in Europa*, Tübingen, 2010, 23.

¹²⁷ Per il senso più profondo della distinzione tra regola declamata e regola operativa, v. ovviamente SACCO, *Legal Formants: A Dynamic Approach to Comparative Law (Instalment I of II)*, in 39 *Am. Journ. Comp. Law* (1991), 1 ss.; e per una declinazione nel settore oggetto d'esame, REIMANN, *Product liability*, cit., 259.

¹²⁸ Cfr. BUSSANI, INFANTINO, *Tort Law and Legal Culture*, in 63 *Am. Journ. Comp. Law* (2015), 77 ss. 97 s.; OWEN, *Figuring Foreseeability*, in 44 *Wake Forest Law Rev.* (2009), 1277

¹²⁹ WUYTS, *The product liability directive – more than two decades of defective products in Europe*, cit., 25; WHITTAKER, *Liability for products. English law, French law, and European harmonisation*, cit., 509.

¹³⁰ V. ancora Commission Staff Working Document SWD(2018), cit., 25.

¹³¹ Per l'interoperabilità di apparecchi e sistemi come un elemento coesenziale alla progettazione di un ambiente IoT, v. ancora MACAULAY, *RIoT Control: Understanding and Managing Risks and the Internet of Things*, cit., 197 ss.

¹³² Cfr. TEUBNER, *Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten*, cit., 158; con alcuni distinguo, che tuttavia si basano sulla (non sempre realistica) premessa della possibilità di isolare il contributo di uno specifico elemento del Sistema IoT come univoca fonte unitaria del danno, v. HOWELLS, TWIGG-FLESNER, WILLETT, *Product Liability and Digital Products*, cit., 193.

¹³³ Sebbene in un contest diverso, v. KLEFFNER, *Successive Torts Resulting in a Single, Indivisible Injury: Plaintiffs, Prepare to Prove the Impossible*, in 64 *Mo. Law Rev.* (1999), 1003.

¹³⁴ STEEL, *Proof of Causation in Tort Law*, Cambridge, 2015, 139.

¹³⁵ Per una panoramica, KORNHAUSER, *Economic Analysis of Joint and Several Liability*, in ARLEN (ed.), *Research Handbook on the Economics of Torts*, Cheltenham, 2013 199; INFANTINO, ZERVOGIANNI, *The Comparative Assessment*, in EADD (eds.), *Causation in European Tort Law*, Cambridge, 2017, 587 ss., a 632 ss.

¹³⁶ Più nel dettaglio, con analisi fondate sulla comparazione, INFANTINO, *Causation theories and causation rules*, in BUSSANI, SEBOK (eds.), *Comparative Tort Law*, cit., 279 ss., a 286 ss.; ROGERS (ed.), *Unification of Tort Law: Multiple Tortfeasors*, Alphen aan den Rijn, 2004.

¹³⁷ 33 Cal.2d 80, 199 P.2d 1.

¹³⁸ Art. § 830, Abs. 1, BGB, sul quale, per una trattazione descrittiva, cfr. MAGNUS, *Multiple Torfeasors under German Law*, in ROGERS (ed.), *Unification of Tort Law: Multiple Torfeasors*, cit., 87.

¹³⁹ Cfr. VAN BOOM, *Multiple Torfeasors under Dutch Law*, in ROGERS (ed.), *Unification of Tort Law: Multiple Torfeasors*, cit., 135, con riguardo all'Art. 6:99 del codice civile olandese ('Where the damage is caused by two or more events, for each of which another person is liable, and it is ascertained that the damage originates from at least one of these events, then each of these liable persons is joint and several liable for that damage, unless a liable person proves that this specific damage is not caused by the event for which he himself is liable') e all'Art. 6:166 ('If a person, when belonging to a group of people, causes damage through a tortious act and the risk that this damage could be inflicted should already have refrained the other persons, belonging to that group, from their collective behaviour, then each of the members of this group is joint and several liable as far as this collective behaviour can be attributed to him individually. In their internal relationship all liable persons must contribute for equal shares in the payable damages, unless fairness demands, in view of the prevailing circumstances, another imputation').

¹⁴⁰ BORGHETTI, *The development of product liability in France*, in WHITTAKER (ed.), *The development of product liability*, cit., 87 ss., 99.

¹⁴¹ V. diffusamente STEEL, *Proof of Causation in Tort Law*, cit., 192 s.

¹⁴² Indirizzo di politica del diritto, quello in commento, sintetizzabile secondo la seguente idea: 'A condizione che l'attore abbia dimostrato il danno subito nell'utilizzo del sistema IoT, gli operatori coinvolti nella fornitura di una o più delle componenti essenziali di quest'ultimo sono responsabili per l'intero ammontare del danno, così da garantire un pieno risarcimento al soggetto interessato'.

¹⁴³ Più nello specifico, l'analisi condotta nel settore IoT porta a rintracciare tutte le tre condizioni che, in termini di politica del diritto, sono considerate necessarie per giustificare l'imposizione di un regime di responsabilità solidale come quello accennato nel testo: (i) la presenza di oggettive difficoltà probatorie per il danneggiato; (ii) la condivisa presenza di istanze volte all'individuazione di un centro di imputazione capace di assicurare tutela risarcitoria alla vittima, favorendo una riallocazione dei costi attesi dei danni; (iii) istanze di prevenzione generale, connesse alla natura indivisibile del danno: cfr. ampiamente KORNHAUSER, *Economic Analysis of Joint and Several Liability*, cit., 200 ss.

¹⁴⁴ In un quadro teorico più ampio, v. WENDEHORST, *Consumer Contracts and the Internet of Things*, in SCHULZE, STAUDENMAYER (eds.), *Digital Revolution: Challenges for Contract Law in Practice*, cit., 189.

¹⁴⁵ Perfetto esempio dell'atteggiamento descritto nel testo è rappresentato dalla disciplina sul danno da illecito anticoncorrenziale, armonizzata in Europa dalla Direttiva 2014/104/UE del Parlamento europeo e del Consiglio del 26 novembre 2014, relativa a determinate norme che regolano le azioni per il risarcimento del danno ai sensi del diritto nazionale per violazioni delle disposizioni del diritto della concorrenza degli Stati membri e dell'Unione europea. Per una più puntuale disamina delle peculiarità introdotte da quel regime normativo (recepito in Italia con il d.lgs. 19 gennaio 2017, n. 3) e per un tentativo di messa a sistema proprio alla luce degli obiettivi di politica del diritto che hanno ispirato l'intervento del legislatore dell'Unione, sia concesso il rinvio al mio *Effettività delle tutele e funzioni della responsabilità civile (dalla prospettiva del 'danno antitrust')*, in MANTUCCI, G. PERLINGIERI, D'AMBROSIO (a cura di), *Dibattito sulle ricerche della dottrina civilistica nel biennio 2017-2018*, Napoli, 2021, 995 ss., spec. 1020 ss.

¹⁴⁶ Su possibili modelli alternativi di risoluzione dell'incertezza causale, cfr. GILEAD, GREEN, KOCH, *Causal Uncertainty and Proportional Liability: Analytical and Comparative Report*, in IDD. (eds), *Proportional Liability: Analytical and Comparative Perspectives*, Berlin, 2013, 1 ss., a 10.

¹⁴⁷ INFANTINO, ZERVOGIANNI, *The Comparative Assessment*, cit., 646 s.; STEEL, *Proof of Causation in Tort Law*, cit., cit., 194.

¹⁴⁸ Cfr. *retro*, § 1. Più nel dettaglio, per un'articolata analisi di soluzioni volte a garantire una ripartizione proporzionale di responsabilità, e dei relativi benefici nella prospettiva di future azione di danno nel settore del digitale, MARTIN CASALS, *Causation and Scope of Liability in the Internet of Things (IoT)*, in LOHSSE, SCHULZE, STAUDENMAYER (eds.), *Liability for Artificial Intelligence and the Internet of Things*, cit., 201 ss., 219 ss.

Consenso e intelligenza artificiale: limiti e prospettive*

ANTONINA ASTONE

Sommario: 1. Conoscibilità della decisione algoritmica e autodeterminazione. - 2. Dati misti e consenso nel GDPR. - 3. I limiti del consenso nei sistemi basati sull'intelligenza artificiale. - 4. Qualche soluzione prospettabile. - 5. Buona fede, trasparenza e governabilità dei meccanismi di funzionamento del trattamento algoritmico.

1. Conoscibilità della decisione algoritmica e autodeterminazione

Per analizzare il problema complesso del rapporto tra autodeterminazione e strumenti o sistemi dotati di intelligenza artificiale appare opportuno partire da quanto la Corte Costituzionale tedesca nel 1983¹, nella c.d. *Volkszählungsurteil*, sentenza sul censimento, ha scritto nel delineare un “diritto fondamentale all'autodeterminazione informativa” con riferimento all'utilizzo tecnologico dei dati personali. Dopo avere sottolineato come l'autodeterminazione presuppone, anche per il trattamento delle informazioni, che ai singoli individui sia data la libertà di decidere se scegliere di intraprendere o di rinunciare a determinate attività, compresa la possibilità di comportarsi di conseguenza, la Corte precisa che “Chi non è in grado di sapere quali delle sue informazioni personali sono note in determinati contesti del suo ambiente sociale, e chi non può valutarne la conoscenza da parte di possibili interlocutori, può essere considerevolmente limitato nella sua libertà di autodeterminarsi”.

Ed è proprio questo il problema su cui, a distanza di anni, continua a misurarsi ancora la giurisprudenza in quanto la co-

noscibilità delle modalità di trattamento dei dati, che è alla base dell'Intelligenza artificiale², rimane una questione aperta, dal momento che i processi di apprendimento, come il *machine learning* che la caratterizzano, sembrano in grado di sfuggire persino al controllo umano.

La Suprema Corte³, in continuità con alcuni significativi interventi del Consiglio di Stato⁴, pur sottolineando come nel “caso di utilizzo di un sistema automatizzato di calcolo, il presupposto della liceità del relativo trattamento dei dati personali è costituito dalla validità del consenso che si assume prestato al momento dell'adesione”, tuttavia, ha evidenziato come sia necessaria, preventivamente, la sussistenza della conoscibilità della decisione algoritmica in quanto “non può logicamente affermarsi che l'adesione a una piattaforma da parte dei consociati comprenda anche l'accettazione di un sistema automatizzato, che si avvale di un algoritmo, per la valutazione oggettiva di dati personali, laddove non siano resi conoscibili lo schema esecutivo in cui l'algoritmo si esprime e gli elementi all'uopo considerati”.

Ma è evidente che esistono indubbie difficoltà connesse alla conoscibilità dei meccanismi che presidiano allo svolgimento dei compiti di cui è investito l'algoritmo, che trovano il loro *ubi consistam* nel fatto che le informazioni e le conoscenze conseguentemente acquisite, che connotano i sistemi di intelligenza artificiale, sono sorrette da un processo metodologico particolare in cui i dati costituiscono il “motore trainante” degli algoritmi che hanno il compito di individuare correlazioni difficilmente rinvenibili dalle “classiche” tecnologie⁵. Ed è questo uno dei fattori che rende i sistemi c.d. AI molto complessi anche da regolamentare per il diritto e pone in crisi quelle logiche “proprietary”, sottese al diritto all'autodeterminazione, che trovano le loro radici nel pensiero di Locke⁶ e che si sono trasfuse, nelle moderne codificazioni, con l'individuazione del consenso

come base giuridica fondamentale, per compiere atti di disposizione che attengono a diritti fondamentali.

Peraltro allo stato attuale, nel mercato globale, emerge sempre più lo stretto legame fra economia, intelligenza artificiale e popolazione che, con la propria attività svolta sia nel mondo “reale” che in quello “virtuale”, costituisce la principale fonte di dati che, ormai notoriamente, hanno assunto anche l’accezione di beni in senso economico⁷.

È questa la ragione per cui nella geo-politica dell’attuale società postmoderna si registra un interesse molto forte sulla intelligenza artificiale, soprattutto da quando il Consiglio di Stato della Repubblica popolare cinese, nel 2017, ha elaborato il Piano di sviluppo per una nuova generazione d’intelligenza artificiale (Aidp), ponendosi il proposito di acquisire nel campo la *leadership*. Le altre superpotenze si sono attivate per evitare che la Cina abbia, anche in questo settore, un primato, a livello eurounitario⁸, si è puntato l’acceleratore sull’AI come dimostra il “proludio” di risoluzioni, libro bianco, istituzione di gruppo di esperti e da ultimo la bozza di regolamento sull’A.I.⁹, da cui traspare l’esigenza e, quindi, il tentativo quanto mai arduo, di coniugare l’uso di questa tecnologia con la tutela dei diritti fondamentali della persona coinvolti.

2. Dati misti e consenso nel GDPR

Se è vero che i sistemi di IA si basano su tre architravi: accesso ad informazioni aggregate, correlazione di dati e abilità di calcolo, non sembra un caso se, nel percorso verso la regolamentazione di questa nuova frontiera tecnologica, la strategia europea si sia concentrata sui dati, dapprima con il Regolamento UE n.679/2016 (GDPR) relativo *alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*, nonché alla libera circolazione degli stessi che ha abrogato la direttiva 95/46/CE e,

poco dopo, con quello n.1807/2018/ UE relativo a un *quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea*¹⁰. Entrambi sono mossi da un'unica finalità: favorire la circolazione dei dati sia personali che non in quanto l'Unione europea parte dalla premessa¹¹ che “solo se i dati circolano liberamente l'Europa può sfruttare al meglio le opportunità offerte dalle tecnologie e dal progresso digitali”. I *Big data* debbono circolare senza ostacoli “per il corretto funzionamento del mercato unico digitale, rafforzare la fiducia nel *cloud computing* e cambiare o porre fine ai contratti di *cloud computing* in modo più semplice”¹².

Base di partenza, è il riferimento alla “funzione sociale” (cons. 4 GDPR)¹³, che è assegnata al trattamento anche dei dati personali, intesa come clausola riassuntiva dei valori sia economici che sociali, emergenti nell'ordinamento giuridico, idonea, di per sé, a conformarne il contenuto di tale diritto. Il diritto alla protezione dei dati personali non può, pertanto, considerarsi una “prerogativa assoluta” (cons.4 GDPR), in quanto involge una valutazione superindividuale del trattamento¹⁴. In particolare, è emersa, in questo contesto, la duplice veste assunta dai dati personali: da un verso espressione di un diritto della persona e dall'altro, come detto, beni in molti casi essenziali per la collettività, sia sotto il profilo non patrimoniale, basti pensare a quelli inerenti alla salute, sia sotto quello patrimoniale, in quanto, fondamentali per lo sviluppo dell'economia.

Peraltro, nel mercato dei *Big data*, esiste una commistione tra dati personali e non personali¹⁵, come si verifica per i dati acquisiti per l'esplicitamento di servizi pubblici come quelli sanitari. Se i dati personali sono facilmente individuabili e, quindi definibili, la delimitazione di dato non personale è meno scontata in quanto, all'interno di questa categoria, rientrano molti tipi di dati ed, in particolare: dati che *ab origine* non sono riferiti ad una persona, come ad esempio, quelli relativi alle condizioni

meteorologiche; dati che inizialmente erano personali ma che, poi, sono stati resi anonimi¹⁶.

Nei casi di dati “indissolubilmente legati”, le tutele giuridiche previste nel Regolamento UE n.679/2016 sono applicabili anche agli insiemi di dati misti, dal momento che l’art. 2, par. 2, del Regolamento UE n.2018/1807, lascia impregiudicata l’applicazione del GDPR.

Se la normativa di riferimento è, per lo più, quella del Regolamento UE n.679/2016 bisogna quindi porsi la domanda se il consenso che, in molti casi, legittima il trattamento, possa o meno ancora rivestire un ruolo in ordine ai sistemi AI.

A tal fine, bisogna premettere che nelle varie fasi, che scandiscono il procedimento di apprendimento dei sistemi di intelligenza artificiale, generazione ed acquisizione dei dati, estrazione, correlazione, ed infine, analisi, la veste di protagonista, nella prima, è svolta da quelli che sono stati definiti “agenti informazionali interconnessi”, le persone nell’ambito di attività svolte, sia di tipo *online* che *offline*¹⁷. Diversi i dispositivi che generano dati, nell’ambito dell’IoT, e tra essi un ruolo cruciale assolve lo *smartphone*, che scandisce, ormai, la vita dell’utente.

Ed è, pertanto, fondamentale, in questa fase, che i dati siano legittimamente acquisiti: per quanto concerne i trattamenti automatizzati, nell’ambito dei quali potrebbero essere ricompresi tutti quelli basati sull’AI, il GDPR li sottopone a misure particolarmente restrittive. Tuttavia, anche in questo caso, la prestazione del consenso esplicito, purché, sorretto da adeguata informazione, ex art. 22, par. 2, lett. c), che integra una delle tre eccezioni al divieto di utilizzo di tale misure¹⁸, che possono essere permesse, come è noto, anche in altre due ipotesi: la decisione automatizzata è necessaria per concludere/eseguire un contratto o se è stata autorizzata dal diritto dell’UE o da uno Stato membro.

Nei casi in cui il consenso è richiesto, quindi in presenza di dati personali e dati misti, ai sensi degli artt. 4, 7, 8 del GDPR, occorre un atto con il quale l'interessato manifesta una volontà libera, specifica, informata di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta che si dovrebbe tradurre nella compilazione di un modulo specifico corredato dal caricamento *on line* di un documento d'identità personale¹⁹.

Inoltre, ai sensi dell'art. 7 par.2, “se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta, che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro”. Il legislatore europeo al fine di scongiurare la frequente acquisizione ed utilizzazione surrettizia dei dati ha stabilito altresì che, nel valutare se il consenso è liberamente prestato” ai sensi dell'art. 7 par. 4, fra i parametri da considerare, vi è “l'eventualità che la prestazione di un servizio sia condizionata alla prestazione di un trattamento dei dati non necessario all'esecuzione del contratto”²⁰.

Elemento conformativo del consenso è l'informazione ²¹: il GDPR punta, infatti, molto l'accento sull'adempimento degli obblighi informativi, essenziale per rendere consapevole il titolare dei dati anche dell'utilizzo ultroneo che può essere connesso al trattamento. La previsione di un'informazione che non solo deve essere data “chiaramente” ma, anche, “separatamente da qualsiasi altra”, recepisce quelle istanze, in merito al rafforzamento della tutela degli utenti, sollecitate dalla Commissione europea²², che sospingono verso un adempimento degli obblighi informativi calibrato sul titolare del dato, considerato non in astratto ma in concreto. In questo senso, paradigmatico è quanto statuito dall'art. 12, n. 1, del GDPR, e recepito nell'ordinamento italiano dall'art. 2-*quiquies*, comma 2, del d.lgs.

n.101/2018, a proposito di soggetti deboli, come i minori, per i quali si precisa che l'informazione deve essere resa accessibile, attraverso un linguaggio chiaro e semplice che, come specifica il considerando n. 58, " il minore possa capire facilmente". Altra caratteristica del consenso è la sua revocabilità ai sensi dell'art.7 par.3 da parte dell'interessato, in qualsiasi momento, su cui, preventivamente deve essere edotto. A rafforzare la capacità di autodeterminazione sui dati vi è inoltre il diritto di rettifica, ex art 16 GDPR, in conformità a quanto statuito dal par.2 dell'art. 8 della Carta di Nizza cui si aggiunge l'ulteriore diritto ad opporsi al trattamento se, però, esiste un motivo legittimo, ex art. 21 GDPR. Completa il quadro anche il diritto alla c.d. "portabilità dei dati " introdotto dal GDPR ²³ che semplifica le procedure connesse in favore dell'utente che stipuli un contratto di servizio con un nuovo gestore, esonerandolo dal rifornire tutti i suoi dati al nuovo. La finalità di semplificare l'utilizzo dei propri dati, da parte del legittimo titolare, si coniuga, in tal caso, con l'esigenza di stimolare la concorrenza nel mercato digitale dominato dai giganti della tecnologia²⁴.

3. I limiti del consenso nei sistemi basati sull'intelligenza artificiale

Il consenso, così come disegnato nel Regolamento n.679/2016/UE, applicato all'automazione che connota i sistemi di intelligenza artificiale, mostra, al momento, una certa debolezza²⁵.

In essi, i dati elaborati sono estratti e sottoposti ad un processo di analisi, capace di ricavare informazioni che assolvono una funzione in grado di predire una serie di comportamenti. Si tratta di informazioni di rilevante interesse economico da vendere a soggetti, come società, che le potranno utilizzare per pubblicità mirata o per investire su beni e servizi che, attraverso, l'incrocio dei dati appaiono utili o interessanti per la popolazione.

Nell'ambito degli strumenti di analisi si rinvencono, essenzialmente, algoritmi di “interrogazione” e di “apprendimento”: i primi rispondono a delle domande degli utenti, i secondi, invece, sono in grado di ricavare ulteriori informazioni, sfruttando metodologie come il *machine learning*. Queste, in particolare, recano il rischio di incontrollabilità della decisione algoritmica che si lega, sostanzialmente, al fatto che è proprio l'algoritmo che dà e gestisce gli impulsi, sulla base dei dati forniti da uno o da una comunità di programmatori.

Emerge, pertanto, un'inconciliabilità con i requisiti che costituiscono condizioni di legittimità del consenso, sulla base del GDPR, con particolare riferimento a tre aspetti: libertà di manifestazione del consenso, principio di minimizzazione dei dati e individuazione *ex ante* delle finalità del trattamento²⁶.

In ordine al primo profilo, è opportuno richiamare quanto previsto nel cons. 42 del GDPR ove si afferma che il consenso non dovrebbe essere considerato liberamente prestato se l'interessato non è in grado di operare una scelta autenticamente libera; altrettanto se è nell'impossibilità di rifiutare o revocarlo senza subire pregiudizio. Queste circostanze non sembra che possano essere rispettate con l'uso delle nuove tecnologie. L'analisi delle *policies*, che accompagnano i prodotti integrati con l'AI, sono allo stato predisposte per rendere il funzionamento dei prodotti “ostaggio” del consenso nel senso che l'utilizzo degli stessi, anche nel lungo periodo, è legato al rilascio dello stesso. In tale contesto il consenso rappresenta, così, quasi un atto obbligato più che voluto per usufruire di una serie di beni e servizi erogati che, in alcuni casi attengono, anche ad infrastrutture critiche per la vita dell'uomo, nel settore dell'energia e dei trasporti, della finanza, dei servizi giudiziari, sanitari, universitari, scolastici, solo per fare qualche esempio.

In relazione al secondo aspetto, relativo al c.d. principio di minimizzazione dei dati, in quanto essenziali alle finalità che il

trattamento deve perseguire, è noto che il suo rispetto costituisce un requisito di validità dello stesso trattamento; il parametro richiesto è quello dello “stretto necessario” per usufruire del servizio richiesto. È possibile notare, tuttavia, che i dispositivi con IA, a partire dai dati loro forniti, sono in grado di dedurre molte altre informazioni, che magari l’utente avrebbe scelto di non condividere.

Questa considerazione consente di sviluppare un analogo ragionamento per il terzo aspetto correlato al “principio di finalità”: il GDPR punta l’accento sul fatto che il trattamento dei dati personali deve essere necessario ma, soprattutto, severamente calibrato sugli scopi da perseguire, che devono essere definiti specificatamente e sorretti da un’adeguata informazione, con un argine netto rispetto al passato. L’art. 6 del GDPR si esprime in termini di liceità del trattamento, in una serie di casi, tra cui vi è quello che se l’interessato abbia espresso il consenso per una o più specifiche finalità, in ottemperanza a quanto stabilito alla lett. b), par. 1 dell’art. 5 GDPR, in base al quale “i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità”. Si tratta dell’applicazione di un principio espresso dal par. 2 dell’art 8 della Carta di Nizza²⁷, che comporta, evidentemente che le finalità, per cui i dati sono raccolti e trattati, non possono essere modificate senza chiedere nuovamente il consenso agli interessati, pena l’illegittimità del trattamento. Invece un calcolatore dotato di AI, nel processo di autoapprendimento, che comporta un adattamento all’ambiente circostante e quindi la possibile modifica dei suoi comportamenti, potrebbe cambiare tali finalità in autonomia; si configurerebbe un trattamento non supportato dal consenso essendo non preventivamente predeterminato e predeterminabile e, quindi, illecito. Ne consegue che i *dati*, in genere, possono essere trattati per scopi predeterminati solo in termini generali: le finalità non possono, in realtà, specificatamente essere individuate *ex*

ante, atteso che le correlazioni fra i dati emergono solo nella fase dell'estrazione successiva alla raccolta degli stessi. I dati possono, pertanto, acquisiti con il consenso ma, come visto, da essi possono essere ricavate informazioni ultronee, spesso oggetto di vendita, e di questo non vi è consapevolezza all'atto di prestazione del consenso.

Infatti un problema ulteriore è poi costituito dall'inserimento, in molte *policies* che corredano *smart object*, di una serie di clausole di esonero dalla responsabilità per l'uso che terze parti acquirenti dei dati effettueranno, sulle quali non c'è sufficiente chiarezza.

Peraltro, concentrando l'attenzione sui prodotti dotati di AI, in cui esiste un'interazione tra bene e servizio²⁸, non solo esprimere un consenso realmente consapevole è complesso ma vi è, poi, l'aspetto non trascurabile della sorveglianza realizzata attraverso l'uso dei dati biometrici²⁹ all'interno delle abitazioni, delle autovetture ma, anche, nei luoghi pubblici che è stata accelerata dalla pandemia³⁰. Il GDPR, all'art. 9, par. 1, stabilisce che, in linea generale, è vietato il trattamento di "dati biometrici intesi ad identificare in modo univoco una persona fisica". Tuttavia deroghe sono previste in una serie di casi ben precisi: infatti, al par. 2, è sancito che il trattamento dei dati biometrici è consentito quando, ancora una volta l'interessato ha prestato il proprio consenso esplicito al trattamento dei dati personali, per uno o più specifici utilizzi, come può avvenire nel caso di registrazione preliminare degli oggetti *smart*, di uso domestico. Il problema si amplifica per la sorveglianza di massa che appare profilarsi con l'uso di sistemi AI negli edifici pubblici e nelle strade.

4. Qualche soluzione prospettabile

I limiti dell'applicazione della disciplina del consenso, brevemente prima richiamata, alle nuove tecnologie basate sull'intelligenza artificiale sembrano imputarsi a diversi fattori. Fra questi ad

incidere, sensibilmente, è quella che appare quasi una mutata conformazione giuridica dello stesso e la connessa inadeguatezza a garantire la capacità di autodeterminazione del singolo.

Se il valore in gioco non è più la *privacy* insita nel dato, ma l'informazione che da esso è ricavabile, si comprende come il consenso, attualmente, è piegato a logiche di mercato nell'ambito delle quali gli stessi titolari dei dati, solo in piccolissime percentuali, sono disposti a negarlo se sanno di non potere usufruire di un determinato bene o servizio³¹. Questo nuovo paradigma fa sì che l'atto di manifestazione del consenso all'utilizzo dei propri dati personali e dei metadati sembra assumere carattere sempre più negoziale³² sul presupposto della configurazione del dato come corrispettivo, inquadramento che lo allontana dalla sua qualificazione classica come atto giuridico di natura autorizzatoria³³. D'altra parte anche la giurisprudenza amministrativa³⁴, pur qualificando il dato personale come *res extra commercium*, ha riconosciuto "la patrimonializzazione del dato personale", da parte delle società "attraverso la messa a disposizione del dato e la profilazione dell'utente a fini commerciali". Proprio l'interpretazione, in chiave "sinallagmatica", del consenso sembrerebbe trovare sostegno sempre maggiore con riferimento al trattamento dei dati legato alla loro circolazione, in quanto il riutilizzo e/o, circolazione dei dati per fini di *marketing*, fa emergere l'aspetto del dato come bene³⁵. Parte della dottrina³⁶ ha, opportunamente, osservato come il Regolamento n.679/2016 è fondato su una modalità di trattamento dei dati per certi versi "obsoleta" in quanto essenzialmente basata su una dualità di soggetti: il titolare del dato e il titolare del trattamento a cui il titolare consegna i propri dati, confidando nel rispetto di quel principio di *accountability* che presuppone l'osservanza di una serie di norme e procedure imposte dal legislatore e che, in pratica, dovrebbe garantire il corretto uso dei dati in conformità al consenso per cui il titolare lo ha rilasciato e alla normativa vigente. Ma questa

dimensione duale è superata nel momento in cui i dati sono destinati a circolare ed a generare nuove informazioni come nei meccanismi di funzionamento che presidiano l'AI.

Il GDPR, sostanzialmente si concentra su una dimensione essenzialmente non patrimoniale del dato personale che appare in parte superata. Al contempo, non si può non pretermettere di riconoscere come nello stesso regolamento si manifestano i segni di una progressiva decadenza del consenso³⁷: se *prima facie*, infatti, potrebbe rinvenirsi una continuità tra l'art. 23 del previgente Codice *privacy*, sostanzialmente coincidente con quello dell'art. 11 della l. n.675/1996 che sanciva, genericamente, che il trattamento era ammissibile solo “con il consenso espresso dell'interessato”, nel GDPR il consenso, pur rilevante, perde sempre più centralità. Alla base, quasi, una sfiducia verso la sua concreta efficacia e la consapevolezza della sua inadeguatezza a garantire la capacità di autodeterminazione del singolo in sistemi di trattamento automatizzati dei dati molto complessi e sofisticati.

Per superare le criticità evidenziate una soluzione, tra quelle proposte, potrebbe essere rappresentata dal ricorso al *dynamic consent*, un consenso c.d.granulare (cons. 32 GDPR) sperimentato nel settore medico riguardo le c.d. bio-banche. Si risolve nell'acquisizione, per gradi, della consapevolezza del tipo di trattamento, che dovrà essere praticato partendo, dapprima da un consenso ampio, sulla base di un'informativa generale in ordine alle finalità del trattamento e, successivamente, procedendo ad un consenso specifico riguardo a trattamenti specificatamente individuati e descritti. Inoltre il contenuto dell'informativa potrebbe essere affiancato da una simulazione, anche video o grafica, di quelli che potrebbero essere gli effetti del trattamento. Ma il limite di una simile procedura è che il soggetto interessato, subendo troppe informazioni, sia indotto a rispondere in modo automatico, senza prestare attenzione al contenuto delle spiegazioni fornite e questo problema si amplifica per i minori i quali

hanno l'età minima per esprimere il consenso nell'ambito dei servizi della società dell'informazione.

Al fine di garantire la libertà di autodeterminazione la strada da intraprendere sembra essere quella di ricercare altre soluzioni che prescindano dal consenso: ad esempio per i sistemi di automazione domestica³⁸, che captano indiscriminatamente anche dati dei minori o per i prodotti di consumo, dotati di IA integrata, tra cui anche giocattoli per bambini nel Regno Unito³⁹, l'ICO, il Garante della *privacy*, ha emanato delle linee guida che assoggettano tali prodotti, a *standards* diretti ad ampliare la garanzia di un'adeguata ed efficiente tutela dei dati raccolti. È stato elaborato un "*Codice di design*", per i dispositivi ideati per bambini e che, secondo uno studio, potrebbe diventare un modello generale per tutte le tecnologie di automazione domestica. Secondo questa analisi, sarebbe sufficiente che ogni qualvolta i dati captati da un dispositivo *smart*, includono quelli di minori, questi non vengano venduti a terze parti e le norme relative alla *privacy* non li considerino come dati concessi volontariamente. Ma, a ben vedere, una soluzione ulteriore può essere rinvenuta nella possibilità di imporre alle società produttrici, che trattano dati altamente contestualizzati, come quelli presenti nell'ecosistema domestico, di ricorrere alle certificazioni o ai sigilli e marchi di cui all'art. 42 del GDPR, che attestino il rispetto di determinati *standards*, finalizzati ad assicurare un'adeguata protezione dei dati.

5. Buona fede, trasparenza e governabilità dei meccanismi di funzionamento del trattamento algoritmico

Se intorno al diritto sui dati sembrano, evidentemente, coagularsi più situazioni giuridiche soggettive che attengono alla sfera esistenziale e patrimoniale⁴⁰, è possibile affermare che il modello dei contratti del consumatore, innestato su quello della tutela dei dati, può utilmente essere adattato per ridurre le

asimmetrie esistenti tra piattaforme ed utenti⁴¹. Apparentemente, allora, questo accostamento sembrerebbe riportare in auge il consenso ma, tenuto conto dei limiti evidenziati nelle pagine precedenti, per colmare lo squilibrio giuridico in cui versa l'utente nei sistemi AI, l'autodeterminazione potrebbe essere potenziata legandola più che al consenso ad altri profili quali l'informazione, il riconoscimento del diritto di accesso, il c.d. *ius poenitendi*, ma, soprattutto concentrandosi sulla conformazione normativa del contenuto delle condizioni generali predisposte dai professionisti.

Negli interventi normativi, successivi al GDPR, si assiste ad una spiccata tendenza verso "un' autonomia conformata" delle condizioni generali di contratto, che si sostanzia in una predeterminazione legale del contenuto, che schiude ad una nuova fase: ciò si evince a partire dal *Digital services act* e *Digital market act* fino ad arrivare alla bozza di Regolamento sull'intelligenza artificiale (*Regulation on European Approach for Artificial Intelligence*).

Tra i vari livelli di rischio legati all'uso di sistemi AI⁴², predefiniti dal legislatore, forse un po' rigidamente, se paragonati all'approccio più flessibile dell' *accountability*, che caratterizza il Regolamento n. 679/2016, si punta a specifici obblighi di trasparenza, come emerge, ad esempio, dall'art. 52 sul funzionamento del sistema, non solo nei confronti dell'interessato ma, anche, nei confronti di chi acquista e utilizza tali sistemi all'interno dei propri servizi. Nei sistemi "a rischio limitato" e in quelli a "rischio minimo", come applicazioni quali videogiochi o filtri anti *spam* basati sull'AI, sarà la documentazione tecnica a dovere dimostrare la corrispondenza, ai requisiti del regolamento al fine di renderne trasparente il funzionamento. L'utilizzo di sistemi "ad alto rischio", invece, è scandita da norme imperative che impongono alto livello di robustezza, sicurezza del trattamento, documentazione dettagliata e garanzia della supervisione umana⁴³.

Si registra, in sostanza, una procedimentalizzazione dell'attività sottesa al funzionamento dei sistemi AI, con un'operazione simile a quella verificatasi in materia di tutela del consumatore⁴⁴ ove, però, non fossero previste tutta una serie di eccezioni al trattamento dei dati, in materia, ad esempio di giustizia e sicurezza, che appaiono indebolire la normativa proposta sull'AI. Corollario ulteriore è che lo spazio di tutela per i dati, si apre ad una dimensione più collettiva che individuale e ciò può essere importante ai fini di eventuali contenziosi, anche per superare ed affrontare le difficoltà probatorie ed i rilevanti costi economici di un giudizio⁴⁵.

In conclusione, senza cedere a tentazioni che si pongono in chiave critica sul ruolo delle tecnologie digitali, capaci di rievocare la filosofia di fondo al movimento del c.d. luddismo⁴⁶, occorre individuare altri punti cardinali di riferimento per salvaguardare la libertà di autodeterminazione⁴⁷. Tenendo presente che "il trattamento deve porsi al servizio dell'uomo", così come specificato nel cons. 4 del GDPR⁴⁸ e peraltro, già espresso nella direttiva n.95/46, il primo che sembra venire in rilievo è il principio di buona fede⁴⁹, secondo quanto prescritto nel par.2 dell'art. 8 della Carta dei diritti fondamentali dell'Unione europea. La buona fede già, peraltro, delineata più generalmente in capo al prestatore di servizi *on line*, nel cons.48 della direttiva sul commercio elettronico n.31/2000, deve conformare di sé, nella prospettiva nuova introdotta dal GDPR e che arriva fino alla proposta di Regolamento sull'AI, anche le procedure di acquisizione, trattamento e circolazione dei dati, scongiurando accordi diretti a raccogliere dati per scopi vari, in maniera surrettizia, in violazione delle regole di correttezza che, nel *Digital services act*⁵⁰, sembrano assumere una valenza centrale, come risulta dal capo III, rubricato *Obblighi in materia di dovere di diligenza per un ambiente online trasparente e sicuro*.

Analogamente negli Stati Uniti la FTC ha emanato delle linee guida alle aziende per l'utilizzo dell'intelligenza artificiale

ispirato a “verità ed equità”. Ad essere richiamate alcune disposizioni che li operatori del settore devono obbligatoriamente rispettare: la sez. 5 del *FTC act* che vieta le pratiche commerciali scorrette, nelle quali rientrerebbe il ricorso ad algoritmi sleali, che potrebbero comportare scelte di tipo discriminatorio, il *Fair Credit Reporting Act* (FCRA), legge federale del 1970, intesa a promuovere verifiche corrette per l'utilizzo delle informazioni connesse all'erogazione del credito al consumo e l'*Equal Credit Opportunity Act* (ECOA), emanato nel 1974 come parte del più ampio *Consumer Credit Protection Act* (CCPA),⁵¹ che vieta ai finanziatori di discriminare in base alla razza, religione, origine, sesso o fonte di reddito i consumatori. Recenti approdi giurisprudenziali, in Italia, sembrano indirizzarsi in tal senso imponendo la consegna del c.d. codice sorgente⁵², che può rivelarsi utile chiave di accesso per consentire un'eventuale sindacabilità delle scelte, adottate dagli algoritmi e, conseguente individuazione dell'imputazione della responsabilità, per eventuali errori o gli illeciti ad esse connessi⁵³. La conoscibilità delle scelte, anche se esteriorizzate nella forma matematica, costituisce, evidentemente, fattore chiave di trasparenza, non solo *ex ante* ma, anche *ex post*, in via rimediabile, rispetto alla violazione dei diritti fondamentali, da parte di *agenti software*⁵⁴.

Un altro nodo chiave da sciogliere attiene alla complessità del “governo” della decisione algoritmica : il Consiglio di stato⁵⁵ ha individuato un ulteriore principio del diritto europeo, rilevante in materia, ossia quello di “non esclusività della decisione algoritmica”. Si tratta di un principio di rilievo globale in quanto, ad esempio, utilizzato nella nota decisione *Loomis vs. Wisconsin* che postula, sulla base dell'art 22 del GDPR, che ogni persona, destinataria di una decisione automatizzata, che produca effetti giuridici che la riguardano o che incidano significativamente su questa, ha diritto a che tale decisione non sia basata unicamente su tale processo automatizzato.

Proprio sul controllo di questa eventuale capacità, si svolge la partita più importante che dovrebbe vedere, in un approccio più di *accountability* che di “incasellamento” in categoria di rischio predeterminate *ex lege*, così come invece proposto, l’individuazione di meccanismi per impedire che, la decisione algoritmica divenga imprevedibile ed incontrollabile, non rispondendo più ai comandi dell’uomo.⁵⁶

Utilizzo leale degli algoritmi e governabilità dei loro meccanismi di funzionamento eviterebbero che si prosegua nel sovvertimento, in corso, della scala di valori in cui gli uomini contano non *uti singuli* come persona ma, nell’insieme come utenti⁵⁷, fonte principale di informazioni necessarie per il funzionamento dell’economia digitale.

Note di chiusura

* Il presente saggio, rielaborazione della relazione tenuta nella *Summer school on line, Digital innovation and sustainability - Jean Monnet module digital Citizenship in the European Union*, presso l'Università degli studi L'Orientale di Napoli, l'8 giugno 2021, è stato pubblicato nel n. 2/2022 della rivista *Contratto e impresa*.

¹ BVerfG, 15 dicembre 1983, in *BVerfGE*, 65, 1984, www.Bundesverfassungsgericht.de in cui la Corte delinea l'esistenza di un "Diritto che garantisce la facoltà dei singoli di autodeterminarsi" e "di stabilire se divulgare e utilizzare i propri dati personali" e, quindi, di decidere "quando e entro quali limiti rivelare questioni relative alla propria vita personale": tale diritto è fatto discendere dal principio d'invulnerabilità della dignità umana e dalla libertà di agire. In Germania, peraltro, già nel 1977, era stata emanata la prima legge federale sulla Protezione dei Dati Personali, *Bundesdatenschutzgesetz* e, successivamente, la Corte costituzionale tedesca, con una decisione del 27 febbraio 2008, www.bundesverfassungsgericht.de, in *Riv. trim. dir. pen. eco.*, 3, 2009, con nota di R. FLOR, p. 679 ss., ha affermato l'esistenza di un « diritto alla integrità dei sistemi informativi tecnologici, funzionale allo sviluppo della personalità», come parte del diritto alla riservatezza della persona. In tale ambito un ruolo fondamentale è stato, inoltre, svolto dalla giurisprudenza della Corte di Strasburgo, della Corte di giustizia europea e della Corte suprema americana, per un'analisi delle cui decisioni si rinvia ad O. POLLICINO, *Judicial protection of fundamental rights on the internet. A road towards digital constitutionalism?* Oxford-New York, 2021, p.184 ss.

² G. ALPA (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020; S. LANNI, *Datataquake: intelligenza artificiale e discriminazione del consumatore*, in *Nuovo dir. civ.*, 2, 2020, p. 97ss.; U. SALANITRO, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, in *Riv. dir. civ.*, 6, 2020, p. 1246 ss.; G. GITTI, *Tecnologie digitali, persona e istituzioni*, *ibidem*, 1231ss.; A.M. GAMBINO - M. MANZI, *Intelligenza Artificiale e tutela della concorrenza*, in *Giur.it.*, 7, 2019, p. 1744 ss.; A. AMIDEI, *Intelligenza Artificiale e product liability: sviluppi del diritto dell'Unione Europea*, *ibidem*, p. 1718; E. GABRIELLI - U. RUFFOLO (a cura di), *Intelligenza Artificiale e diritto*, *ibidem*, p. 1657 ss.; U. RUFFOLO (a cura di), *Intelligenza artificiale e responsabilità*, Milano, 2018; F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018.

³ Cass.civ., Sez.I, ord.25 maggio 2021, n. 14381, riguardo la definizione del c.d. *rating reputazionale*.

⁴ Cfr. Cons.St., Sez. VI, 13 dicembre 2019, n.8472; in senso conforme Cons. St., Sez.VI, 8 aprile 2019, n. 2270 che, qualificato il *software* come un "atto amministrativo informatico", sottolinea come la regola tecnica, che governa cia-

scun algoritmo, “resta pur sempre una regola amministrativa generale, costruita dall’uomo e non dalla macchina, per essere poi (solo) applicata da quest’ultima”. Ne consegue che la conoscibilità di una regola, espressa in un linguaggio differente da quello giuridico, deve essere garantita in tutti gli aspetti, “ dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti”, *v.infra* par.5.

⁵ S. CERI, *On the role of statistics in the era of big data: a computer science perspective*, in *Statistics & Probability Letters*, 136, 2018, p.68ss.

⁶ Su cui v.A.AGNELLI, *J.Locke*, in *Noviss. Dig.it.*, IX, Torino, 1963, p.1060; sull’autodeterminazione, in particolare C.CASTRONOVO, *Autodeterminazione e diritto privato*, in *Europa e dir.priv.*, 4, 2010, p.1037ss.; ID., *Eclissi del diritto civile*, Milano, 2015, p.100 che sottolinea come “il luogo costituzionale dell’autodeterminazione” è quello della libertà personale, ex art 13 Cost, come erede moderno dell’*habeas corpus* ed è questa l’idea di fondo al diritto alla salute ed alle scelte complesse che attengono ai trattamenti sanitari ed al fine vita su cui v. P. PERLINGIERI, *Il diritto alla salute, quale diritto della personalità*, in *Rass.dir.civ.*, 4, 1982, p. 126; P.ZATTI, *Il corpo e la nebulosa dell’appartenenza*, in *Nuova giur.civ.comm.*, II, 2007 p.2; L.NIVARRA, *Autonomia (bio)giuridica e diritti della persona*, in *Europa e dir. priv*, 2009, p.719ss.; L. BALESTRA, *L’autodeterminazione nel «fine vita»*, in *Riv. trim.*, 2011, 4, p. 1009 ss.; G.DI ROSA, *La persona oltre il mercato.La destinazione del corpo post-mortem*, in *Europa e dir.priv.*, 4, 2020, p.1179 M. FOGLIA, *Danno non patrimoniale - la lesione del diritto di determinarsi liberamente nella scelta dei propri percorsi esistenziali*, in *Giur. it.* 6, 2020, p.1.348 ss. In giurisprudenza Corte Cost., 23 dicembre 2008, n.438 su cui S.RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, p.265 .

⁷ Sui nuovi beni è d’obbligo il riferimento a C.REICH, *The new property*, in *The Yale Law Journal*, 1964, 73, 5, p.733 ss.; ID., *The “ new property” after 25 years*, in *University San Francisco law review* 24, 1990, 232ss. ; nella dottrina italiana specificatamente sui dati, come beni, P. PERLINGIERI, *L’informazione come bene giuridico*, in *Rass. dir. civ.*, 1990, p. 326 ss.; V. CUFFARO, *Il consenso dell’interessato*, in, (a cura di ID. e V. Ricciuti), *La disciplina del trattamento dei dati personali* Torino, 1997, p. 216; F. MACARIO, *La protezione dei dati personali nel diritto privato europeo*, in *La disciplina del trattamento dei dati personali*, op.ult.cit., p. 12 ss.; S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ.*, II, 2001, p. 641 ss.; V. ZENO ZENCOVICH, *Sull’informazione come “bene” (e sul metodo del dibattito giuridico)* in *Riv. crit. dir. priv.*, 1999, p. 485 ss.;

V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. Informazione e informatica*, 4, 2018, p. 689 ss.; ID., *L'equivoco della privacy*, Napoli, 2022; G. RESTA, V. ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete* in *Riv. trim. dir. e proc. civ.*, 2, 2018, p. 411 ss.; D. POLETTI, *Comprendere il Reg.UE 2016/679: un'introduzione*, in (a cura di) ID. e A. Mantelero, *Regolare la tecnologia: il Reg.UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa, 2018, p. 10; v.infra nt.31 e 39.

⁸ Per un'analisi si rinvia a G. ALPA, *Quale modello normativo europeo per l'intelligenza artificiale?*, in *Contr. e impr.*, 4, 2021, p.1003 ss.

⁹ Sul piano quinquennale, pubblicato nel 2016, in Cina v. report del CNR, *AI per lo sviluppo sostenibile*, p. 154, www.cnr.it. Nella Risoluzione del Parlamento europeo, del 20 gennaio 2021 (2020/2013(INI)), *relativa all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale* si rinviene una definizione di "sistema di intelligenza artificiale (IA)" ossia di "un sistema basato su software o integrato in dispositivi hardware che mostra un comportamento che simula l'intelligenza, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici". Il Parlamento europeo, nell'ottobre 2020 ha inviato alla Commissione UE alcune proposte per l'adozione di tre regolamenti, in ordine agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate. Il 21 aprile 2021 è stata depositata la bozza di regolamento sull'intelligenza artificiale, *Regulation on European Approach for Artificial Intelligence* che si pone sullo sfondo di un intervento di revisione della direttiva sui prodotti difettosi. Cfr., altresì, Risoluzione del 12 febbraio 2019, su una *Politica industriale europea globale in materia di robotica e intelligenza artificiale*, P8_TA-PROV(2019)0081, nonché il *White paper* del 19 Febbraio 2020, che la Commissione UE ha pubblicato per implementare la fiducia in Europa nei sistemi di AI ed il *Report on the safety and liability aspects of AI*; prima ancora, la Risoluzione del 16 febbraio 2017 del Parlamento europeo, che reca "Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica", in www.europa.eu.

¹⁰ In generale v. (a cura di) S. SICA, V. D'ANTONIO e G.M. RICCIO, *La nuova disciplina europea della privacy*, Padova, 2016; G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017; F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2, 2107, p. 369 ss.; A.A. MANTELE-RO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg.UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia Spagna*, cit.; V. CUFFARO, A. D'ORAZIO, V.

RICCIUTO, (a cura di), *I dati personali nel diritto europeo*, Torino, 2018; E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. e impr.*, 1, 2018, p. 106 ss.; N.ZORZI GALGANO (a cura di), *Persona e mercato dei dati .Riflessioni sul GDPR* a cura di Padova, 2019. Sul reg. n.1807/2018/UE, A.DEL PIZZO, *Trattamento dei dati non personali: punti di contatto tra il Regolamento (UE) 2018/1807 e il GDPR.*, in *Dir. di internet*, 2020, www.diritto-diinternet.it

¹¹ Cons.10 reg.n.1807/2018/UE; Cons. 6 reg.n.679/2016/UE.

¹²Così la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Strategia per il mercato unico digitale in Europa*, Bruxelles, 6.5.2015com (2015) 192 final. Sul mercato unico digitale, cfr., per tutti in dottrina G.ALPA, *Il mercato unico digitale*, in *Contr.impr.eur.*, n.1, 2021, www.contrattoeimpresaeuropa.eu. Sui *Big data*, M.DELMASTRO, A.NICITA, *Big data-Come stanno cambiando il nostro mondo*, Bologna, 2019, p.10 ; A.C.DI LANDRO, *Big data. Rischi e tutele nel trattamento dei dati personali*, Napoli, 2020, p.170; cfr., altresì *Indagine conoscitiva volta ad approfondire la conoscenza degli effetti prodotti dal fenomeno dei Big Data e analizzarne le conseguenze in relazione all'attuale contesto economico- politico-sociale*, in www.agcm.it.

¹³ Specificatamente A. RICCI, *Sulla “funzione sociale” del diritto alla protezione dei dati personali*, in *Contr. e impr.*, 2, 2017, p. 586 ss.; ma sul punto, più in generale, S. PUGLIATTI, *La proprietà e le proprietà*, in *La proprietà nel nuovo diritto*, Milano, 1964, p. 278; U. NATOLI, *La proprietà*, Milano, 1980, p. 273ss.; V. SCALISI, *Il nuovo volto della proprietà.Da “potere” a “titolo” di godimento*, in ID. *Categorie e istituti del diritto civile nella transizione al postmoderno*, Milano, 2005, p. 482 ss; U. MATTEI, *Una primavera di movimento per la “ funzione sociale della proprietà”*, in *Riv.crit. dir. priv.*, 2013, p. 531 ss.; A. FEDERICO, *La proprietà in Europa tra “ funzione sociale” e “ interesse generale”*, in G. D'AMICO (a cura di) *Proprietà e diritto europeo*, Napoli, 2013, p. 125 ss.; nella letteratura internazionale R.A. EPSTEIN, *Takings-Private property and the power of eminent domain*, Harvard University Press, 1985, p.166 ss. che indaga il rapporto tra interessi pubblici e privati, sottesi al diritto di proprietà, al fine di dimostrarne la possibile convergenza, nell'ambito della medesima situazione giuridica.

¹⁴Così V. CUFFARO, *Il diritto europeo sulla protezione dei dati personali e la sua applicazione in Italia: spunti per un bilancio*, in *Regolare la tecnologia*, cit. p.30. In proposito v. L. GATT, R. MONTANARI, I.A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in (a cura di) P.Passaglia e D.Poletti, *Nodi virtuali, legai informali: Internet alla ricerca di regole*, Pisa, 2016, p. 57 ss.

¹⁵ Cfr., in tal senso, il punto 4.1.2. della *Comunicazione della Commissione al Parlamento europeo e al Consiglio - Linee guida sul Regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea*, del 25 settembre 2019 - COM (2019) 250 final che, al punto 2.2, fa più volte riferimento alla contiguità tra dati personali e non personali evidenziando come “gli insiemi di dati misti rappresentano la maggior parte degli insiemi di dati” .

¹⁶ L'anonimizzazione ovviamente è differente dalla pseudonimizzazione, come emerge dal reg. n.679/2016/UE. Ai sensi dell'art. 4, par. 1, n. 5 del GDPR, con la pseudononimizzazione i dati trattati non vengono attribuiti a un interessato identificato ma ad uno pseudonimo e, per ricondurre i dati alla persona, sono necessarie delle informazioni aggiuntive da conservarsi separatamente. La pseudonimizzazione, a differenza dell'anonimizzazione è una misura di sicurezza che non esclude la possibilità di reidentificazione dell'interessato. Nel GDPR la pseudonimizzazione, insieme alla cifratura, è considerata tra le misure da utilizzare per proteggere i dati personali trattati.

¹⁷ Così L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Cortina, 2017, p. 106 ss. ; ID., *Pensare l'infosfera. La filosofia come design concettuale*, Milano, 2020.

¹⁸L'art. 22 del GDPR riprende, in gran parte, la formulazione, già contenuta nelle disposizioni precedenti, a partire dall'art. 15 della dir. n.46/95/CE, che vietava che la persona potesse essere sottoposta a decisioni fondate, esclusivamente, su un trattamento automatizzato di dati, che produca “effetti significativi” nei suoi confronti. L'art.13, par. 2, lett. f) del GDPR chiarisce che, per garantire un trattamento corretto e trasparente, il titolare del trattamento, oltre ai contenuti essenziali dell'informativa, deve mettere a conoscenza l'interessato dell'esistenza di un processo decisionale automatizzato, compresa la profilazione, e fornire allo stesso informazioni sulla logica utilizzata nonché sull'importanza e sulle conseguenze previste.

¹⁹ Così *Guidelines 05/2020 on consent under Regulation 2016/679/UE*, emanate dall'*European data protection board*, www.edpb.europa.eu, su cui v.infra nt. successiva.

²⁰ Interessante è quanto si legge nelle *Guidelines 05/2020 on consent under Regulation 2016/679/UE*, cit., sulla pratica del c.d. *cookie walls*, schermata che consente la visione dei contenuti del sito, solo acconsentendo ai *cookies* e alla relativa informativa. L'EDPB sottolinea come sia impossibile ritenere che il consenso sia liberamente prestato, in quanto l'utente non si è trovato di fronte a una scelta consapevole ed analogamente se la fornitura del servizio, da parte del *provider*, è subordinata alla prestazione del consenso nel caso di c.d.

scrolling, avviso che continuare a scorrere il sito costituirà un'espressione di consenso. In proposito v. anche Cass.civ., Sez.I, 2 luglio 2018, n. 17278, in *Riv. dir. media*, 3, 2018, con nota di A. VIGENTINI, www.medialaws.eu secondo cui il condizionamento sussiste quanto più la prestazione offerta dal gestore del sito Internet sia infungibile ed irrinunciabile per l'interessato, e non nei casi di offerta di un generico servizio informativo, trattandosi di informazioni agevolmente acquisibili attraverso vari siti ed anche l'editoria cartacea, con la conseguenza che ben può rinunciarsi a detto servizio senza gravoso sacrificio; Corte giust. UE, 11 Novembre 2020, caso C-61/19, Orange România SA. c. AN-SPDCP, in *Riv. dir. media*, n.1, 2021, con nota di M. C. MENEGHETTI, www.medialaws.eu che ha sancito che "una clausola contrattuale secondo cui l'interessato è stato informato e ha acconsentito alla raccolta dei suoi dati non è idonea a dimostrare la valida manifestazione di volontà dell'interessato se : è stata preselezionata dal titolare; induce in errore l'interessato circa la necessità del consenso per la stipulazione del contratto; la libera scelta di opporsi al trattamento è pregiudicata dall'esigenza per l'interessato di negare attivamente il proprio consenso mediante la compilazione di un modulo".

²¹ Nel Regolamento sui dati personali si ricorre ad una formula analoga a quella contenuta nell'art. 5 c. cons., in cui si prevede che il contenuto dell'informazione, che il professionista ha l'obbligo di fornire al consumatore, deve essere espresso in "modo chiaro e comprensibile" al fine di rafforzare la consapevolezza del consumatore nella scelta". Cfr. S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, cit., p. 627; sulle diverse finalità dell'informazione in questo ambito V. ZENO ZENCOVICH, *Il "consenso informato" e la "autodeterminazione informativa" nella prima decisione del garante*, in *Corr. giur.*, 1997, p. 915 ss.; F. MACARIO, *La protezione dei dati personali nel diritto privato europeo*, Torino, 1997, p. 29; A. BARBA, *Le modalità del trattamento*, in *La disciplina del trattamento dei dati personali*, cit., p. 178 ss.

²² Per la protezione dei dati, in particolare, sul consenso all'attività di *profiling*, cfr. le linee guida del 3 gennaio 2017, individuate nel piano d'azione del "Gruppo di lavoro art. 29", www.europa.eu/dataprotection/it.

²³ Si tratta di un diritto già riconosciuto ai consumatori, basti pensare alla portabilità del numero telefonico; ai sensi dell'art. 20 del GDPR "l'interessato ha il diritto di ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento, senza impedimenti da parte del titolare del trattamento cui li ha forniti". In generale v. P. PACILEO, *Il diritto alla portabilità*, in *La nuova disciplina europea della privacy*, cit., p. 221 ss.

²⁴ A tale riguardo si rileva che la maggior parte di applicazioni e siti web si avvalgono in *outsourcing* dei sistemi di tracciamento messi a punto dai c.d. *Over the top*, Apple, Google e Facebook che, evidentemente, godono di una posizione privilegiata per la disponibilità dei dati acquisiti.

²⁵ Così S.SICA, *La responsabilità civile per il trattamento illecito dei dati personali*, in *Regolare la tecnologia*, cit, p. 162. Sottolinea come il modello culturale, prima ancora che giuridico, sul quale si base il Regolamento è quello dell'autodeterminazione ma, tale logica, benchè mitigata dall'*accountability*, non può essere applicata a grandi masse di dati.

²⁶ In tal senso si rinvia a T.TANI, *L'incidenza dei Big data e del machine learning sui principi alla base del Regolamento Europeo per la tutela dei dati personali (2016/679/UE) e proposte per una nuova normativa in tema di privacy*, in *Società delle tecnologie esponenziali e General Data Protection Regulation: Profili critici nella protezione dei dati*, a cura di S.Bonavita, Milano, 2018, p. 35 ss. Sul principio di minimizzazione dei dati Cass. civ., Sez.I, 19 dicembre, 2019, n.34113.

²⁷ Nell'art. 11 del D.lgs. n.196/2003 già era specificato che i dati devono essere trattati in modo lecito e corretto, per gli scopi specifici, espliciti e legittimi, non eccedenti rispetto alle finalità per le quali sono raccolti. Cfr. E. NAVARRETTA, sub art. 11, in (a cura di) M.C.Bianca e F.D.Busnelli, *La protezione dei dati personali*, *Commentario al D.Lgs. 30 giugno 2003, n. 196*, Padova, 2007, p. 241 ss.

²⁸ A.QUARTA, *La dicotomia bene-servizio alla prova del supporto digitale*, in *Contr. e impr.*, 2019, p.1013 ss.

²⁹ I dati genetici e dati biometrici sono stati, opportunamente, aggiunti dal GDPR al novero dei dati sensibili, anche definito "il nocciolo duro" della riservatezza da G. BUTTARELLI, *Banche dati e tutela della riservatezza*, in *La privacy nella Società dell'informazione*, Milano, 1997, p.375.

³⁰ Sul problema della sorveglianza v.*infra* par.5, nt.56.

³¹ M.FRANZONI, *Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale*, in *Jus civile*, 1, 2021, p.9 ss. che sottolinea come se "l'interesse per lo scambio sembra prevalere sulla privatezza delle singole informazioni, sul piano generale, fatti salvi i limiti derivanti dalla natura stessa dei diritti della persona "allora il diritto alla riservatezza "collegato al trattamento dei dati personali non può essere sempre regolato con la logica del consenso del titolare (proprietario) per l'uso che altri fanno del dato (della cosa) e neppure con la stessa logica applicata all'esercizio del diritto alla salute, nel rapporto medico paziente fondato sul consenso informato".

³² V. RICCIUTO, *Comunicazione e diffusione dei dati personali e trattamento di dati particolari*, in *La disciplina del trattamento dei dati personali*, cit., p. 293 ss., che evidenzia come la circolazione dei dati, realizzata attraverso la cessione, nel rispetto del principio di finalità, conferma l'idea di una negoziabilità dei dati; G. OPPO, *Sul consenso dell'interessato*, in (a cura di) V. Cuffaro, V. Ricciuto e V. Zeno Zencovich, *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 123, non esclude che potrebbero sussistere gli elementi per una qualificazione in chiave contrattuale del consenso.

³³ Riconduce il consenso agli atti di natura autorizzatoria D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, p. 350 ss.; analogamente G.M. RICCIO, *Sub artt. 23-27*, in (a cura di) S.Sica e P.Stanzione, *La nuova disciplina della privacy: commento al D.lgs. 30.6.2003, n. 196*, Bologna, 2005, p.98 ss., secondo cui il consenso al trattamento dei dati personali costituirebbe un'autorizzazione privata che ha la funzione di rimuovere un limite posto dal legislatore, nell'interesse del titolare dei dati; secondo S. PATTI, *sub art. 23*, in *La protezione dei dati personali. Commentario*, cit., p. 541 ss., il consenso al trattamento dei dati personali costituisce un elemento della fattispecie legale, cui la legge attribuisce "l'effetto di far venire meno il carattere dell'antigiuridicità che altrimenti presenterebbe l'attività relativa ai dati personali".

³⁴ Cons. St., Sez.V, 29 marzo 2021 n. 2631, conferma così la decisione del Tar Lazio, Roma, Sez. I, 10 gennaio 2020, n. 260 affermando che "Il fenomeno della "patrimonializzazione" del dato personale, tipico delle nuove economie dei mercati digitali, impone agli operatori di rispettare, nelle relative transazioni commerciali, quegli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore, che deve essere reso edotto dello scambio di prestazioni che è sotteso alla adesione ad un contratto per la fruizione di un servizio, quale è quello di utilizzo di un social network". Peraltro, la configurazione del dato, come "prezzo", troverebbe riconoscimento in alcuni interventi normativi del legislatore europeo: il riferimento è alla dir. n. 2019/770/UE del Parlamento europeo e del Consiglio del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali nella parte trasfusa nell'art.135 octies, par.2, let.g, del Codice del consumo. In dottrina si rinvia alle puntuali osservazioni di V.RICCIUTO, L'equivoco della privacy , in particolare p.174ss.

³⁵ Considerando il dato come un bene economico da potere scambiare all'interno del mercato, sottolinea che l'approccio americano è più facilmente adattabile alle mutazioni tecnologiche, non a caso negli Stati Uniti la raccolta può essere anche indiscriminata M.BRKAN, *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and be-*

yond”, *International Journal of Law and Information Technology*, 27(2), 2019, p.91ss.; v.nt. 7.

³⁶ Così F. PIZZETTI, *GDPR e Intelligenza artificiale, Codici di condotta, certificazioni, sigilli, marchi e altri poteri di soft law previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire l'applicazione proattiva del Regolamento europeo nell'epoca della IA*, in *Regolare la tecnologia*, cit., p. 216; A.R. POPOLI, *Codici di condotta e certificazioni*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., p. 408ss.

³⁷ V.CUFFARO, *Il regolamento generale sulla protezione dei dati*, in *Trattamento dei dati personali e regolamento UE n. 2016/679*, in *Speciali digitali del Corriere giur.*, 2018, p. 2 ss. sottolinea il diverso ambito prospettico del codice della *privacy* dove, all'art. 1, l'accento sembra porsi sul diritto dominicale della persona sui propri dati, così da accreditare un modello di disciplina sostanzialmente prossimo a quello tradizionalmente adottato per i diritti della personalità, appunto delineati in termini di appartenenza esclusiva del bene al soggetto, e l'art. 1, comma 1 del reg. dove “il punto di incidenza della disciplina è spostato direttamente sulla tutela della persona, nella misura in cui il trattamento dei dati possa determinare pregiudizio ai diritti ed alle libertà fondamentali”; F.DI CIOMMO, *Archivi digitali (onnivori) e diritti fondamentali (recessivi)*, in *Nuovo dir. civ.*, 2, 2020, p.29ss.

³⁸ Sul tema v. l'ampia ricostruzione di L.VIZZONI, *Domotica e diritto, La smart home tra regole e responsabilità*, Milano, 2021, p. 35ss.

³⁹ È la tesi di “*Home life data and children's privacy*”, www.childdatacitizen.com, uno studio realizzato, nel 2018, da V. BARASSI, *Digital citizens? Data traces and family life*, in *Journal of the Academy of Social Sciences*, 2017, p. 84 ss..

⁴⁰ Sulla prospettiva “dualistica”, che distingue all'interno del medesimo diritto della personalità un contenuto indisponibile, strettamente personale, e uno di carattere patrimoniale, suscettibile di disposizione, C. SCOGNAMIGLIO, *Il diritto all'utilizzazione economica del nome e dell'immagine delle persone celebri*, in *Dir.inf.*, 1988, p. 26 ss. Nel senso che la distinzione tra momento personale e patrimoniale, di origine francofona, sia “artificiosa” protendendo per una considerazione monistica dei diritti della persona, sulla base di una soluzione ricavabile dal diritto d'autore A. ZOPPINI, *Le nuove proprietà nella trasmissione ereditaria della ricchezza (note a margine della teoria dei beni)*, in *Riv. dir. civ.*, I, 2000, p. 236 ss. Dal diritto della persona si realizzerebbe, nella forma del contratto di licenza, un acquisto “derivativo costitutivo”, che crea una “situazione giuridica soggettiva nuova che limita senza estinguerlo il diritto in capo al titolare”. Il risultato pratico delle due soluzioni non appare, tuttavia, così differente.

⁴¹ In dottrina sottolineano come il mercato non sia in grado di correggere, tali asimmetrie S.BONAVITA-R. PARDOLESI, *GDPR e diritto alla cancellazione e (oblio)*, in *Danno e resp.*, 3, 2018, p.274, per cui “assumere che il consenso possa essere liberamente revocato è una consolazione alquanto grama”.

⁴² Si distinguono rischio inaccettabile, che attiene a quelle applicazioni che potrebbero avere il fine di manipolare i comportamenti umani, come il c.d. *social scoring*; rischio alto, riguardo i sistemi di IA che potrebbero mettere a rischio la sicurezza ed i diritti fondamentali degli individui, come dispositivi medici basati su sistemi di IoT; rischio limitato, ad esempio, *chatbot*, che devono essere trasparenti per fare acquisire all’utente la consapevolezza di interagire con una IA; rischio minimo, ad esempio, filtri spam o *videogame* basati su sistemi di IA per i quali non sono previste particolari limitazioni.

⁴³ All’art. 13 si prevede che i sistemi di IA ad alto rischio “devono essere progettati e sviluppati in modo da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare l’output del sistema e utilizzarlo in modo appropriato”. Ne deriva l’obbligo di svolgere una Valutazione d’Impatto sulla protezione dei dati, così come previsto dall’art. 35 GDPR. L’art. 62 impone ai fornitori dei sistemi di IA, ad alto rischio, di notificare alle Autorità competenti nazionali ogni incidente o malfunzionamento grave, analogamente a quanto previsto nel GDPR per l’obbligo di notifica del *data breach*.

⁴⁴ Per una ricostruzione storica sui contratti di massa cfr., per tutti, C.M. BIANCA, *Le condizioni generali di contratto*, Milano, 1979; G. ALPA, (a cura di), *I contratti del consumatore*, Milano, 2014.

⁴⁵ Sottolinea, d’altra parte come “non è possibile pensare ad una gestione di tipo individuale dei dati, tanto meno se basata sul consenso. Il consenso, astrattamente il miglior modello possibile, si rivela spesso non adeguato nel fornire una tutela effettiva ed inefficace”, G. FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati personali*, in *Giur.it.* 2019, p.1677; in senso analogo D. POLETTI, *GDPR tra novità e discontinuità-Le condizioni di liceità del trattamento dei dati personali*, in *Giur.it.*, 2019, p.2785; in giurisprudenza v. Cons.St., Sez. VI, n.8472/2019 che ha posto l’onere probatorio a carico del soggetto che si avvale della procedura robotizzata tenuto a dimostrare “la necessaria verifica di logicità e legittimità della scelta e degli esiti affidati all’algoritmo”, in quanto l’impossibilità di capire come sia stata presa una determinata decisione, costituisce di per sé “un vizio tale da inficiare la procedura”.

⁴⁶ Ad aprire il dibattito si segnalano le opere di N.G.CARR a partire da *It doesn’t matter*, in *Harvard business review*, 2003, www.hbr.org e di J LANIER *Dieci ragioni per cancellare subito i tuoi account social*, trad. F.Mastruzzo, Milano, 2018.

⁴⁷ Ritieni che “il fatto di riscontrare la insufficienza del consenso a regolare il trattamento nelle sue diverse forme, con conseguente perdita di protezione della persona “ non deve essere inteso nel senso di una resa alla tecnica. Occorre muovere dalla constatazione che l’economia dei beni immateriali o dematerializzati, si muove e segue logiche differenti da quelle dell’economia reale.” Sicché il mondo digitale è “un universo parallelo, che funziona con regole che necessariamente devono essere proprie e non riflesse da quelle del mondo reale che, peraltro, non può essere sostituito”, M.FRANZONI, *Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale*, cit., p.12.

⁴⁸ In tal senso G. ALPA, *L’identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr.e impr.*, 2017, p. 726 ss.

⁴⁹ Principio già previsto dall’art. 12 della *Dichiarazione dei diritti di internet (Diritti e garanzie delle persone sulle piattaforme)*, elaborata dalla Commissione parlamentare per i diritti e doveri in Internet, costituita presso la Camera dei deputati e presieduta da Stefano Rodotà su cui cfr. ID., *Il diritto di avere diritti*, cit., p. 386.

⁵⁰ Regolamento UE 2022/2065.

⁵¹ *Federal trade commission, report Aiming for truth, fairness, and equity in your company’s use of AI*, su cui E. JILLSON, *Aiming for truth, fairness, and equity in your company’s use of AI*, 19 aprile 2021, www.ftc.gov.

⁵² In tal senso, in giurisprudenza, TAR Roma, Sez. III-bis, 30 giugno 2020, n. 7370, che ha ordinato la consegna del codice sorgente del software gestito dal consorzio Cineca, contenente gli identificativi alfanumerici per l’associazione dei compiti anonimi con i nomi e i cognomi dei candidati. In ordine alla possibile introduzione di un registro relativo al deposito del codice sorgente del software di intelligenza artificiale, che dovrebbe garantire maggiore trasparenza, F. BRAVO, *Software di intelligenza artificiale ed istituzione del registro per il deposito del codice sorgente*, in *Contr. e impr.*, 4, 2020, p. 1412 ss. Oltre all’istituzione di un’Autorità regolatoria indipendente tanto a livello nazionale che europeo, seguendo l’approccio già adottato dal GDPR, nel regolamento proposto sull’AI sono previste delle sanzioni amministrative in caso di violazione o mancata osservanza delle norme in esso contenute che possono arrivare fino al 6% del fatturato globale annuo cifra ancor più elevata del 4% prevista dal GDPR.

⁵³ Prospettano, la necessità di una rimodulazione delle norme, che tenga conto delle peculiarità della nuova generazioni di prodotti e che, possibilmente, consenta di individuare un percorso di responsabilità unitario, allo scopo di semplificare e, quindi, agevolare il fruitore del bene nel caso in cui il “formatore” dell’algoritmo sia diverso dal produttore del bene che incorpora A.

AMIDEI, *Intelligenza Artificiale e product liability: sviluppi del diritto dell'Unione Europea*, in *Giur. it.*, 2019, p.1726; U. RUFFOLO, *Intelligenza Artificiale, machine learning e responsabilità da algoritmo*, ibidem, p. 1692 ss.; in proposito v.nt.47.

⁵⁴ E. PALMERINI, *Robotica*, in *Enc. di Bioetica e scienza giuridica, Parte giuridica*, X, Napoli, 2016, p. 1100; E. PALMERINI, A. BERTOLINI, *Liability and Risk Management in Robotix*, in (a cura di)R. Schulre e D.Standenmayer, *Digital Revolution; Challengers for Contract Law in Practice* Baden-Baden, 2016, p. 225 ss.

⁵⁵ Cons. St., Sez.VI, n. 2270/2019, cit., v.nt.4 .

⁵⁶ Nella Risoluzione del Parlamento europeo del 20 gennaio 2021 (2020/2013(INI)), relativa *all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale*, si definisce sistema AI – “autonomo” quello “basato sull'intelligenza artificiale che opera interpretando determinati dati forniti e utilizzando una serie di istruzioni predeterminate, senza essere limitato a tali istruzioni, nonostante il comportamento del sistema sia legato e volto al conseguimento dell'obiettivo impartito e ad altre scelte operate dallo sviluppatore in sede di progettazione”. Suggestive le pagine di A.TURING, *iComputing machinery and intelligence*, in *Mind*, 1950, p.456 che proponeva ai progettisti un metodo di insegnamento, rivolto alle macchine, come se si dovessero educare dei bambini, attraverso quelli che egli definiva degli “imperativi”, cui la macchina è obbligata ad obbedire. In ordine ad una possibile imprevedibilità dell'azione dell'agente *software* la risposta al problema era esemplificata associando « punizioni e ricompense» nel corso del processo d'insegnamento delle macchine, come avviene per i bambini: “La macchina deve essere costruita in modo che sia impossibile che si ripetano gli avvenimenti che precedettero di poco il verificarsi di un segnale di punizione, mentre un segnale di ricompensa aumenta la probabilità di ripetizione degli avvenimenti che hanno condotto ad esso”.

⁵⁷ Nelle linee guida “per un'intelligenza artificiale affidabile”, pubblicate il 18 dicembre 2018, *l'High level expert group on AI*, al punto 5.1 del *Draft* ha, espressamente, chiarito come i diritti fondamentali rappresentino una *stepping stone*, pietra miliare verso un approccio *human centric*, www.europa.eu. In chiave, per certi versi, distopica, S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power*, London 2019. Si rinvia, inoltre, all'analisi di G. ALPA, *Code is law: il bilanciamento dei valori e il ruolo del diritto*, in *Contr. impr.*, n.2, 2021, p.384 che richiama il libro D.LYON, *La cultura della sorveglianza. Come la società del controllo ci ha reso tutti controllori*, Roma 2020, ove si sottolinea che dall'accettazione della logica della sorveglianza ne traiamo tutti beneficio.

Piattaforme tecnologiche: protezione ed educazione dell'utente all'utilizzo delle infrastrutture informatiche nei mercati a concorrenza imperfetta

ANTONELLA CORRENTI

Sommario: 1. Premessa. - 2. La profilazione dei dati personali: il consenso dell'utente al trattamento è rimedio efficace o superato? - 3. I minori: una particolare categoria di utenti. - 3.1. La tutela dei minori nel contesto dei giochi elettronici e online. - 4. Conclusioni.

1. Premessa

Il progresso tecnologico e la proliferazione di strumenti di comunicazione multimediale hanno reso i motori di ricerca e i social network strumenti privilegiati per accedere all'informazione e al marketing. Gran parte delle attività quotidiane, anche a causa dell'emergenza sanitaria che da due anni ha stravolto l'esistenza della collettività, viene ormai espletata attraverso le piattaforme digitali. A favorire il radicarsi delle infrastrutture di rete ha contribuito il processo di informatizzazione della società, che ha segnato il passaggio dal dominio dell'uomo alla sovranità della tecnica.

Inizialmente l'intelligenza artificiale aveva un raggio di azione limitato ai laboratori di ricerca; oggi, ha invaso tutti i campi del sapere con innegabili benefici e innovazioni, ma con altrettanti rischi legati a posti di lavoro o a interi settori soppiantati dalle macchine. L'uso generalizzato di protocolli digitali ha edificato un'architettura globale senza precedenti e generato un nuovo ordine economico che sfrutta il proprio potere per sfidare la democrazia ed erodere la libertà individuale¹.

Ci troviamo di fronte a un fenomeno che, per contenuti e potenzialità applicative, non risulta di facile comprensione e regolamentazione: occorre reperire le misure più adeguate per ridimensionarne l'impatto e ridurne la portata offensiva nei confronti di tutti i soggetti deboli (imprese, utenti, consumatori), impreparati e disattenti nell'utilizzo della rete.

Viviamo in una fase definita dagli studiosi di terza modernità, governata dai grandi imperi della rete, che sfruttano i dati forniti, consapevolmente o inconsapevolmente, dagli utenti per incentivare proposte commerciali personalizzate.

Il successo della ragione artificiale scaturisce paradossalmente dal suo essere modellata sul cervello umano *considerato una forma organizzativa e sistemica perfetta di elaborazione dell'informazione e di apprensione del reale*².

Attraverso l'*espropriazione* dei dati³ i monopolisti on line si impadroniscono di tutte le notizie utili per prevedere e anticipare, non solo le scelte degli utenti, ma anche le strategie dei concorrenti.

I servizi offerti, tramite l'accesso a internet, a dispetto della presunta gratuità degli stessi hanno un prezzo, rappresentato dalla gestione delle informazioni personali che i consumatori versano alle aziende informatiche. In quest'ottica i dati forniti acquistano una duplice connotazione "come bene della vita" e "come valore economico" da contemperare in funzione dell'equilibrio da perseguire tra persona e mercato⁴.

Il potenziale di pericolosità di internet, sia per l'ambito di riferimento che per la forza di attrazione, richiede restrizioni più intense rispetto a quelle previste per i tradizionali strumenti di comunicazione.

Gli organi istituzionali di diversi Paesi indagano sulla capacità dei sistemi normativi vigenti di fronteggiare le sfide offerte da una società dell'informazione e della comunicazione digitalizzate, adoperandosi per rendere effettiva la tutela della riser-

vatezza dei consumatori, della trasparenza delle transazioni commerciali e della regolare competizione dei mercati.

La necessità di educare gli utenti all'uso degli strumenti multimediali rappresenta il punto di approdo di una lunga evoluzione che, nel tempo, ha messo in luce priorità e prospettive di intervento. Se l'assetto concorrenziale pende a favore delle società più abili nella raccolta e nel trattamento dei dati, per evitare la chiusura dei mercati e stimolare la partecipazione anche degli operatori di piccole dimensioni occorre affidare l'ultima parola ai consumatori (utenti), al fine di garantire una *competition on the merits*⁵, secondo cui sono le scelte "sovrane" degli stessi consumatori a premiare o punire le strategie commerciali delle imprese.

2. La profilazione dei dati personali: il consenso dell'utente al trattamento è rimedio efficace o superato?

Attesa la natura corrispettiva delle informazioni trasmesse dagli operatori *on line* durante la navigazione, occorre stabilire se la manifestazione del consenso e l'accettazione delle condizioni generali di utilizzo, in sede di registrazione per l'accesso ad una piattaforma digitale, siano sufficienti a evitare uno sfruttamento non autorizzato dei dati trasmessi⁶.

A generare perplessità, circa l'idoneità dello strumento del consenso, centrale nel Regolamento n. 2016/679/UE (GDPR)⁷, a scongiurare i rischi connessi a un illecito o abusivo utilizzo delle informazioni rilasciate sul web, vi è la tendenza dei colossi tecnologici (*Big tech*) ad operare trasversalmente, in altri mercati, con conseguente trasferimento dei dati degli utenti da una piattaforma all'altra. Più si accresce il numero degli utenti, più aumenta il valore della piattaforma, rendendo gli utilizzatori della rete sempre meno attenti e interessati alle misure di protezione della privacy⁸.

L'interrogativo che si pone la dottrina riguarda la natura della manifestazione del consenso: se integri un vero e proprio tra-

sferimento della titolarità sul dato personale o una sorta di delega all'utilizzo del dato medesimo⁹.

La tesi della trasmissione di un diritto di proprietà sui dati sembrerebbe avallata dalla previsione di cui all'art. 20 del reg. n. 2016/679/UE (GDPR), sul diritto alla portabilità dei dati¹⁰.

La disposizione richiamata, pur favorendo il controllo del soggetto interessato sui propri dati, non elimina l'inconveniente del trasferimento non autorizzato nelle ipotesi di uso secondario degli stessi¹¹. La problematica della traslazione delle informazioni personali da una infrastruttura a un'altra, all'insaputa dei soggetti interessati, è strettamente correlata alla capacità delle imprese dominanti on line di agire su più versanti nella duplice veste di titolare dell'asset e di imprenditore. Nella Relazione sulla Politica di Concorrenza – Relazione Annuale 2019 (2019/2131(INI)) il Parlamento Europeo, in merito all'adattamento delle regole concorrenziali all'era digitale, ha rilevato che *“alcuni soggetti, beneficiando del doppio status di piattaforma e fornitore, abusano della loro posizione per imporre condizioni sleali ai concorrenti”* e ha invitato la Commissione ad esaminare la questione della cosiddetta *auto-preferenza* e della possibilità di imporre *obblighi di regolamentazione ex ante*, nel caso in cui il diritto concorrenziale non sia in grado di assicurare la *contendibilità in tali mercati* (punto 30).

Se, quando ancora l'economia digitale muoveva i suoi primi passi, poteva apparire giustificato un approccio sganciato dalla considerazione dei dati come attributi della personalità¹², ragionevolmente dettato dall'esigenza di contemperare i diritti dell'individuo con le esigenze di mercato, nel momento attuale occorre rafforzare le garanzie e offrire al consumatore una percezione più chiara del valore dei propri dati personali.

Un corretto inquadramento della fattispecie richiede la considerazione di un concetto di privacy in senso lato¹³, onnicomprensivo di tutti gli aspetti evocativi dell'identità personale, dai più risalenti (diritto alla riservatezza, al nome, all'immagine), ai

più recenti (diritto all'oblio)¹⁴, diretto a far recuperare agli utenti maggiore consapevolezza dell'importanza delle informazioni cedute¹⁵.

La sfida più difficile è la monetizzazione dei dati personali, che costituiscono *un bene giuridico, oggetto di un diritto di libertà che, come tale, non può essere alienato, prima che una risorsa economica*¹⁶.

Una risposta concreta al radicarsi della sovranità dei giganti degli algoritmi richiede un mutamento di prospettiva rispetto a quella finora adottata: è necessario non solo reprimere le ipotesi di trattamento non autorizzato dei dati, ma anche avviare un percorso di educazione digitale dell'utenza. L'elaborazione di un apparato normativo a tutela dei diritti e delle libertà individuali non è sufficiente e va accompagnata dall'adozione di misure destinate a rendere il cittadino maggiormente diligente nell'uso degli strumenti informatici. Ad essere intercettate non sono, esclusivamente, le informazioni trasmesse volontariamente dagli utenti, ma anche i dati inconsapevolmente disseminati o tracciati offline¹⁷. Il contesto digitale, con il diffondersi di tecniche sempre più evolute di captazione e registrazione dei comportamenti umani, diviene uno spazio sempre meno sicuro e difficile da regolamentare.

Gli utilizzatori della rete assumono un atteggiamento superficiale e poco attento alle insidie celate dalla stessa in quanto, spesso, ignorano le conseguenze derivanti dalla cessione delle informazioni personali, accettando condizioni di un servizio, apparentemente gratuito, in cambio di frammenti della propria libertà personale.

L'autorizzazione al trattamento dei dati, in questo variegato scenario, non risulta funzionale alla salvaguardia di un bene inalienabile, la protezione del dato, ma diviene essa stessa finalizzata allo *sfruttamento economico del dato medesimo*¹⁸.

Si crea una sorta di asimmetria c.d. digitale¹⁹ che vede le piattaforme, soggetti forti, contrapposte agli utenti, soggetti deboli, che si avvalgono delle stesse senza comprenderne le modalità di funzionamento²⁰.

La celerità con cui si evolvono i mercati digitali richiede interventi normativi adeguati, improntati non soltanto a una tutela *ex post*, ma a una regolamentazione *ex ante*, volta a promuovere una cultura dell'utilizzo degli strumenti telematici.

In ambito europeo in più occasioni si è messa in evidenza la necessità di procedere a un bilanciamento tra la finalità di creazione di un mercato digitale unico e la tutela del trattamento dei dati personali e della libera circolazione degli stessi²¹.

Significative in tal senso sono le proposte della Commissione europea che hanno portato all'emanazione del reg. n. 2022/2065/UE (Digital Service Act) del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali che modifica la dir. n. 2000/31/CE²² e il reg. n. 2022/1925/UE (Digital Market Act) del 14 settembre 2022, sui mercati equi e contendibili nel settore digitale²³.

Il *Digital service act* si propone la realizzazione di un ambiente digitale sicuro, che favorisca sviluppo, innovazione e leale competizione non solo in Europa, ma a livello mondiale. Gli obiettivi richiamati richiedono l'introduzione di norme specifiche che, attraverso un meccanismo di notifica e azione (art.14), impediscano la circolazione in rete di contenuti illegali e circoscrivano la sfera d'azione delle piattaforme di maggiori dimensioni (sezioni 3 e 4). Meccanismi di questo tipo, affiancati da strumenti di vigilanza effettivi ed efficaci, dovrebbero consentire una tempestiva rimozione delle pubblicazioni illegali. L'intervento normativo, con riferimento alla protezione dei minori, non prevede strumenti di verifica dell'età, ma intende rafforzare il ruolo degli utenti nell'ambiente online garantendo l'esercizio di diritti fondamentali quali la protezione dei dati e della vita privata in rete.

Fatte salve le norme contenute nella dir. n. 2000/31/CE sul commercio elettronico e le disposizioni in materia di protezione dei dati personali e della riservatezza delle comunicazioni (GDPR), il legislatore europeo sente di dover intervenire con una disciplina uniforme, in grado di fronteggiare i rischi connessi all'emersione

di sempre più invasivi servizi digitali²⁴. L'incapacità degli addetti ai lavori di arginare un fenomeno in rapida diffusione ha messo in evidenza la necessità di una regolamentazione omogenea per colmare le lacune prodotte da un apparato normativo frammentato.

Un ruolo complementare al *Digital Services Act* riveste il *Digital Markets Act*, che mira all'introduzione di rigide regole di comportamento per gli operatori digitali che agiscono come "gatekeeper", individuati in base alle dimensioni dell'azienda, ai poteri esercitati e alla posizione ricoperta sul mercato. Le imprese, rientranti nell'ambito di applicazione del *Digital Markets Act*, dovranno rispettare le prescrizioni ivi contenute, al fine di prevenire pratiche sleali o che limitino la contendibilità, pena l'irrogazione di sanzioni, quali ammende e penalità di mora.

Le proposte, condividendo punti di partenza e prospettive di intervento, avrebbero dovuto trovare consacrazione in un unico testo normativo. Purtroppo, non è sufficiente l'introduzione di una regolamentazione *ad hoc*, se non associata a un'attività di monitoraggio costante e a un adeguato sistema di *enforcement*.

L'affermazione e il consolidamento dell'economia digitale hanno favorito la cristallizzazione di un modello d'impresa incentrato sulle infrastrutture informatiche, in cui gli utenti che se ne servono, sia nell'esercizio dell'attività professionale che per ragioni di consumo, risultano parti deboli rispetto alle imprese titolari degli asset digitali. In un contesto così congegnato, le piattaforme sfruttano la propria superiorità tecnologica, informativa e negoziale, creando una fitta rete di relazioni che possono coinvolgere tre differenti figure: il fornitore del servizio, l'utente commerciale e il consumatore finale²⁵.

Con l'emanazione del reg. n. 2019/1150/UE, che promuove equità e trasparenza nell'ambito dei servizi di intermediazione online per gli utenti commerciali e i titolari di siti web aziendali che siano in relazione con motori di ricerca online, si coglie un

segnale della preoccupazione del legislatore europeo per le insidie celate dalla rete ai nuovi attori sulla scena economica digitale.

Nella stessa direzione si muove la proposta di Regolamento relativa al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche²⁶, che abrogherà la direttiva 2002/58/CE, non più adeguata di fronte ai cambiamenti segnati dagli sviluppi tecnologici ed economici, e integrerà le disposizioni del GDPR, salvaguardando la riservatezza anche delle persone giuridiche. La proposta intende offrire una tutela specifica agli operatori che si avvalgono degli strumenti informatici, garantendo un'applicazione uniforme delle disposizioni in tutta l'Unione nell'ottica di realizzare un mercato unico digitale. Tra le novità si registra l'attrazione, nell'ambito di riferimento della normativa medesima, della regolamentazione delle cosiddette *over the top*, grandi aziende internazionali che finora erano rimaste estranee alla sfera di operatività degli interventi europei.

In questo articolato scenario l'interrogativo che deve porsi il giurista riguarda l'attualità del consenso alla raccolta e al trattamento dei dati come misura di salvaguardia dei clienti, controparti deboli dei giganti industriali. La risposta al quesito si rinviene nelle normative più recenti menzionate, in cui il consenso sembra dismettere la tradizionale centralità, lasciando il posto a interventi rivolti a un ampliamento degli obblighi di trasparenza nelle condizioni contrattuali e a un adeguamento delle misure di protezione della riservatezza degli utenti alle differenti tipologie di comunicazione elettronica adoperate.

3. I minori: una particolare categoria di utenti

Nel contesto della presente indagine suscita particolare interesse l'influenza che le nuove tecnologie esercitano sui comportamenti e sulle abitudini dei minori. Il dilagare di internet tra i giovanissimi rende l'obiettivo della protezione della privacy e

della sicurezza di tale categoria di utenti prioritario nell'ambito della gestione delle criticità sollevate dall'uso del digitale. L'esigenza di intervenire con misure più stringenti è strettamente correlata alla peculiare condizione dei soggetti coinvolti che, pur se definiti nativi digitali, hanno scarsa consapevolezza dei pericoli legati all'uso delle infrastrutture informatiche²⁷.

Le aziende erogatrici dei servizi di rete realizzano veri e propri modelli di business basati sulla raccolta e sulla condivisione di dati personali, che vengono trasmessi non soltanto per usufruire di motori di ricerca o social network, ma anche nell'ambito delle piattaforme di gioco, utilizzate su dispositivi mobili e console per videogiochi che, includendo l'impiego di microfoni e altri hardware speciali, sfruttano talvolta i dati biometrici dei giocatori.

Il quadro giuridico europeo in materia appare scarno. Un esplicito riferimento ai minori si rinviene nel *considerando* n. 38 del reg. n. 2016/679/UE (GDPR), secondo cui *“i minori meritano una specifica protezione relativamente ai propri dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali”*.

Lo stesso regolamento, al paragrafo 1 dell'art. 8, nel disciplinare l'offerta diretta dei servizi della società dell'informazione, ha sancito la liceità del trattamento dei dati personali del minore ove lo stesso abbia compiuto il sedicesimo anno di età; in caso contrario è necessaria la manifestazione del consenso o l'autorizzazione da parte *del titolare della responsabilità genitoriale*.

Il legislatore ha voluto colmare le lacune contenute nella disciplina precedente (dir. n. 95/46/CE) che non distingueva il trattamento dei dati del minore da quello dei soggetti adulti. Nel nostro ordinamento una tappa importante, nell'iter di recepimento delle norme europee, è rappresentata dal D.lgs. n. 101 del 2018 che ha adeguato il Codice in materia di protezione dei dati personali (D. lgs. 30 giugno 2003, n.196) alle disposizioni del reg. n.2016/679/UE.

In armonia al dettato normativo del citato art. 8 paragrafo 1, che fa salva la possibilità degli Stati membri di stabilire un'età diversa, purchè non inferiore a 13 anni per il consenso, il comma 1 dell'art 2-*quinqies* del novellato Codice sulla privacy prevede il compimento del quattordicesimo anno per l'autorizzazione al trattamento dei dati. La soluzione normativa trova riscontro nei sistemi di Common law ed in particolare negli Stati Uniti, in cui il *Children's Online Privacy Protection Act* (COPPA)²⁸ fissa l'età di 13 anni (§ 312, 2) come parametro al di sotto del quale non è possibile prestare un valido consenso per il trattamento dei dati, prescrivendo il *verifiable consent* dei genitori per i servizi rivolti ai minori che richiedono la raccolta dei dati medesimi. Nel Regno unito il 2 settembre 2021 è entrato in vigore l'*Age Appropriation Design Code* (anche detto "*Children's Code*"), una normativa rivolta a salvaguardare i minori di 18 anni nell'ambito dei servizi offerti per via elettronica dai prestatori della società dell'informazione, che includono non solo app, ma anche social e giochi informativi. L'obiettivo alla base della disciplina citata è la garanzia dell'interesse superiore del bambino tramite l'offerta di informazioni semplici e chiare, la minimizzazione dei dati, la limitata condivisione degli stessi e il divieto di servizi di localizzazione.

Il *Children's Code* si ispira ai principi contenuti nel COPPA e nel GDPR, ma mette in luce la necessità di predisporre informative e contenuti a prescindere dalla specifica fascia d'età a cui è rivolto il servizio.

Se il concetto di privacy, in ambito digitale, assume i caratteri di una vera e propria risorsa economica, quando i destinatari delle istanze di tutela sono soggetti fragili come i minori è richiesta un'attenzione maggiore. L'esposizione dei ragazzi in età scolare alle incognite della rete, molto spesso, è il riflesso di condotte poco accorte degli stessi esercenti la potestà genitoriale, i quali condividono informazioni che li riguardano o si

servono dei propri figli come tramite per l'utilizzo delle risorse telematiche²⁹.

Il tema della tutela dei minori in internet è stato attenzionato sotto diversi profili a livello europeo, internazionale e nazionale, al fine di reprimere comportamenti più gravi quali cyberbullismo e pedopornografia. Indubbiamente, la prospettiva civilistica costituisce la sede naturale del dibattito e rende necessario un ripensamento delle strategie di regolamentazione, che andrebbero riviste e adeguate coniugando, e non separando, diritto e tecnologia.

Le disposizioni sull'età per la valida manifestazione del consenso o sul controllo genitoriale non sono da sole sufficienti a neutralizzare i pericoli³⁰ che lo spazio digitale presenta per gli individui fragili e, per questo, sarebbe opportuno introdurre criteri di verifica del consenso per evitare la circolazione di informazioni non autorizzate sul web.

Un'analisi comparativa, imprescindibile ai fini di una visione completa degli argomenti oggetto di riflessione, non può non attingere dal modello statunitense³¹ e, nella specie, dal COPPA, che ha minuziosamente regolamentato le attività di raccolta e divulgazione on line dei dati personali riguardanti minori, attraverso la previsione di una serie di adempimenti (§ 312,3) a carico di operatori di siti web, di servizi on line, che siano consapevoli di trattare informazioni concernenti bambini.

La normativa si articola in un insieme di previsioni atte a proteggere la privacy on line dei minori e onera gli addetti ai lavori (§ 312.4) ad avvisare preventivamente i genitori, per ricevere un consenso verificabile prima delle attività di raccolta e trasmissione dei dati³².

Elemento centrale nella disciplina richiamata è la puntuale individuazione di criteri di verificabilità del consenso utili ad offrire una regolazione effettiva ed efficace dello stesso. Il paragrafo § 312.5, rubricato "*Consenso dei genitori*", prescrive specifi-

catamente un metodo di verifica (§ 312.5 B) “*ragionevolmente calcolato, alla luce della tecnologia disponibile, per garantire che la persona che fornisce il consenso sia il genitore del bambino*”.

Si prevedono, in particolare, la sottoscrizione da parte del genitore di un modulo da restituire all’operatore; la notifica al genitore titolare di *carta di credito, di debito o di altro sistema di pagamento on line* di ogni transazione effettuata; la possibilità del genitore di mettersi in collegamento con *personale addestrato* tramite chiamata o video conferenza; la verifica dell’identità del genitore medesimo.

La puntuale descrizione delle attività, finalizzate ad ottenere un consenso verificabile, prodromiche a qualsivoglia operazione avente ad oggetto i dati personali, rende chiaro l’approccio da seguire per intervenire in maniera stringente a tutela della sfera personale dei bambini, evidenziando le lacune in ambito europeo, ove è opportuno potenziare i criteri di verifica del consenso, per appurarne l’effettiva manifestazione da parte dei soggetti titolari della potestà genitoriale. L’esigenza di trovare una linea di intervento comune tra diritto e tecnologia, sebbene possa sembrare paradossale, nasce in realtà dall’acquisita consapevolezza che per gestire i rischi connessi alle innovazioni digitali è utile sfruttare i rimedi forniti dall’intelligenza artificiale. L’esplosiva diffusione di internet tra adolescenti e bambini rappresenta un fenomeno emergenziale che non può essere sottovalutato e richiede un approccio mirato, che tenga conto delle conseguenze imprevedibili dell’accesso alla rete per i minori.

Recenti fatti di cronaca hanno visto coinvolto un popolare social network, particolarmente gradito ai giovani, messo sotto accusa per l’incitamento a sfide e giochi pericolosi, filmati dai ragazzi e divulgati in rete, suscitando sentimenti di emulazione che, in alcuni casi, hanno condotto a esiti nefasti³³.

La sicurezza del web non abbraccia, quindi, esclusivamente la privacy, ma ha una portata maggiore, che coinvolge la dili-

genza e la capacità di discernimento dei piccoli utenti; il richiesto controllo da parte delle famiglie non sempre sortisce gli effetti sperati, essendo anche gli adulti disattenti e imprudenti nell'uso delle tecnologie.

La sinergia tra diritto e tecnica rappresenta l'unico canale possibile per ottenere risultati proficui, unitamente a un'attività di controllo costante, da parte delle autorità competenti, sul rispetto delle normative vigenti, corroborata dalla diffusione di campagne di sensibilizzazione ed educazione all'uso della rete.

Le misure che attualmente esistono in Europa a garanzia dei minori - oltre al consenso che, come evidenziato, non può fornire la certezza sulla liceità del trattamento dei dati, ove non suffragato da idonei elementi verificatori - fanno leva anche sulla trasparenza e completezza delle informazioni erogate. L'art. 5 del GDPR chiarisce che i dati devono essere trattati in modo lecito, corretto e trasparente e raccolti per *finalità determinate, specifiche e legittime*. Il concetto di trasparenza viene nuovamente richiamato nell'art. 12, a norma del quale le informazioni e le comunicazioni relative al trattamento dei dati devono essere concise, trasparenti e scritte in modo chiaro e semplice *in particolare nel caso di informazioni destinate specificamente ai minori*³⁴.

La necessità di reperire rimedi dalle stesse infrastrutture di rete, che si auspica di regolamentare, trova riscontro nella disposizione del GDPR (art.40 lett. g par.2) che faculta *le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento* all'emanazione di codici di condotta, diretti a chiarire l'applicazione del Regolamento, tra l'altro, sull'informazione fornita e sulla protezione del minore, sulle modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale³⁵. La creazione di codici di autoregolamentazione, qualora fosse condivisa e attuata dalle maggiori aziende digitali, potrebbe imprimere una traiettoria di avvicinamento e uniformazione sotto il profilo rimediale tra le diverse realtà statali³⁶.

Le ragioni di un simile approdo vanno individuate nella presa d'atto che è più pensabile di poter procedere a un'efficace regolazione della società basata sugli algoritmi, senza attingere dal bagaglio di innovazioni da essi stessi ottenute per trovare risposte soddisfacenti agli interrogativi irrisolti.

Il perfezionamento dei contenuti e delle tecniche di redazione delle informative sulla privacy, cui hanno puntato le politiche europee, non è servito a rendere consapevoli gli utenti (soprattutto i minori) dell'importanza dei dati trasmessi.

3.1. La tutela dei minori nel contesto dei giochi elettronici e online

L'ambito dei videogiochi attira un vasto bacino di utenti soprattutto minorenni che, proprio per la propensione a condividere propri dati, rappresentano le prede privilegiate delle aziende fornitrici dei relativi prodotti e servizi. Anche il settore dei giochi si alimenta con i progressi delle tecnologie digitali, attraendo, attraverso le strategie della rete, un numero sempre più consistente di clienti.

Il mercato di riferimento è strutturato in maniera tale da ricomprendere giochi mobili, console per videogiochi e piattaforme: la prima categoria comprende i giochi scaricabili sui dispositivi mobili e costituisce una pratica particolarmente diffusa nella prassi quotidiana che interessa gli utilizzatori di una fascia di età giovanissima (anche al di sotto dei 10 anni), i quali adoperano cellulari o tablet; le console per videogiochi sono apparecchi che, di regola, si collegano ad un televisore o possono essere muniti di uno schermo autonomo; le piattaforme, che nel tempo si sono diversificate e perfezionate, prevedono una serie di giochi di azione caratterizzati dal superamento di livelli da parte del soggetto con il quale si identifica il giocatore. Il mondo virtuale costituisce una grave minaccia per i giovani utenti, i quali spesso si ritrovano protagonisti di esperimenti

che ne mettono alla prova i comportamenti e creano dipendenza dalla rete.

Emblematica è la vicenda riguardante il videogioco *Pokemon Go*, lanciato nel 2016 dalla Niantic Inc., una società di sviluppo software americana, in collaborazione con Game Freak, The Pokemon Company e Nintendo (note aziende giapponesi del settore). Il gioco su piattaforma sfrutta la realtà, mediata dall'elaboratore e geolocalizzata, per coinvolgere i giocatori in una sorta di caccia al tesoro alla ricerca di figure virtuali, i Pokemon appunto, che appaiono sul display degli smartphone. L'utente si muove alla ricerca delle creature digitali finendo col ritrovarsi in spazi pubblici o privati senza rendersene conto. L'obiettivo è di catturare l'intera collezione di Pokemon acquisendo livelli superiori nel gioco. Il caso *Pokemon Go* riflette una problematica comune a tutte le fattispecie di gioco virtuale, concernente i possibili rischi legati alla sicurezza e alla privacy degli utilizzatori.

Il gioco proietta i giocatori in una realtà parallela e il sistema di geolocalizzazione registra tutti gli spostamenti, avvalendosi dell'ausilio di altri soggetti per la raccolta e l'interpretazione dei dati *raccogliendo continue fonti di surplus comportamentale*³⁷.

L'indagine circa le regole da seguire non può non attingere dal modello statunitense, in cui il programma Privacy Certified dell'ESRB (Entertainment Software Rating Board) prende in considerazione i rischi sulla privacy e gli obblighi a carico delle società di gioco³⁸; i principali ideatori di console prevedono un insieme di informazioni da scambiare tra gli utenti e gli sviluppatori di software³⁹, e aziende leader nel settore, come Apple e Google, impongono ai programmatori di app di impegnarsi a rispettare le linee guida sui dati, come prerequisito per la vendita di giochi nei rispettivi app store⁴⁰.

Riguardo agli acquisti in app merita menzione una recente decisione della Corte distrettuale della California, nel contenzioso azionato da Epic Games, società produttrice del gioco

multiplatforma *Fortnite*, nei confronti di Apple. La controversia ha avuto origine dalla rimozione da parte della società di Cupertino del gioco in seguito all'introduzione da parte di Epic Games di un'opzione di pagamento alternativa e con commissioni inferiori rispetto a quelle del 30% applicate dalla convenuta. La Corte, pur disattendendo le ragioni di parte attrice in merito alla configurazione di una condotta monopolistica illecita in capo ad Apple, ha imposto a quest'ultima di non vietare in futuro canali alternativi di pagamento⁴¹.

Sebbene i giochi siano sovente offerti in una versione gratuita, forniscono, in genere, anche opzioni per l'acquisto di costumi o oggetti virtuali per gli utenti desiderosi di acquisire abilità superiori o migliorare le prestazioni. I molteplici canali attraverso cui le società produttrici raccolgono i dati (hardware, funzionalità della piattaforma, tecnologie di tracciamento) minacciano la privacy degli utilizzatori. Avvenendo le transazioni attraverso appositi strumenti di pagamento (carte di credito, poste pay o altri mezzi simili), i titolari degli strumenti medesimi dovranno vigilare sull'uso accorto delle credenziali di accesso per l'autorizzazione delle operazioni.

Per limitare la possibilità per i minori di accedere a contenuti non adatti alla propria età o di effettuare operazioni pericolose, la gran parte delle aziende informatiche ha introdotto il cosiddetto *parental control* (controllo genitoriale), una funzionalità che mette in sicurezza i bambini da materiali e attività non consentiti, escludendo l'uso di giochi specifici e gli acquisti in app o richiedendo appositi codici di accesso. Il contenuto del dovere di vigilanza dei genitori va nondimeno controbilanciato con il principio di libertà di espressione e il diritto all'informazione spettanti al minore nell'esercizio della propria capacità di autodeterminazione⁴².

A destare allarme è la tendenza delle società produttrici dei giochi a estendere i flussi di dati raccolti a partner o fonti ester-

ne (piattaforme pubblicitarie), rendendo più complicati i controlli a garanzia dei soggetti deboli.

Se in ambito europeo il quadro giuridico non appare sufficiente a tutelare i minori, la cui attività in rete risulta sempre più variegata, un ruolo fondamentale svolgono le Autorità amministrative indipendenti, primo fra tutti il Garante Privacy, coadiuvato dal Comitato europeo per la protezione dei dati, che contribuisce all'attuazione delle norme contenute nel GDPR e promuove la cooperazione tra le autorità competenti nell'ambito dell'UE.

Nel 2011, con la legge del 12 luglio n. 112, è stata istituita l'Autorità garante per l'infanzia e l'adolescenza in attuazione della Convenzione ONU sui diritti dell'infanzia approvata dall'Assemblea Generale delle Nazioni Unite il 20 novembre 1989⁴³.

Nel 2014 è stato creato l'Osservatorio delle garanzie per i minori e dei diritti fondamentali della Persona su internet, al fine di analizzare le problematiche connesse all'utilizzo dei social network e di verificare l'efficacia delle procedure adottate dagli operatori.

In Italia, l'Autorità per le Garanzie nelle Comunicazioni (AGCOM), per far fronte all'inadeguatezza dei rimedi tradizionali rispetto alla digitalizzazione delle comunicazioni, ha elaborato, a partire dal 2013, un primo "Libro Bianco" sul rapporto tra media e minori, pubblicato il 24 gennaio 2014, seguito dal "Libro Bianco Media e minori 2.0" del 16 gennaio 2018.

Le iniziative intraprese, sotto l'impulso dell'AGCOM, hanno messo in luce le lacune degli apparati normativi tradizionali e la necessità di intervenire attivamente per reagire all'uso distorto della rete⁴⁴.

Sulla tutela dei minori e dei soggetti deboli, con riferimento ai cosiddetti acquisti *in-game*, è di recente intervenuta l'Autorità Garante della Concorrenza e del Mercato, che ha aperto un procedimento d'infrazione, ipotizzando pratiche commerciali scorrette a carico delle società del Gruppo Activision Blizzard, attive negli Stati Uniti e in Europa, in relazione alla promozione

e vendita sul mercato italiano, tramite siti internet, di videogiochi che offrivano la possibilità di effettuare acquisti all'interno dei giochi con denaro reale⁴⁵. L'istruttoria dell'Authority prendeva le mosse da segnalazioni e rilevazioni *ex officio* circa la mancanza di informazioni trasparenti e esaustive sulla presenza di acquisti in giochi, presentati come gratuiti, suscettibili di essere utilizzati da bambini e adolescenti. Il procedimento è stato definito con l'assunzione da parte del professionista di impegni in ordine a miglioramenti informativi, accompagnati da strumenti che consentano ai genitori di supervisionare l'utilizzo dei giochi da parte dei figli minori, in modo da prevenire acquisti indesiderati.

4. Conclusioni

Il quadro, fin qui delineato, suggerisce una chiave di lettura delle misure di tutela da adottare, improntata ad *una nuova sensibilità sulla cultura della comunicazione* per stimolare lo *spirito critico* e l'*autonomia decisionale* degli utenti⁴⁶.

La diffusione di internet e l'affermazione della sovranità digitale delle piattaforme tecnologiche hanno determinato una rivisitazione del concetto di privacy, al fine di adeguarne il contenuto all'esigenza di protezione dei dati personali. Siamo ormai lontani dalla concezione del diritto alla privacy come diritto ad essere lasciati soli e anzi, paradossalmente, siamo proiettati in una dimensione opposta, in cui appare naturale la condivisione delle informazioni riconducibili alla sfera privata come controprestazione dell'uso delle risorse digitali.

Nel travagliato percorso evolutivo, che ha portato a una ridefinizione del contenuto della privacy, un ruolo significativo hanno assunto dottrina e giurisprudenza nell'individuare le lacune e nel reperire le soluzioni più idonee per rimediare alle carenze degli apparati normativi esistenti.

Nelle molteplici articolazioni che la tematica può assumere, una peculiare connotazione riveste il profilo attinente alla salvaguardia degli interessi dei minori, minacciati dalla spregiudicatezza dei giganti online. L'analisi in chiave comparatistica ha messo in luce la necessità di vagliare l'effettiva consapevolezza, da parte dei giovani utilizzatori e di coloro che sono chiamati ad esperire l'attività di vigilanza⁴⁷, dell'incidenza delle tecnologie sulla sicurezza e sulla riservatezza dei soggetti coinvolti.

La tendenza a trascurare, o a non leggere completamente, le condizioni di accesso alle piattaforme rende superfluo il miglioramento dei criteri redazionali delle informative, cui hanno puntato le discipline di tutela europee e statunitensi, dimostrando l'inutilità dello strumento del consenso ad offrire, in via esclusiva, una protezione effettiva ed efficace. Un'attenzione maggiore, come evidenziato, merita il settore dei videogiochi, per le ricadute non solo nell'ambito della garanzia dei dati, ma anche per la correttezza delle transazioni commerciali. Il fenomeno degli acquisti in app, consueto nelle piattaforme di gioco, espone gli utenti all'applicazione di tariffe eccessive o a negoziazioni indesiderate, agevolate dalla scarsa attenzione prestata alle previsioni contrattuali.

La risposta alle perplessità segnalate non è la passiva accettazione della supremazia delle tecnologie digitali, ma, al contrario, una reazione attiva per frenarne la pervasività, veicolandone le abilità anche a servizio degli utenti, nell'ottica di avviare un percorso di sensibilizzazione al corretto utilizzo delle infrastrutture informatiche.

Note di chiusura

¹ S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019, p.531. L'affermazione del *capitalismo della sorveglianza* preoccupa gli studiosi, al punto da ritenere che vi sia una sconfitta delle democrazie occidentali, una *recessione democratica*.

² E. SADIN, *Critica della ragione artificiale. Una difesa dell'umanità*, Roma, 2019, p.11. L'autore ritiene che *stiamo entrando nell'era antropomorfa della tecnica*, ma non *in senso letterale*. Egli distingue un *antropomorfismo aumentato*, modellato sul cervello umano, ma più rapido; un *antropomorfismo frammentario* per lo svolgimento di compiti specifici; un *antropomorfismo intraprendente*, in grado di intraprendere azioni rivolte ad esiti prestabiliti.

³ S. ZUBOFF, *Il capitalismo della sorveglianza*, cit., pp. 18-78. Il *capitalismo della sorveglianza* trova origine nella *scoperta del surplus comportamentale*, ovvero nell'estrazione di più dati di quelli utili ad accrescere la qualità dei servizi e nel loro reinvestimento, che permette di prevedere le scelte future degli utenti trasformando i motori di ricerca in un'*intelligenza artificiale onnicomprensiva*.

⁴ M. ASTONE, *Il diritto all'oblio on line alla prova dei limiti territoriali*, in *Europa e dir. priv.*, 2020, n.1, pp. 223-235. Sulla connotazione e sul valore del dato personale cfr. V. Z. ZENCOVICH - G. G. CODIGLIONE, *Ten legal perspectives on the "big data revolution"*, in F. DI PORTO (a cura di), *Big Data e concorrenza*, n. spec., di *Conc. merc.*, 2016, p.29 ss.

⁵ L'espressione costituisce il cuore della dottrina dell'abuso, cioè dell'improprio ricorso da parte delle imprese alla più che legittima loro libertà di iniziativa economica, che incontra il necessario limite nel riconoscimento dell'altrui libertà di iniziativa, compresa quella - decisiva per l'*antitrust* - che si esprime nelle scelte sovrane dei consumatori. Anche la Corte giust. UE ha fatto più volte riferimento all'espressione medesima, in particolare, nelle decisioni *France Télécom*, 2 aprile 2009, C-202/07,109; *Deutsche Telekom*, 14 ottobre 2010, C-280/08,177; *Intel*, Grande Sez. 6 settembre 2017, C-413/14,136.

⁶ La registrazione rappresenta la moderna manifestazione del consenso al trattamento dei dati. I dati personali raccolti dai social network transitano, nella maggior parte dei casi, oltreoceano al fine di essere trattati e/o conservati dalla casa-madre: attualmente Facebook utilizza quattro data-center negli Stati Uniti e uno in Svezia; Twitter invece sfrutta data-center già esistenti, corrispondendo canoni di locazione degli spazi ai gestori, anch'essi tutti operanti all'interno del territorio statunitense.

⁷ Il reg. n. 2016/679/UE (GDPR) del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al

trattamento dei dati personali nonché alla libera circolazione di tali dati e attribuisce un ruolo centrale al consenso inteso come *qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato* (art.4, punto 11).

⁸ G. PITRUZZELLA, *Big data, competition and privacy: a look from antitrust perspective*, in *Conc. merc.*, 2016, p.15; M. MIDIRI, *Le piattaforme e il potere dei dati (Facebook non passa il Reno)*, in *Dir. inf.*,2021, n.2, II, p. 111.

⁹ N. ZORZI GALGANO, *Persona e mercato dei dati, Riflessioni sul GDPR*, Padova, 2019, p. 27.

¹⁰ La norma chiarisce che il soggetto interessato deve “ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare cui li ha forniti qualora:a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo1,lettera a),o dell'articolo 9,paragrafo2,lettera a),o su un contratto ai sensi dell'articolo 6, paragrafo 1,lettera b); e b) il trattamento sia effettuato con mezzi automatizzati.”(art. 20, comma 1 GDPR). A. MACERATINI, *Privacy e informazione nell'era dei Big Data*, in *Tigor: rivista di scienze della comunicazione e di argomentazione giuridica*, A., 2019, n. 2, XI, p. 87.

¹¹ M. BORGHI, *Portabilità dei dati e regolazione dei mercati digitali*, in *Merc. conc. reg.*, 2018, n.2 p. 243. L'autore chiarisce che la norma in quanto riferita a tutti coloro che effettuano operazioni di trattamento di dati personali, indipendentemente da eventuali contegni scorretti assunti, è stata criticata da parte della dottrina americana contraria all'applicazione di una cosiddetta *per se rule* per le ricadute negative in termini di incentivi ad innovare.

¹² La Carta dei diritti fondamentali dell'Unione, firmata a Nizza il 7 dicembre 2000 e riproclamata il 12 dicembre 2007, (in vista della firma del Trattato di Lisbona, a Strasburgo dal Parlamento europeo, dal Consiglio e dalla Commissione GUUE 14 dicembre 2007, n C. 303), che ai sensi dell'art. 6 par.1, primo comma, del Trattato ha, a partire dal 2007, lo stesso valore giuridico dei Trattati, all'art. 8 fa assurgere al rango di diritto soggettivo la protezione dei dati personali.

¹³ La prima elaborazione teorica in materia di *privacy* risale al volume di S. WARREN, L. BRANDEIS, *The right to privacy*, in *Harv. Law. Rev.*, 1890, 4, pag. 193. Nel sistema giuridico italiano, per una ricostruzione del concetto di *privacy*, v. T. AULETTA, *Riservatezza e tutela della personalità*, Milano, 1978. Nella giurisprudenza di legittimità significativa è la sentenza Cass. civ., 27 maggio 1975, n. 2129, in *Massimario della giurisprudenza italiana*, 1975, 594, in cui il Supremo Consesso ha riconosciuto il diritto di ciascun cittadino a che non siano resi

noti fatti o avvenimenti di carattere riservato senza il proprio consenso. La vicenda riguardava la richiesta di risarcimento avanzata dalla Principessa Soraya, ex moglie dello Shah dell'Iran, ripudiata dal marito a seguito della divulgazione di fotografie che la ritraevano in compagnia di un uomo all'interno della propria abitazione italiana. Qualche anno prima si era pronunciata la Corte costituzionale federale tedesca nel procedimento in cui erano convenuti la casa editrice "Die Welt" e il capo redattore K.-H.V. per aver pubblicato un'intervista della principessa Soraya senza verificarne la veridicità. Bundesverfassungsgericht (Prima Sezione), 14 febbraio 1973, *BverfGE* 34, 269 e *NJW* 1973,1221.

¹⁴ G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in *Dir. inf.*,2010, n.3, XXVI, p. 397; M. ASTONE, *Diritto all'oblio e motore di ricerca (Corte di Giust. Europea (Grande Sezione) sentenza 24 settembre 2019, causa C-507/17)*, in M. ASTONE (a cura di), *Il diritto dei consumatori nella giurisprudenza della Corte di Giustizia Europea*, Pisa, 2021, pp. 105-111.

¹⁵ La normativa italiana sulla privacy (d.lgs. 196/2003, che ha abrogato la precedente legge n.675/1996, razionalizzando e semplificando le disposizioni in materia) sancisce il *diritto alla protezione dei dati personali* (art. 1, d.lgs. 196/2003) e il *principio di necessità nel trattamento* (art. 3), che deve avvenire in "maniera lecita e secondo correttezza" (art. 11, lett. a): *i dati devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello occorrente al perseguimento degli scopi per i quali essi sono stati raccolti o successivamente trattati* (art. 11, lett. e).

¹⁶ Intervista a Pasquale Stanzone, Garante Privacy, *Monetizzazione dati fra le sfide più delicate*, in *Corriere delle comunicazioni*, 5 ottobre 2020.

¹⁷ Si pensi a tutti i dispositivi elettronici indossati dagli utenti o agli assistenti digitali di cui gli stessi si servono e che raccolgono e registrano dati in maniera continuativa.

¹⁸ C. CONTESSA, *Il potere pubblico al tempo dei Big Data*, in *Testo Unico dei servizi di media audiovisivi e radiofonici*, Piacenza, 2021 p. 9, secondo cui il titolare/consumatore/utente, pur accettando il trattamento dei propri dati, non si rende conto di cedere diritti inviolabili, facendo arretrare il loro ambito e l'apparato normativo a loro presidio a tutto vantaggio dei diritti proprietari di matrice economica.

¹⁹ Cfr. N. HELBERGER - O. LYNSKEY - H-W. MICKLITZ - P. ROTT -M. SAX - J. STRYCHARZ, *EU Consumer Protection 2.0, Structural asymmetries in digital consumer markets. A joint report from research conducted under the EUCP2.0 project*, 2021, p. 51 (<https://www.beuc.eu/publications/eu-consumer-protection-20-structural-asymmetries-digital-consumer-markets-0>), in cui si rileva che *l'asimmetria digitale è un*

fenomeno strutturale che colpisce tutti i consumatori e non può essere superato fornendo sempre più informazioni. Poiché il consumatore è strutturalmente e universalmente incapace di “capire” l’architettura digitale, l’informazione in qualsiasi forma non può rimediare all’asimmetria esistente.

²⁰ M.W. Monterossi, *La tutela dell’utente commerciale nei mercati digitali*, in *Contr. impr.*, 2021, n.3, Vol.37, p. 928.

²¹ La Commissione europea ha emanato una Comunicazione “*Verso uno spazio comune europeo dei dati*” (COM 2018, 232, 25 aprile 2018) proponendo un pacchetto di misure, *come passo essenziale verso uno spazio comune dei dati nell’UE, un’area digitale senza soluzione di continuità, la cui scala consenta lo sviluppo di nuovi prodotti e servizi basati sui dati.*

²² Il Parlamento europeo ha adottato una risoluzione “*recante raccomandazioni alla Commissione sulla legge sui servizi digitali: migliorare il funzionamento del mercato unico*” (2020/2018(INL)); una risoluzione “*recante raccomandazioni alla Commissione sulla legge sui servizi digitali: adeguare le norme di diritto commerciale e civile per i soggetti commerciali che operano online*” (2020/2019(INL)); una risoluzione “*sull’atto sui servizi digitali e le questioni sollevate in materia di diritti fondamentali*” (2020/2022(INL)).

²³ Già in passato l’UE si era prefissata l’obiettivo di intervenire in quest’ambito, in particolare la Commissione europea ha emanato una Comunicazione “*Verso uno spazio comune europeo dei dati*” (v., *supra*, nota 21). Nello stesso anno il Parlamento europeo e il Consiglio con la dir. n.2018/1972/UE hanno istituito il codice europeo delle comunicazioni elettroniche, ponendosi nel quadro della verifica dell’adeguatezza della regolamentazione (Regulatory Fitness- REFIT), nel cui ambito rientrano quattro direttive, le dir. nn. 2002/19/CE, 2002/20/CE, 2002/21/CE, 2002/22/CE, e il reg. n. 1211/2009/CE del Parlamento europeo e del Consiglio. La dir. 2018/1972/UE convoglia la regolamentazione dei settori delle telecomunicazioni, dei media, delle tecnologie dell’informazione in un unico codice europeo, dedicandosi alla disciplina delle reti e dei servizi delle comunicazioni elettroniche, ma non dei contenuti delle stesse.

²⁴ Il Consiglio europeo ha accolto favorevolmente la proposta di una legge sui servizi digitali al fine di garantire un adeguato livello di certezza del diritto. Cfr. Conclusioni del Consiglio sul tema “*Plasmare il futuro digitale dell’Europa*”, 8711/20, del 9 giugno 2020, su <https://www.consilium.europa.eu/media/44389/st08711-en20.pdf>.

²⁵ M.W. MONTEROSSO, *La tutela dell’utente commerciale nei mercati digitali*, cit., p. 929-930. L’autore chiarisce che nell’ambito digitale si creano tre tipologie di relazioni contrattuali: *quella tra il fornitore del servizio e l’utente commerciale;*

quella tra il fornitore del servizio e l'utente finale consumatore, quella tra l'utente commerciale e l'utente finale consumatore, precisando che, rispetto a quest'ultima, è sufficiente che il servizio promuova un contatto digitale e non che si perfezioni una transazione.

²⁶ Il 10 febbraio 2021 il Consiglio Europeo ha raggiunto un accordo sulla stesura finale del testo, che troverà attuazione due anni dopo la sua approvazione.

²⁷ C. PERLINGIERI, *La tutela dei minori di età nei social networks*, in *Rass. dir. civ.*, 2016, n.4, p.1324 e ss. A. Thiene, *I diritti della personalità dei minori nello spazio virtuale*, in *Annali online della Didattica e della Formazione del Docente*, 2017, n.13, IX, pp. 26-39.

²⁸ Il COPPA, 15 U.S.C. è una legge federale degli Stati Uniti, entrata in vigore il 21 aprile del 2000 e modificata nel 2013 dalla Federal Trade Commission (Federal Register / Vol. 78, No. 12 / Thursday, January 17, 2013 / Rules and Regulations), che riguarda la raccolta on line di informazioni personali di minori di età inferiore a 13 anni.

²⁹ La Suprema Corte (Cass. civ., sez. III, 5 settembre 2006 n. 19069) ha evidenziato la necessità di salvaguardare il minore nel contesto dei mezzi di comunicazione, richiamando l'art 16 della Convenzione sui diritti del fanciullo approvata a New York il 20 novembre 1989, che vieta interferenze arbitrarie o illegali nella sua vita privata, nella sua famiglia, nel domicilio o nella corrispondenza o lesioni alla sua reputazione o all'onore.

³⁰ A. GATTO, *Responsabilità genitoriale e controllo Facebook*, in M. BIANCA (a cura di), *The best interest of the child*, Roma, 2021, p. 208. L'autrice distingue tre tipologie di rischi in cui incorrono i minori nell'uso dei social: il *content risk* (rischio da contatto), il *contact risk* (rischio cui conduce l'uso di internet), il *conduct risk* (conseguenze dell'uso inappropriato della rete).

³¹ In materia di privacy negli Stati Uniti esiste un regime di tutela settoriale a seconda delle categorie di informazioni coinvolte. Oltre al già citato COPPA, meritano menzione: l'*Health Insurance Portability and Accountability Act* del 1996, una legge federale che richiede la creazione di standard nazionali per proteggere le informazioni sanitarie sensibili del paziente dalla divulgazione senza il consenso o la conoscenza del paziente stesso; il *Gramm-Leach-Bliley Act* del 1999, destinato alle società e alle istituzioni finanziarie che, nell'offerta dei propri prodotti o servizi finanziari, si rivolgono ai consumatori, imponendo loro di spiegare le pratiche di condivisione delle informazioni ai propri clienti e di salvaguardare i dati sensibili; il *Fair Credit Reporting Act* del 1970, che protegge le informazioni raccolte dalle agenzie di segnalazione dei consumatori

come agenzie di credito, società di informazioni mediche e servizi di screening degli inquinanti; il *Video Privacy Protection Act* del 1988, che regola la divulgazione di informazioni sull'utilizzo di contenuti video da parte dei consumatori, imponendo requisiti specifici per ottenere il consenso a tale divulgazione.

³² Il § 312,4 del COPPA individua analiticamente il contenuto dell'avviso da inoltrare ai genitori del fanciullo, al fine di ottenerne il *consenso affermativo alla raccolta, all'uso e alla divulgazione delle informazioni personali*.

³³ A seguito della morte di una bimba palermitana di 10 anni per asfissia, dopo una sfida su *Tik Tok*, il 22 gennaio 2021 il Garante della Privacy ha disposto (provvedimento n. 20) il blocco immediato di tutti i dati degli utenti per i quali non fosse stata verificata l'età anagrafica. Il social network si è adeguato al provvedimento del Garante, impegnandosi ad accertare l'età degli utilizzatori dell'app e introducendo un pulsante che permette agli utenti di segnalare eventuali altri utenti che non abbiano l'età di 13 anni, richiesta per l'accesso al social. L'episodio di cronaca ha stimolato l'introduzione di messaggi promozionali e lo stesso Garante per la Privacy, in collaborazione con il Telefono azzurro, ha deciso di avviare una campagna di sensibilizzazione per sollecitare i genitori ad effettuare i dovuti controlli nel momento in cui i figli utilizzano la piattaforma.

³⁴ Il principio è già sancito nel *considerando* 58 del reg. n. 2016/679/UE, secondo cui *"Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente"*.

³⁵ Il reg.n.2016/679/UE, al *considerando* 77, fa riferimento tra le possibili soluzioni all'adozione di codici di condotta attraverso i quali i titolari o i responsabili del trattamento possano autoregolamentarsi.

³⁶ G. PEDRAZZI, *Minori e social media: tutela dei dati personali, autoregolamentazione e privacy*, in *Infor. dir.*, XLII annata, 2017, n.1-2, XXVI pp. 437-451, p. 449. L'autore ritiene che, se i diversi Stati membri adottassero fasce di età differenti per il consenso al trattamento dei dati dei minori per i servizi on line, lo strumento dei codici di autoregolamentazione potrebbe servire a colmare una frammentazione normativa.

³⁷ S. ZUBOFF, *Il capitalismo della sorveglianza*, cit., p. 328, chiarisce che il videogioco costituisce la realizzazione del sogno del capitalismo della sorveglianza, consentendo la raccolta di dati per prevedere e indirizzare i comportamenti collettivi futuri.

³⁸ ESRB Privacy Certified, ENTM'T SOFTWARE RATING BB., su <http://www.esrb.org/privacy/> [<http://perma.cc/G82G-JYPB>].

³⁹ N. C. RUSSEL, J. R. REIDENBERG, S. MOON, *Privacy nel gioco*, 29 *Fordham Intell. Prop. Media & Ent. L.J.* 61, su <http://www.lexisnexis.com>, che si rifanno a J. Newman, *Press Start to Track? Privacy and the New Questions Posed by Modern Video Game Technology*, 42 *AIPLA Q.* 527, 567 (2014).

⁴⁰ App Store Review Guidelines, APPLE, su <https://developer.apple.com/app-store/review/guidelines/#privacy> [<https://perma.cc/9KSJ-T7YA>]; Developer Policy Center, GOOGLE PLAY, su <https://play.google.com/about/developer-content-policy-print/> [<https://perma.cc/G6H2-C6TT>].

⁴¹ *Epic Games Inc. v. Apple Inc.*, Case No. 4:20-cv-05640-YGR (United States District Court for the Northern District of California September 10, 2021). La Corte ha emesso un'ingiunzione preliminare permanente (con effetti a partire dal 9 dicembre 2021), con la quale obbliga Apple a non vietare agli sviluppatori l'inclusione, nelle loro app, di strumenti che indirizzino gli utenti a modalità di acquisto esterne alla piattaforma che potrebbero essere più vantaggiose per gli operatori.

⁴² Le libertà di espressione e di comunicazione (riconosciute dall'art. 21 della Costituzione italiana del 1948, dall'art.10 della Convenzione di Roma del 1950 e dall'art.11 della Carta dei diritti fondamentali dell'Unione Europea del 7 dicembre del 2000) spettano anche ai minori una volta raggiunta un'adeguata maturità psicofisica.

⁴³ La Convenzione è stata ratificata dall'Italia con la Legge n.176 del 27 maggio 1991.

⁴⁴ L'AGCOM, con Delibera n.16/22/Cons del 4 febbraio 2022, ha indetto una consultazione pubblica finalizzata all'adozione di Linee guida in attuazione dell'art. 7-bis del D.L. 30 aprile 2020, n. 28, relativo ai sistemi di protezione dei minori dai rischi del cyberspazio. Le risposte alla consultazione dovranno pervenire entro 45 giorni dalla data di pubblicazione della delibera sul sito web dell'AGCOM, e le linee guida saranno adottate entro i successivi 60 giorni.

⁴⁵ AGCM, *PSI1595 - Activision Blizzard-Acquisti nei videogiochi*, Provvedimento n. 28452 del 17 novembre 2020, in *Boll.* 48/2020.

⁴⁶ I. CORTONI, *La questione della consapevolezza digitale nei minori*, in M. BIANCA (a cura di), *The best interest of the child*, cit., p. 191. Interessante il riferimento dell'autrice al concetto di "Media Literacy", che individua la capacità di accesso, comprensione e valutazione dei media, e al concetto di "Media Education", riferito alle misure educative per rendere più consapevoli adulti e giovani nel contesto sociale (mediato e non mediato).

⁴⁷ G. VOTANO, *Il libro bianco Media e minori: l'età del consenso digitale tra consapevolezza e responsabilità*, in M. BIANCA (a cura di), *The best interest of the child*, cit., p. 248, il quale ritiene ormai superata la distinzione tra *nativi digitali* (bambini e adolescenti) e *immigranti digitali* (adulti), che adoperano attivamente gli strumenti multimediali e, purtroppo, assecondano l'uso non appropriato degli stessi da parte dei minori.

Trasformazione della filiera distributiva e responsabilità delle piattaforme del commercio elettronico nella proposta di direttiva “sulla responsabilità per danno da prodotti difettosi”

ROSARIO PETRUSO E GUIDO SMORTO

SOMMARIO: 1. Osservazioni introduttive: la proposta di direttiva “sulla responsabilità per danno da prodotti difettosi” del 28 settembre 2022. - 2. I legittimati passivi all’azione da prodotto difettoso negli intenti riformatori: l’art. 7 della proposta di direttiva. - 3. Un breve raffronto con l’art. 3 della direttiva 85/374/CEE: molte novità, nel solco della tradizione. - 4. Spunti di diritto comparato: il modello statunitense. - 4.1. La responsabilità delle piattaforme digitali per il danno da prodotto nel *case law* statunitense. - 4.2. Uno studio per fattispecie: i casi *Stiner v. Amazon*, *Loomis v. Amazon* e *McMillan v. Amazon*. - 4.3. L’applicabilità alle piattaforme del commercio elettronico della sezione 230 del *Communications Decency Act*. - 4.4. Elementi di riflessione e di sintesi sugli orientamenti giurisprudenziali d’Oltreoceano. - 5. Le funzioni principali della distribuzione: il servizio commerciale nell’apparato distributivo tradizionale. - 6. Funzioni della distribuzione e mercati digitali. - 7. Considerazioni critiche sul progetto di riforma. - 8. Osservazioni conclusive.

1. Osservazioni introduttive: la proposta di direttiva “sulla responsabilità per danno da prodotti difettosi” del 28 settembre 2022

A fine settembre 2022¹ la Commissione europea ha presentato una proposta di direttiva sulla responsabilità da prodotto difettoso², la quale – «tenuto conto dell’ampiezza delle modifiche necessarie e a fini di chiarezza e certezza del diritto»³ – si propone di sostituire integralmente la vecchia disciplina di armonizzazione

in materia risalente al 1985⁴. Secondo la Commissione, infatti, la disciplina vigente non sarebbe più in grado di dare risposte adeguate alle esigenze di tutela dei consumatori. Le ragioni di questa insufficienza sono identificate nei numerosi mutamenti dei modelli produttivi e distributivi verificatisi nel corso degli ultimi decenni, secondo una traiettoria che la Commissione riassume con la locuzione di sintesi “economia digitale e circolare”⁵. Per un verso, la digitalizzazione del sistema produttivo e di scambio (“economia digitale”) e, per l’altro verso, nuovi modelli di produzione e di consumo basati su condivisione, prestito, riutilizzo, riparazione, ricondizionamento e riciclo dei materiali e prodotti esistenti (“economia circolare”) hanno reso obsoleto un quadro di regole pensato per governare mercati profondamente diversi. Nasce da questa radicale trasformazione dei sistemi produttivi e distributivi l’esigenza di ridefinizione delle regole, che ha trovato una prima traduzione nella proposta di direttiva in commento.

La futura disciplina, il cui iter seguirà la procedura legislativa ordinaria, condivide con la direttiva 85/374/CEE la medesima base giuridica. Come la direttiva che andrebbe ad abrogare, la nuova si fonda sull’articolo 114 del TFUE⁶ e ha l’obiettivo di armonizzare le norme nazionali per promuovere la libera circolazione delle merci e per garantire la protezione dei consumatori⁷. In particolare, in linea di continuità con la disciplina vigente, la proposta ha lo scopo di conseguire un preciso equilibrio tra gli interessi dell’industria, dell’impresa commerciale e dei consumatori, perseguendo tre obiettivi specifici: 1) garantire che le norme sulla responsabilità riflettano la natura e i rischi dei prodotti nell’era digitale e nell’economia circolare; 2) assicurare che esista sempre un soggetto con sede nell’Unione responsabile per i prodotti difettosi acquistati da fabbricanti stranieri; 3) alleggerire l’onere della prova nel caso di beni complessi e allentare le limitazioni alla presentazione di domande di risarcimento, garantendo nel contempo un giusto

equilibrio tra produttori e consumatori⁸. A questi obiettivi si aggiunge l'ulteriore esigenza di allineare la disciplina da danno da prodotto alle importanti novità normative registratesi negli anni successivi all'approvazione della direttiva 85/374/CEE in settori ad essa complementari: in primo luogo, la legislazione in materia di sicurezza dei prodotti e di vigilanza nel mercato⁹ e, più di recente, il regolamento (Ue) 2022/2065 sui servizi digitali¹⁰, oltre che le numerose proposte legislative della Commissione attualmente in fase di negoziazione: dall'intelligenza artificiale¹¹, ai prodotti macchina¹², oltre che naturalmente la proposta di regolamento sulla sicurezza generale dei prodotti¹³.

Il livello di armonizzazione prescelto è quello "massimo"¹⁴. Pertanto, nelle materie che rientreranno nell'ambito di applicazione dello strumento di armonizzazione, gli Stati membri non potranno adottare disposizioni che rafforzino o indeboliscano le tutele previste in sede europea a beneficio del consumatore¹⁵.

Sul piano contenutistico le novità principali nascono tutte dalle innovazioni dovute alla digitalizzazione e ai nuovi modelli di produzione e consumo. In primo luogo, la proposta affronta la questione dell'irruzione sul mercato di prodotti innovativi, come ad esempio quelli interconnessi e/o dotati di intelligenza artificiale. In secondo luogo, si propone di normare inedite tipologie di danni, come nel caso di pregiudizi riconnessi alla perdita o alla corruzione di dati¹⁶. Infine, la proposta ridefinisce le responsabilità tra i diversi attori della filiera a seguito dell'ingresso di nuovi attori economici, tanto nella produzione (si pensi, ad esempio, alla comparsa di "ricondizionatori", produttori di software e fornitori di servizi digitali: tutte figure che contribuiscono a determinare, anche in un momento successivo all'immissione del prodotto nel mercato, le caratteristiche di sicurezza dei beni) quanto nella fase della commercializzazione dei beni (si pensi, ad esempio, all'avvento delle piattaforme del commercio elettronico che danno accesso al mercato a una miriade di venditori stranieri).

Alla luce di queste premesse, il presente lavoro si propone di esaminare l'ingresso dei nuovi attori economici digitali nella filiera di commercializzazione dei beni e la conseguente distribuzione delle responsabilità per il pregiudizio subito dal singolo a causa della difettosità di un prodotto venduto da terzi sulle piattaforme del commercio elettronico¹⁷. A tal fine, il lavoro prende in specifico esame l'art. 7 della proposta di direttiva, ossia la norma che amplia la platea dei legittimati passivi all'azione da danno da prodotto, per poi operare un raffronto tra la proposta di direttiva e la direttiva 85/374/CEE, al fine di verificare se e quanto il progetto riformatore si allontani dalla normativa vigente. In prospettiva comparatistica, il lavoro compie inoltre un raffronto con il modello statunitense, il quale offre una nutrita e poliedrica casistica sul tema. Inoltre ricostruisce le funzioni della filiera distributiva tradizionale per mostrare come le trasformazioni in atto nella struttura commerciale pongano un'esigenza nuova di tutela del consumatore. Nelle conclusioni l'articolo prova a formulare alcune considerazioni critiche relativamente alla completezza degli attuali programmi normativi di riforma.

2. I legittimati passivi all'azione da prodotto difettoso negli intenti riformatori: l'art. 7 della proposta di direttiva

Uno dei principali obiettivi dell'iniziativa legislativa consiste nell'assicurare che sia sempre reperibile, all'interno del mercato unico, un soggetto responsabile per i prodotti difettosi fabbricati da produttori stabiliti fuori dall'Unione. In questa prospettiva, l'intervento normativo si giustifica per una duplice ragione. Innanzitutto, perché i canali distributivi digitali - nel consentire l'acquisto di beni direttamente da produttori o venditori non situati all'interno del mercato unico - lasciano sprovvisto di tutela quel consumatore che non abbia come referente diretto un operatore economico della filiera distributiva tradi-

zionale stabilito nell'Unione. In secondo luogo, si rileva come le nuove "catene di approvvigionamento globali"¹⁸ creino distorsioni nel mercato tra i produttori con sede nell'Unione e i produttori stranieri, con i primi esposti alla concorrenza diretta dei secondi, i quali riescono agevolmente a sottrarsi al regime di responsabilità oggettiva scorporato nella direttiva 85/374/CEE.

L'art. 7 della proposta di direttiva - rubricato "operatori economici responsabili del danno da prodotti difettosi" - si propone l'obiettivo di dettare una disciplina che, al di là di dati meramente nominalistici, estenda al massimo grado il novero dei soggetti potenzialmente responsabili del danno da prodotto, chiamando in causa gli attori del ciclo sia produttivo sia distributivo¹⁹. In base a quanto stabilito dall'art. 7 rientrano tra i legittimati passivi all'azione proposta dal danneggiato tutti gli operatori economici della produzione. Ad essere chiamati in causa sono, innanzitutto, il fabbricante e il fabbricante del componente difettoso (cfr. comma 1). A tal proposito, è interessante osservare come la definizione normativa di "fabbricante" sia decisamente ampia: ai sensi della norma, per fabbricante si intende, infatti, ogni «persona fisica o giuridica che sviluppa, produce o fabbrica un prodotto o lo fa progettare o fabbricare, o che lo commercializza apponendovi il proprio nome o marchio, oppure che sviluppa, produce o fabbrica un prodotto per uso proprio» (art. 4 comma 1, n. 11).

Fanno parte della cerchia dei responsabili diretti del danno da prodotto anche coloro che modificano un bene già immesso sul mercato o già messo in servizio (art. 7, comma 4)²⁰. Ad essere chiamati in causa sono tutti coloro che, nell'ottica del riutilizzo del bene, ricondizionano o rigenerano un prodotto secondo i nuovi modelli aziendali tipici dell'economia circolare. Perché anche tali soggetti rispondano dei pregiudizi sofferti dal singolo, sarà, però, necessario che la modifica apportata al bene sia sostanziale e che sia effettuata al di fuori del controllo del fabbricante originario.

Con riferimento specifico alla filiera distributiva, nei casi in cui il fabbricante sia stabilito al di fuori dell'Unione rispondono del danno, il rappresentante autorizzato²¹ e l'importatore del prodotto difettoso²² (cfr. art. 7, comma 2). Nel caso in cui questi ultimi due operatori economici non siano stabiliti nell'Unione, del danno subito dal consumatore risponderà il "fornitore di servizi di logistica" (cfr. comma 3). Tale figura è definita al primo comma dell'art. 4 (n. 14) della proposta di direttiva come la «persona fisica o giuridica che offre, nel corso di un'attività commerciale, almeno due dei seguenti servizi: immagazzinamento, imballaggio, indirizzamento e spedizione di un prodotto, senza essere proprietario del prodotto»²³.

In via residuale, qualora non sia possibile identificare alcuno degli operatori economici prima elencati, del danno cagionato dal difetto del prodotto risponderà ogni "distributore" (comma 5). Tale responsabilità è, però, limitata alle sole ipotesi in cui quest'ultimo soggetto, richiesto, dalla vittima del fatto illecito, di rivelare l'identità di colui che, a propria volta, gli ha fornito il prodotto, ometta di identificarlo entro un mese dal ricevimento della richiesta. Alla posizione del distributore è parificata quella dei "fornitori di una piattaforma online" («diversi dal fabbricante, dall'importatore o dal distributore») che consentono ai consumatori di concludere contratti a distanza con altri operatori commerciali (art. 7, comma 6). Gli attori digitali espressamente considerati dall'ultimo comma della norma si aggiungono alla cerchia dei legittimati passivi all'azione per danno da prodotto esclusivamente in alcune ipotesi determinate. Si tratta, in particolare, di quei casi - richiamati in forza del rinvio al terzo comma dell'art. 6 del regolamento sui servizi digitali²⁴ - in cui tali soggetti presentino «informazioni specifiche o rendano altrimenti possibile l'operazione specifica in questione in modo tale da indurre un consumatore medio a ritenere che [...] il prodotto [...] oggetto dell'operazione, [sia] fornit[o] dalla piattafor-

ma stessa o da un destinatario del servizio che agisce sotto la sua autorità o il suo controllo».

3. Un breve raffronto con l'art. 3 della direttiva 85/374/CEE: molte novità, nel solco della tradizione

Un raffronto con la disciplina vigente consente di mettere in luce le non poche novità inserite nella proposta della Commissione, accanto a importanti similitudini. Nel riflettere la realtà economica del tempo, la direttiva 85/374/CEE rende responsabili gli attori tradizionali della filiera produttiva e distributiva: innanzitutto il fabbricante del prodotto finito e quello di una sua componente o della materia prima (art. 3, comma 1). In via vicaria, del danno da prodotto sono chiamati a rispondere anche alcuni operatori economici della filiera distributiva: i “produttori apparenti²⁵” (quei soggetti, cioè, che commercializzano prodotti commissionati a terzi, aggiungendovi il proprio marchio) e gli importatori (art. 3 comma 2). La ricerca dei legittimati passivi è estesa, infine, nella disciplina attualmente in vigore, ad «ogni fornitore» che non abbia comunicato al danneggiato, entro un termine ragionevole, l'identità del produttore, dell'importatore o degli altri soggetti della filiera che gli abbiano fornito il prodotto (art. 3 comma 3).

Rispetto alla disciplina vigente, nel progetto riformatore fanno ingresso nuove figure del sistema distributivo. Alcune di esse identificano operatori economici già contemplati dal legislatore europeo in altre normative recenti. Ad esempio, il “rappresentante autorizzato del fabbricante” e il “fornitore di servizi di logistica” sono rispettivamente presi in considerazione nel quadro comune per la commercializzazione dei prodotti²⁶ e nella normativa relativa alla vigilanza del mercato e alla conformità dei prodotti²⁷. Altre figure, invece, chiamano espressamente in causa, con un riscontro letterale corrispondente, fi-

gure ignote per l'innanzi: i nuovi attori, dunque, dell'economia digitale. È questo il caso dei "fornitori di piattaforme online".

Il confronto con la direttiva 85/374/CEE mette ancora in luce come, in prospettiva innovativa, una simile estensione del novero dei soggetti responsabili abbia lo scopo di evitare le angustie di qualificazioni meramente nominalistiche. Al fine di riflettere la sempre maggiore complessità della filiera distributiva, che - si legge al considerando n. 27 della proposta - coinvolge talvolta «operatori economici la cui nuova forma fa sì che non rientrino facilmente nelle catene di approvvigionamento tradizionali», il legislatore europeo si è preoccupato di adottare definizioni volutamente ampie. È questo il caso dei "fornitori di servizi di logistica", identificati con riferimento ad una rosa ampia di attività: immagazzinamento, imballaggio, indirizzamento e spedizione di un prodotto. Allo stesso modo, è questo pure il caso dei "fornitori di piattaforma online", definiti - tramite il rinvio all'art. 3 del regolamento sui servizi digitali - come quei prestatori di servizi «di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza[no] e diffond[ono] al pubblico informazioni²⁸».

Su altri fronti non si registrano, invece, mutamenti di passo rispetto al quadro normativo in via di superamento e ci si pone nel solco della disciplina vigente. Ci si riferisce, innanzitutto, alla scelta di fare salva la peculiare impostazione di fondo che - come notato in dottrina - «eleva il produttore al ruolo di soggetto dominante entro il sistema economico» e che pone in posizione solo «servente» la distribuzione commerciale²⁹. Allo stesso modo, non si annoverano cambiamenti di rotta nemmeno con riguardo alle specifiche ripartizioni del carico delle responsabilità tra gli attori della distribuzione³⁰. Trova conferma l'idea, centrale nella normativa da superare, che distingue le responsabilità di tali soggetti a seconda dei compiti svolti nella catena di approvvigionamento, in base ad un modello secondo cui alcuni operatori economici

sono chiamati a rispondere del danno subito dal consumatore in maniera più severa rispetto agli altri soggetti della stessa filiera, conservando la vittima il diritto di agire nei loro confronti in aggiunta e non in alternativa agli effettivi fabbricanti del prodotto difettoso o agli anelli precedenti del momento distributivo.

Nella normativa attualmente vigente l'attribuzione di un carico maggiore di responsabilità si articola secondo una linea di demarcazione che si fonda sul ruolo giocato da ciascun soggetto nella circolazione del prodotto³¹. Alla "immissione" nel mercato unico si accompagnano le maggiori responsabilità fissate dall'art. 3, comma 2, della direttiva 85/374/CEE. Alla successiva circolazione del prodotto difettoso si accompagna, invece, il regime - meno severo - di cui al comma 3 della medesima disposizione³². Nella direttiva 85/374/CEE la responsabilità degli importatori (quali soggetti preposti, nel diritto dell'Unione, alla prima messa a disposizione di un prodotto sul mercato unico) concorre con quella degli effettivi fabbricanti del prodotto difettoso con cui essi risponderanno in solido³³. Di contro, il fornitore - e, dunque, ogni distributore che nella catena commerciale partecipa insieme ad altri alla ulteriore circolazione del bene all'interno del mercato unico - risponde del danno da prodotto solo in via eccezionale e residuale, dato che la responsabilità si arresta allorché abbia consentito di individuare, l'attore della filiera che lo precede a prescindere dalla solvibilità e dalla effettiva comparsa in giudizio.

Allo stesso modo, nella proposta di direttiva rispondono, insieme all'importatore ed allo stesso titolo di quest'ultimo, quei soggetti che contribuiscono fattivamente alla prima messa a disposizione nel mercato unico di un prodotto fabbricato fuori dall'Unione: il "rappresentante autorizzato del fabbricante" e il "fornitore di servizi di logistica"³⁴. In secondo luogo, ed analogamente a quanto previsto nella direttiva 85/374/CEE, anche nel progetto di riforma, "distributori" e "fornitori di piattafor-

me online” rispondono del danno solamente in ipotesi residuali: potranno, infatti, esonerarsi da ogni responsabilità tramite la semplice comunicazione alla vittima dell’identità degli attori che li precedono nella catena di fornitura e distribuzione.

4. Spunti di diritto comparato: il modello statunitense

Un’analisi comparatistica del modello statunitense può essere utile ad apprezzare la portata e il significato dell’intervento riformatore della Commissione europea sul tema del danno da prodotto. Come già in passato, il modello statunitense costituisce un punto di riferimento imprescindibile in materia. Ad inizio novecento, con il superamento della *privity of contract* e l’affermazione di un regime di *strict liability*³⁵ seppe adattare il proprio quadro di regole al profondo cambiamento del sistema produttivo e della struttura del mercato, affermando l’esistenza di un rapporto diretto (pur in assenza di contratto) tra produttore e consumatore finale. Allo stesso modo, dinanzi l’affermazione di nuovi attori della filiera, il diritto statunitense ha assunto il ruolo di apripista nel tentativo di individuare in concreto gli effettivi spazi di tutela di cui il consumatore può godere nelle fattispecie di danno di cui ci occupiamo: pur nella estrema eterogeneità delle discipline statali³⁶, si basa su una generale regola di responsabilità estesa, in via solidale, a tutti gli attori della filiera produttiva-distributiva³⁷. Il consumatore, dunque, ben può, agire per il risarcimento integrale del danno nei confronti di uno qualsiasi dei corresponsabili in solido, con possibilità poi, per chi ha risarcito l’intero danno, di regresso nei confronti degli altri.

È per queste ragioni che appare particolarmente proficuo procedere all’esame della giurisprudenza statunitense che prende in considerazione il ruolo svolto dagli intermediari digitali nella distribuzione commerciale. Gli Stati Uniti d’America offrono all’interprete una casistica già molto nutrita. Ad essere og-

getto di scrutinio è in particolare la responsabilità delle piattaforme digitali, le quali sono state chiamate in causa a seguito del verificarsi di incidenti di vario genere: monopattini elettrici che si incendiano e distruggono case³⁸, guinzagli retrattili per cani che si spezzano e accecano i padroni³⁹, batterie di computer portatili che esplodono ferendo il malcapitato⁴⁰, fino alla morte causata dall'assunzione di integratori a base di caffeina⁴¹. In particolare, negli ultimi anni si sono registrati i primi importanti precedenti di corti superiori statali che ben riassumono un quadro giurisprudenziale di prossimità ben più variegato⁴².

Alla luce di queste premesse, nelle riflessioni che seguono ci si propone di illustrare le diverse linee di tendenza che stanno prendendo forma nel *common law* statunitense nel far fronte ai problemi posti dalla transizione digitale. In via preliminare, possiamo distinguere un primo approccio, di tipo formalistico, incentrato sulla effettiva titolarità del prodotto difettoso prima che venga ceduto al consumatore, ed un secondo, più liberale, in cui la riflessione si appunta sul ruolo in concreto assunto dalla piattaforma nella messa in circolazione del bene.

4.1. La responsabilità delle piattaforme digitali per il danno da prodotto nel *case law* statunitense

Al fine di sottrarsi alla distribuzione delle responsabilità tra gli altri agenti del mercato, tipicamente le piattaforme digitali tendono a collocarsi all'esterno della rete di commercializzazione e a presentarsi come meri intermediari che si limitano a facilitare in maniera neutrale e non invasiva l'incontro di domanda ed offerta⁴³. Di fronte a questa rappresentazione, la giurisprudenza americana – nel tentativo di verificare l'effettiva applicabilità del regime del danno da prodotto agli attori digitali della filiera di commercializzazione – segue diversi itinerari, di cui adesso si darà conto.

Secondo un primo orientamento, le piattaforme del commercio elettronico non troverebbero una esatta collocazione all'interno della filiera distributiva e andrebbero esenti dalle connesse responsabilità in quanto avrebbero sviluppato un modello imprenditoriale innovativo che “non dipende dalla titolarità formale del bene⁴⁴”. L'elemento centrale per individuare chi - tra i soggetti che a vario titolo concorrono a portare il prodotto difettoso sino al consumatore finale - debba essere considerato soggetto passivo dell'obbligazione risarcitoria sarebbe la proprietà effettiva del bene⁴⁵: fornendo esclusivamente servizi ancillari al buon funzionamento del mercato, gli intermediari digitali sfuggirebbero ai regimi di responsabilità oggettiva per il danno da prodotto.

In base ad un secondo orientamento, è necessario, invece, sganciarsi da un approccio incentrato sulla titolarità formale del bene e accertare in concreto il ruolo assunto dalle piattaforme nel fungere da tramite tra prodotto e mercato. In questa linea argomentativa, la riflessione si sposta, pertanto, sugli elementi rilevanti ai fini di tale valutazione.

In questo alveo, l'accertamento di tali elementi dà luogo a un'ulteriore biforcazione degli esiti interpretativi. In alcuni casi, le corti hanno individuato nel controllo del singolo prodotto fonte di pregiudizio l'elemento centrale capace di attrarre l'intermediario digitale nel momento distributivo⁴⁶. L'effettiva disponibilità materiale della merce rappresenterebbe il presupposto teorico di attribuzione della responsabilità lungo il canale di approvvigionamento. Elemento indispensabile ai fini della responsabilità in esame si rivela dunque la prestazione da parte della piattaforma di servizi di logistica⁴⁷: non prestando tali servizi, andrebbe considerata come un soggetto fisicamente troppo distante dal processo distributivo, tradizionalmente incentrato su una relazione diretta con il bene⁴⁸. In altri casi, invece, l'accertamento giudiziale ha riguardato il complesso delle attività svolte dalla piattaforma, con la consegna diretta del

bene derubricata a circostanza di per sé non decisiva. Ove nel complesso la piattaforma eserciti un controllo significativo sullo scambio - è la conclusione di questa diversa impostazione - essa è considerata «parte integrante del sistema di produzione e commercializzazione che deve sopportare i costi dei danni derivanti da prodotti difettosi»⁴⁹.

4.2. Uno studio per fattispecie: i casi *Stiner v. Amazon*, *Loomis v. Amazon* e *McMillan v. Amazon*

Fatte queste premesse, occorre adesso entrare nel merito delle più recenti pronunce delle corti superiori nazionali rese negli ultimi due anni. A tal fine esamineremo la decisione della Supreme Court dell'Ohio resa il primo ottobre 2020 nel caso *Stiner v. Amazon.com*⁵⁰, in cui l'attenzione è indirizzata al controllo esercitato dalla piattaforma sul prodotto, la decisione della Court of Appeal della California resa il 26 aprile 2021 nel caso *Loomis v. Amazon.com*⁵¹, in cui l'accertamento compiuto dalla Corte è tutto rivolta a verificare il livello di controllo e di influenza esercitato dalla piattaforma sullo scambio, e la decisione della Supreme Court del Texas resa il 25 giugno 2021 nel caso *Amazon.com v. McMillan*⁵², in cui la *ratio decidendi* si fonda sul dato nominalistico del trasferimento del titolo del prodotto difettoso.

Partendo da quest'ultima pronuncia, in *Amazon.com v. McMillan* la questione della responsabilità delle piattaforme del commercio elettronico è stata presa in esame dalla Corte nell'ambito di un incidente pregiudiziale sollevato dal giudice federale⁵³, chiamato ad applicare in *diversity* il diritto statale. La questione riguardava l'eventuale responsabilità di *Amazon* relativamente alle lesioni permanenti subite da un bambino a causa della ingestione della batteria di un telecomando prodotto in Cina, privo di dispositivi di sicurezza volti a prevenire l'apertura del relativo alloggiamento. Più in particolare, occorre chiarire se la

piattaforma sarebbe potuta essere ritenuta responsabile, ai sensi della normativa statale che regola il danno da prodotti, in qualità di “*seller*”, relativamente ai beni venduti da terzi e gestiti tramite il programma di logistica della piattaforma⁵⁴.

In forza del *Chapter 82 del Texas Civil Practice and Remedies Code* del 1993, infatti, anche il distributore non produttore (“*seller*”) è tenuto - in talune ipotesi statutariamente disciplinate - a rispondere oggettivamente del danno subito dal consumatore a causa della difettosità del bene⁵⁵. In particolare, il “*seller*” è imputabile dei danni causati dalla difettosità del prodotto nel caso in cui l’attore dimostri che «il fabbricante [...] (A) è insolvente o (B) non è soggetto alla giurisdizione della Corte».

In base alla normativa statale applicabile tale operatore economico è definito come quel «soggetto che è impegnato nell’attività di “distribuire” o di “mettere altrimenti in commercio”, per qualsivoglia scopo commerciale, un prodotto o una parte di esso per l’uso o il consumo⁵⁶». Le difficoltà interpretative sorgono perché la norma non spiega cosa significhino le espressioni “distribuire” o “mettere altrimenti in commercio”.

In questo quadro, la Suprema Corte statale ha affermato che il termine “*seller*” ricomprende due tipologie di soggetti: coloro che “distribuiscono” un bene nell’ambito di un’attività propriamente qualificabile come alienazione e coloro che “immettono” un bene in commercio secondo modalità diverse (si pensi alle cessioni di campioni gratuiti effettuate a fini promozionali). Tanto gli uni, quanto gli altri operatori commerciali condividerebbero, però, una prerogativa irrinunciabile: sarebbero qualificabili come “proprietari” delle merci che contribuiscono a piazzare sul mercato. In entrambe le ipotesi, dunque, “*seller*” è colui che, nella catena di distribuzione, non è semplice “detentore” del bene avviato al consumatore finale⁵⁷.

Il mantenimento della titolarità del prodotto ed il conseguente potere di disposizione sino al momento della sua aliena-

zione all'utilizzatore finale rappresentano per la Corte il criterio di imputazione del regime di responsabilità oggettiva previsto per gli attori della filiera distributiva. Ne consegue che coloro che si limitano ad assistere o facilitare le vendite non integrano i requisiti per essere qualificati "seller"; si tratterebbe, piuttosto, di soggetti che coadiuvano i distributori, facilitandone indirettamente il compito (attraverso la fornitura di servizi ancillari e strumentali al buon funzionamento del mercato).

Per la Suprema Corte, dunque, le azioni poste in essere dalla piattaforma digitale - quali quelle di *web hosting*, di pubblicità, di *marketing*, di immagazzinamento, di elaborazione dei pagamenti e di spedizione al consumatore - non sono sufficienti ai fini della imputabilità del danno da prodotto. *Amazon*, si legge conclusivamente nella pronuncia, ha sviluppato un modello imprenditoriale innovativo «che non dipende dal titolo»⁵⁸ e sfugge, pertanto, alle relative responsabilità.

In altre pronunce la *ratio decidendi* si incentra, invece, sul livello di controllo esercitato dall'intermediario digitale sul processo distributivo. In *Stiner v. Amazon.com*⁵⁹ la Supreme Court dell'Ohio è stata chiamata a pronunciarsi sulla applicabilità della normativa interna posta a regolamentazione delle fattispecie di danno di cui ci occupiamo (l'*Ohio Products Liability Act*⁶⁰) relativamente alla morte di un giovane causata dall'assunzione di un integratore a base di caffeina (preparato da un'industria farmaceutica cinese), acquistato da un venditore terzo che operava sulla piattaforma convenuta.

Ai sensi della disciplina sul danno da prodotto vigente in Ohio, il "fornitore" ("*supplier*") è responsabile in circostanze determinate del danno arrecato al singolo dal prodotto difettoso allo stesso titolo del produttore⁶¹. Tra queste, rilevano quelle stesse ipotesi prese in considerazione dalla legge texana su cui prima si è incentrata la riflessione: le evenienze, cioè, in cui il fabbricante non sia soggetto alla giurisdizione della Corte statale o in cui egli

sia insolvente. Inoltre, l'*Ohio Products Liability Act* definisce il “*supplier*” come quel soggetto che, nel corso di un’attività imprenditoriale, «aliena, distribuisce [...], prepara, miscela, impacchetta, etichetta» il prodotto difettoso. Con una norma di chiusura, volta ad estendere ulteriormente⁶² il novero dei soggetti potenzialmente responsabili, il legislatore ha, poi, previsto che è legittimato passivo all’azione anche quel “*supplier*” che «partecipa altrimenti all’immissione del prodotto nella rete commerciale».

A differenza di quanto accaduto nel caso esaminato in precedenza, l’intermediario digitale non aveva assunto alcun ruolo nell’immagazzinamento, nell’impacchettamento e nella successiva spedizione del prodotto al consumatore. Tali compiti erano stati, infatti, integralmente assolti dal venditore. Non avendo svolto la piattaforma alcuna delle attività nominativamente previste dalla prima parte della norma, i giudici del supremo collegio hanno incentrato le proprie riflessioni sulla parte successiva, la quale amplia la cerchia dei legittimati passivi all’azione da prodotto difettoso. La locuzione «partecipa altrimenti all’immissione del prodotto nella rete commerciale» è stata, però, ritenuta applicabile esclusivamente ai fornitori che svolgono funzioni assimilabili a quelle esemplificate nella prima parte della disposizione: azioni, tutte, accomunate - nel ragionamento della Corte - da un atto di controllo sullo specifico prodotto immesso nel mercato⁶³.

Non essendo mai entrata in possesso dell’integratore a base di caffeina, la piattaforma è stata ritenuta un soggetto fisicamente troppo distante dal processo di distribuzione; processo di distribuzione statutariamente incentrato - nell’interpretazione fornita dalla Corte suprema - sul controllo materiale della merce. Il fatto che l’intermediario digitale si fosse riservato la totale discrezionalità nel determinare il contenuto, l’aspetto e il design del proprio sito web, che avesse impedito ai venditori di contattare i clienti, che si fosse attribuito il diritto di modificare

le descrizioni dei prodotti, che avesse imposto dei vincoli sulla determinazione dei prezzi da praticare al dettaglio⁶⁴ sono tutti elementi che – secondo questa prospettiva – dimostrano esclusivamente il tentativo della piattaforma di esercitare nei rapporti interni con i venditori una forza predominante e un penetrante grado di controllo⁶⁵.

Un'altra recente fattispecie relativa alla legittimazione passiva delle piattaforme digitali nell'azione da danno da prodotto è quella esaminata dalla California Court of Appeal in *Loomis v. Amazon.com*⁶⁶. In questo caso i giudici californiani hanno preso in considerazione il ricorso promosso da una consumatrice avverso la sentenza di primo grado che aveva respinto l'azione promossa nei confronti della piattaforma elettronica per il risarcimento del danno derivante dalle lesioni personali subite a causa di un incendio provocato da un *hoverboard* acquistato, tramite l'intermediario digitale, da un venditore cinese il quale aveva provveduto in autonomia alla relativa consegna.

A differenza di Texas e Ohio, nel diritto californiano la responsabilità da prodotto difettoso non ha trovato consacrazione sul piano legislativo, ma è lasciata all'evoluzione del *common law*⁶⁷. Ciò ha tradizionalmente consentito alla giurisprudenza di incentrare la risposta da dare all'interrogativo circa l'estendibilità della legittimazione passiva nell'azione da prodotto difettoso agli anelli della distribuzione non sulle tecnicità di un dato legislativo formale, ma sul concreto accertamento dell'apporto fornito da ciascun operatore della filiera nel facilitare la circolazione del bene fonte di pregiudizio⁶⁸. Su questo fronte si incentra anche la riflessione della Court of Appeal⁶⁹.

L'attenzione della Corte si appunta sul controllo esercitato dalla piattaforma sull'intera concatenazione negoziale che porta il prodotto, attraverso una serie di passaggi intermedi, sino al consumatore finale. In particolare, sono le circostanze peculiari della regolazione dei rapporti intercorrenti con il venditore del

prodotto difettoso e con il consumatore finale che per la Corte meritano la massima considerazione al fine di procedere all'espansione della cerchia dei soggetti responsabili per il danno subito dal singolo.

Per la Court of Appeal, la piattaforma - pur non prestando servizi di logistica⁷⁰ - controlla ogni aspetto della transazione dal versante sia del consumatore sia del venditore⁷¹. Con riguardo all'acquirente, la piattaforma "cattura" i consumatori sul proprio sito⁷², proponendo offerte speciali e programmi in abbonamento che permettono l'accesso a offerte esclusive; li vincola ad interagire direttamente con la piattaforma per effettuare l'ordine del prodotto e per pagare il prezzo di acquisto; ne gestisce le comunicazioni con il venditore sia nella fase che precede l'acquisto (nel caso in cui abbia una domanda da porre al venditore) sia in quella successiva (nel caso in cui sia sorto un problema): la piattaforma si atteggia, pertanto, ad unico interlocutore del consumatore. Con riguardo al venditore, il ruolo di *Amazon* è ritenuto ancora più pervasivo. Il venditore - benché come ammesso in sentenza sia l'unico soggetto che detenga formalmente il titolo sul bene da alienare⁷³ - non ha un rapporto diretto con il consumatore: nella maggior parte dei casi, tra venditore e acquirente non intercorrono comunicazioni; il venditore apprende che una vendita è stata effettuata semplicemente da una notifica da parte della piattaforma; *Amazon* decide in autonomia se consentire o meno il completamento della transazione; le eventuali domande del consumatore rivolte al venditore sono anonimizzate e gestite attraverso un servizio di messaggistica interno; è fatto divieto al venditore di comunicare altrimenti con il consumatore, di richiedere forme alternative di pagamento, di influenzare le decisioni di acquisto di quest'ultimo o di utilizzare le sue informazioni per scopi promozionali.

Con riferimento al livello di controllo e di influenza esercitato dalla piattaforma sullo scambio⁷⁴, richiamando testualmente

il proprio precedente *Bolger v. Amazon.com* la Corte californiana conclude osservando che, al di là di dati puramente nominalistici, «qualunque sia il termine da adoperare per descrivere il ruolo di *Amazon* - che si tratti di “rivenditore”, “distributore” o semplicemente “facilitatore” - la piattaforma è stata fondamentale nel portare il prodotto al consumatore finale⁷⁵».

4.3. L'applicabilità alle piattaforme del commercio elettronico della sezione 230 del *Communications Decency Act*

Da ultimo, occorre menzionare gli ultimi orientamenti giurisprudenziali circa l'applicabilità alle piattaforme del commercio elettronico della disciplina federale di esonero da responsabilità racchiusa nella sezione 230 del *Communications Decency Act* (CDA)⁷⁶. Le contestatissime «ventisei parole che crearono Internet»⁷⁷, nate con lo scopo di escludere che le piattaforme digitali potessero essere equiparate a “*publisher*” o “*speaker*” quanto a responsabilità per i contenuti pubblicati dagli utenti, sono state spesso invocate in giudizio non solamente dalle piattaforme di informazione come *Facebook* e *Twitter*, ma anche da quelle per lo scambio di beni e servizi⁷⁸.

Dinanzi a tale argomento, sollevato dalle piattaforme del commercio elettronico al fine di essere estromesse dal processo⁷⁹, la giurisprudenza statunitense, dopo qualche iniziale oscillazione, è ora concorde nel ritenere che la sezione 230 del CDA possa schermare da responsabilità per prodotti difettosi solo in ipotesi ben delimitate⁸⁰. Se in una prima fase non si esitava, infatti, a sostenere che gli intermediari digitali del commercio elettronico sarebbero stati protetti dall'insorgere di qualsivoglia forma di responsabilità (ivi inclusa, pertanto, quella per danno da prodotto)⁸¹, in una seconda e più recente fase si afferma che la normativa federale del *Communications Decency Act* possa trovare applicazione esclusivamente in quel-

le evenienze in cui la piattaforma sia stata citata a giudizio dal consumatore per non aver fornito le appropriate avvertenze sull'uso del prodotto fonte di pregiudizio o per non averle correttamente modificate ed aggiornate⁸².

In tali casi, infatti, l'azione fatta valere dal consumatore, discenderebbe dal "trattare" l'operatore digitale alla stregua di un editore ("*publisher*"), che dà diffusione a contenuti altrui: una siffatta azione sarebbe, pertanto, inaccoglibile in quanto si incentrerebbe proprio sul tipo di responsabilità escluso dalla sezione 230 CDA⁸³. L'obbligo che si assumerebbe violato sarebbe, infatti, ricollegabile al mancato monitoraggio dei contenuti generati dai venditori terzi (gli annunci di vendita e le schede prodotto presenti sulle piattaforme digitali); obbligo non previsto dalla normativa federale.

Fuori da queste limitate ipotesi, la sezione 230 CDA non sarebbe d'ostacolo all'azione del singolo, danneggiato dal prodotto difettoso. L'imputabilità della piattaforma sarebbe, infatti, da mettere normalmente in relazione con la partecipazione "attiva" dell'intermediario digitale alla vendita (attraverso azioni, quali l'elaborazione dei pagamenti, l'immagazzinamento e la spedizione) e non con il ruolo da esso svolto nella disseminazione delle informazioni fornite da terzi⁸⁴. La condotta della piattaforma da considerare ai fini della imputabilità consiste non nel mancato controllo dei contenuti altrui (condotta che sarebbe del tutto irrilevante ai sensi della sezione 230 CDA), ma nella compartecipazione attiva allo scambio avente ad oggetto il prodotto difettoso.

4.4. Elementi di riflessione e di sintesi sugli orientamenti giurisprudenziali d'Oltreoceano

Una considerazione d'insieme della giurisprudenza statunitense passata in rassegna mette in evidenza, da un punto di osservazione comparatistico, tanto la novità del problema posto dal-

la transizione digitale quanto il punto di maggiore scoperta della attuale direttiva 85/374/CEE che la Commissione europea si propone di superare.

Le sollecitazioni che si possono cogliere dal precedente texano pongono in luce l'originalità dei sistemi di scambio ricollegabili alla digitalizzazione dell'apparato distributivo e le correlate difficoltà di tutela del danneggiato ove il criterio di imputazione della responsabilità della piattaforma sia agganciato alla proprietà effettiva del bene che arreca danno. Come ben messo in luce dalla Supreme Court del Texas, le piattaforme del commercio elettronico hanno sviluppato un modello imprenditoriale innovativo che non dipende dal titolo⁸⁵: da questa prospettiva, tali operatori economici, non trovando una esatta collocazione all'interno della filiera distributiva, andrebbero esenti dalle connesse responsabilità. Le altre due decisioni della Supreme Court dell'Ohio e della Court of Appeal della California per adeguarsi alle trasformazioni del momento economico si svincolano da un'analisi fondata sulla titolarità del bene e si incentrano sul livello di controllo esercitato dalla piattaforma sulla filiera di commercializzazione. Ciò che le diversifica è lo specifico oggetto sul quale si esercita l'influenza della piattaforma nella realizzazione dello scambio con immediate conseguenze sulla tutela spettante al consumatore. Per il giudice dell'Ohio, il controllo deve, infatti, riguardare il singolo prodotto avviato al mercato⁸⁶. Elemento essenziale nell'imputabilità della piattaforma diviene pertanto la prestazione di servizi di logistica. Per la Corte californiana interessa invece verificare se alla piattaforma sia imputabile un grado di partecipazione al circuito distributivo sostanzialmente più significativo: l'attenzione si incentra di conseguenza sul tentativo dell'intermediario digitale di sovrintendere e di governare l'intera operazione commerciale che porta il bene fino al consumatore finale⁸⁷.

L'analisi del modello statunitense restituisce un ulteriore elemento di riflessione utile per lo studio che segue, consistente nella

crescente tendenza dei consumatori ad acquistare prodotti direttamente da produttori e fornitori stranieri che hanno avuto accesso al mercato attraverso le nuove catene globali di approvvigionamento. Le tre fattispecie esaminate riguardavano ipotesi in cui il prodotto fonte di pregiudizio era stato fabbricato in Cina e tutti gli attori del ciclo produttivo-distributivo, benché nominalmente identificabili, risultavano irraggiungibili o economicamente non in grado di risarcire il danno. Su questo dato che ci restituisce l'esame della casistica statunitense si dovrà dunque conclusivamente riflettere per verificare se l'obiettivo della Commissione di «garantire che esista sempre un'impresa con sede nell'UE che possa essere ritenuta responsabile per i prodotti difettosi acquistati direttamente da fabbricanti al di fuori dell'UE» possa o meno dirsi raggiunto.

5. Le funzioni principali della distribuzione: il servizio commerciale nell'apparato distributivo tradizionale

Al fine di ragionare sulle responsabilità attribuibili agli intermediari digitali per il danno da prodotto, può essere utile muovere dalle funzioni più significative svolte dall'apparato distributivo nei mercati tradizionali e esaminare le differenze che intercorrono rispetto ai mercati digitali. Nelle riflessioni successive si concentrerà, pertanto, l'attenzione sui compiti tipicamente demandati alla catena di distribuzione, per poi verificare se e come i nuovi canali di commercializzazione creati dalla digitalizzazione assolvano funzioni analoghe.

Il ruolo principale giocato dalla filiera distributiva è quello di interconnettere in maniera efficiente produzione e consumo⁸⁸ operando da raccordo spaziale e temporale tra i due versanti del mercato. Gli attori dell'apparato distributivo svolgono, infatti, il ruolo di collegamento tra due gruppi di agenti economici distanti fisicamente e/o temporalmente (fabbricanti e acquirenti), dando vita ad un servizio commerciale, consistente nelle attività

necessarie a mettere a disposizione dei consumatori i prodotti che essi desiderano secondo i tempi, i luoghi, le modalità e le quantità desiderate⁸⁹. Questa rappresentazione del servizio commerciale guarda alla distribuzione come ad un servizio essenzialmente logistico finalizzato a far pervenire il prodotto al consumatore. La distribuzione viene attuata da una catena di operatori economici indipendenti che adempiono a singole funzioni: trasporto, immagazzinamento, conservazione, controllo, detenzione di scorte significative, riduzione delle partite di merce a quantitativi al dettaglio, creazione dell'assortimento, esposizioni dettagliate, sforzi promozionali ed anche servizi di assistenza durante il ciclo di utilizzazione del prodotto⁹⁰. Nei mercati tradizionali il canale di distribuzione facilita l'avvicinamento di domanda ed offerta agendo anche su altri fronti: ad esempio, immettendo liquidità nel sistema⁹¹ ed assicurando la continuità e la regolarità degli approvvigionamenti⁹².

Inoltre, il momento distributivo assolve almeno ad altri due compiti fondamentali: la distribuzione, infatti, ha un naturale interesse a sostenere, all'interno del mercato, la fiducia e si propone l'obiettivo di ridurre le asimmetrie informative tra produttori e consumatori. Con riferimento al primo punto (sostenere la fiducia all'interno del mercato), l'intermediario - sia esso importatore, grossista o rivenditore finale -, ha interesse al pari se non maggiore del produttore⁹³ a curare la propria reputazione nei rapporti con l'industria, avendo la necessità di rendersi indipendente dai propri fornitori. Il produttore potrebbe, infatti, abbandonare il mercato: per non rischiare di scomparire a propria volta, gli agenti economici lungo la filiera di commercializzazione si adopereranno per reperire una vasta platea di fornitori e necessiteranno di una buona reputazione così da poter attrarre nel proprio circuito distributivo nuove imprese produttrici⁹⁴.

Allo stesso tempo, il godere di una buona reputazione anche nella percezione degli acquirenti è un fattore imprescindibile per

l'intermediario commerciale. Di norma, infatti, un venditore offre una gamma diversificata di prodotti, di guisa che i consumatori possono fare affidamento sulla fiducia che in esso ripongono, senza dover indagare di volta in volta circa la reputazione dei singoli beni avviati al mercato⁹⁵: la proficuità della sua impresa dipende, in ultima analisi, dal successo dell'intero assortimento⁹⁶. In questa logica, l'intermediario che vende un prodotto di bassa qualità non solo si assume il rischio della mancata vendita dell'intera scorta di quel particolare bene, ma va incontro ad un calo di reputazione, con il più grave rischio di perdere a cascata la fiducia dei consumatori relativamente all'intero assortimento merceologico⁹⁷: per evitare un appannamento della sua immagine, deve farsi carico del controllo di qualità dei beni che immette in circolazione, sviluppando le competenze specifiche per farlo⁹⁸. La filiera della distribuzione, incentivata dai potenziali ritorni economici, innesca un circolo virtuoso che - all'interno di un circuito di operazioni ripetute in cui ogni componente del canale distributivo risulta essere almeno in parte dipendente da tutti gli altri - sostiene la fiducia a vantaggio degli altri attori del mercato⁹⁹.

La funzione distributiva svolge, inoltre, un'importantissima funzione informativa¹⁰⁰, che si esplica nei confronti sia dei consumatori sia dei produttori. Relativamente al consumatore, la componente informativa può assumere, due dimensioni¹⁰¹: una dimensione esplicita ed una implicita.

La prima si concreta nelle informazioni espressamente fornite dal distributore al consumatore nel rapporto diretto con quest'ultimo - dimostrazioni accurate, consigli tecnici qualificati, elaborate spiegazioni¹⁰² - e risponde all'obiettivo di permettere all'acquirente di orientarsi consapevolmente sul mercato attraverso il giudizio fornito professionalmente da chi si è specializzato nel mettere in contatto offerta e domanda tra le diverse alternative che il mercato propone. L'informazione consentita, infatti, al consumatore di «risolvere problemi di valuta-

zione¹⁰³», specie con riferimento ai beni caratterizzati da complessità, da elevati tassi di innovazione o da parametri di natura tecnica non facilmente esaminabili dal singolo.

La seconda dimensione della componente informativa si sostanzia, invece, nella formazione degli assortimenti. Essa opera, dunque, in una fase antecedente al momento dell'acquisto e svolge - sia pur con modalità meno riconoscibili rispetto alle informazioni fornite all'atto della conclusione dell'affare - la medesima funzione di orientare le scelte del consumatore. Questa dimensione implicita della componente informativa consiste, più in particolare, nella valutazione professionale di quanto l'industria produce e nella consequenziale preselezione di ciò che, attraverso il singolo canale distributivo, può raggiungere il consumatore. In questa fase la distribuzione erige delle importanti barriere all'entrata, che ostacolano l'introduzione nel mercato di determinati prodotti. Gli intermediari della distribuzione attuano, cioè, una cernita qualitativa dei beni con la conseguenza di ridurre il rischio che il mercato sia invaso da prodotti insicuri o di bassa qualità.

La funzione informativa svolta dalla distribuzione commerciale si esplica anche nei confronti dell'industria. Relativamente al produttore, tale compito si sostanzia nelle cosiddette "informazioni di ritorno". Nell'agire da raccordo tra i due versanti del mercato, infatti, il distributore ha la possibilità di acquisire, produrre e accumulare informazioni relativamente alle preferenze degli acquirenti e di raccogliere informazioni economiche e statistiche per prevederne le scelte¹⁰⁴.

Da quest'angolo di visuale il servizio commerciale si atteggia a «centro di raccolta di informazioni sul consumatore»¹⁰⁵. Questo patrimonio di informazioni è particolarmente prezioso per l'impresa produttrice¹⁰⁶: sulla base dell'analisi del comportamento della domanda, l'industria avrà la possibilità di apportare gli adattamenti di volta in volta resisi necessari per assecondare aspettative, gusti e capacità di spesa dei consumatori¹⁰⁷.

Alcune tra le scelte più delicate in tema di produzione sono determinate, dunque, dalla struttura del processo distributivo e dalle informazioni di ritorno che essa restituisce¹⁰⁸: fornendo questo tipo di informazioni, la distribuzione commerciale accentua il suo ruolo di interfaccia tra produzione e consumo e finisce con il condizionare i comportamenti dell'industria, permettendo a quest'ultima di programmare, di riadattare, di orientare ed anche di ideare le nuove produzioni.

6. Funzioni della distribuzione e mercati digitali

Passate in rassegna le principali funzioni svolte dalla distribuzione nei mercati tradizionali, occorre verificare come esse siano adempiute dagli intermediari digitali. In particolare, bisogna appurare come i nuovi attori dell'economia di piattaforma sostengano la fiducia all'interno del mercato e come assolvano alla funzione informativa.

Con riferimento al primo punto, gli intermediari digitali si propongono di alleviare i problemi legati all'assenza di fiducia tipici degli acquisti a distanza: la mancanza di contatto diretto del consumatore con il prodotto (che impedisce quei tipici gesti - guardare, toccare, provare - che ne consentono la valutazione) potrebbe, infatti, non invogliare all'acquisto.

A tale scopo, nell'economia di piattaforma vengono forniti al consumatore strumenti di verifica preventiva della reputazione, in modo da stabilire la credibilità del singolo agente economico e contenerne i rischi di inadempimento. Le piattaforme offrono meccanismi di monitoraggio diffuso della soddisfazione dei clienti attraverso il coinvolgimento della comunità degli utenti-consumatori (per mezzo di sistemi di *rating* e *feedback*), arbitrano eventuali momenti di conflitto tra le parti della transazione, assicurano agevoli politiche di reso dei prodotti che non abbiano soddisfatto le aspettative degli acquirenti e forn-

scono garanzie aggiuntive rispetto a quelle previste dalla disciplina consumeristica.

La misura in cui questi strumenti sono destinati a funzionare efficacemente dipende dalle scelte effettuate a monte dagli intermediari digitali circa l'apertura del relativo mercato con riguardo sia all'offerta merceologica sia ai venditori terzi cui consentire l'accesso. A differenza di quanto accade nella distribuzione tradizionale, la tendenza delle piattaforme del commercio elettronico sembra essere quella di eliminare le barriere su entrambi questi fronti. Strategie commerciali così inclusive non sono certo casuali e sono determinate dal tentativo degli intermediari digitali di rendersi attraenti nei confronti di numeri sempre crescenti di acquirenti e di venditori: di sfruttare un particolare tipo di esternalità di rete molto comune nei mercati digitali (le c.d. "esternalità incrociate¹⁰⁹"). Per i singoli consumatori, infatti, il valore del servizio offerto dalla piattaforma aumenta al crescere della rete dei venditori.

Allo scopo di favorire la massima inclusività sul versante dell'offerta, le piattaforme non si limitano ad offrire ai venditori una "piazza virtuale" ed una "vetrina online"¹¹⁰. Esse forniscono anche servizi ancillari, inscindibilmente legati alla prestazione del servizio principale, come indicizzare, organizzare e promuovere i prodotti, sovrintendere agli ordini, riscuotere i pagamenti e gestire le comunicazioni con i consumatori. In aggiunta, alcune piattaforme propongono ai venditori anche la possibilità di fruire di servizi di logistica (trasporto, stoccaggio, imballaggio e spedizione delle merci), consentendo loro di azzerare la maggior parte dei problemi di magazzino e di abbattere i relativi costi. La prestazione integrata di questi servizi favorisce inevitabilmente l'ingresso nel mercato di venditori privi di una vera e propria organizzazione di impresa: chiunque, anche con investimenti minimi, ha la possibilità di affacciarsi sul mercato nella speranza di ritagliarsi facili occasioni di guadagno.

Anche con riferimento alla funzione informativa, gli intermediari digitali tentano di assolvere, secondo modalità per l'innanzi inedite, alle funzioni tipiche della filiera distributiva. A tale scopo, si servono di surrogati volti a sopperire alla mancanza di contatto diretto con il consumatore. Le informazioni, generalmente fornite in modo professionale dagli attori della filiera commerciale, sono adesso decentralizzate ed affidate, nella loro stessa produzione e diffusione, alla rete dei consumatori. Questi ultimi, incentivati da molteplici ragioni¹¹¹, riempiono delle loro recensioni le pagine relative alle singole unità di prodotto rinvenibili nei cataloghi delle piattaforme¹¹², consentendo ai futuri acquirenti di orientarsi attraverso la pubblicazione di informazioni (descrizioni, foto, video, recensioni) sulla qualità e sulle caratteristiche del prodotto¹¹³.

Da questa peculiare modalità di fronteggiare l'assenza di una delle funzioni qualificanti assolte dall'apparato distributivo scaturiscono, però, una serie di problemi riconducibili a due temi fondamentali: l'affidabilità e la genuinità di tali giudizi¹¹⁴.

Come rilevato in dottrina, i consumatori potrebbero non solo non avere le competenze per valutare la qualità e l'assenza di difetti nei prodotti, ma essere anche affetti da pregiudizi¹¹⁵: finanche i sistemi di valutazione meglio progettati non possono, pertanto, eliminare le asimmetrie informative tra le parti dello scambio. Inoltre, a dispetto di quanto inizialmente ipotizzato¹¹⁶, i giudizi dei consumatori non realizzano un controllo sociale "diffuso" e non condizionabile. Al contrario, una grossa fetta delle recensioni rinvenibili nelle piattaforme non è altro che il frutto di sollecitazioni, variamente incentivate dalla stessa industria e dagli altri operatori commerciali che prendono parte ai mercati digitali¹¹⁷. Gli strumenti volti a ridurre le asimmetrie informative incentrati sui *feedback* e sui giudizi dei consumatori possono, pertanto, essere abilmente sfruttati al fine di promuovere determinati prodotti (che difficilmente sarebbero

stati piazzati attraverso il circuito distributivo tradizionale) o di screditarne altri¹¹⁸: un fenomeno difficile da fronteggiare anche per gli stessi intermediari digitali¹¹⁹.

Conclusivamente, occorre considerare come anche il flusso informativo di ritorno nell'economia di piattaforma potrebbe non essere canalizzato dall'intermediario digitale nell'ambito di un circolo virtuoso e dare luogo a fenomeni di parassitismo commerciale: non solamente perché quest'ultimo potrebbe decidere di trattenere per sé i dati raccolti, ma anche perché le stesse informazioni potrebbero essere intercettate da terzi e rivendute a produttori e venditori non professionali che si ripromettono di sfruttare le rapide occasioni di guadagno consentite dal fatto di prendere parte - anche per brevissimi periodi - alle nuove catene di approvvigionamento globali¹²⁰.

7. Considerazioni critiche sul progetto di riforma

Dall'analisi del dato normativo effettuata nei paragrafi iniziali di questo studio si evince come, per quanto riguarda i nuovi attori della distribuzione, il progetto di riforma avanzato dalla Commissione europea si articola su più livelli. Secondo l'impostazione descritta, la disciplina del danno da prodotto non sarebbe più circoscritta alle sole figure della catena di approvvigionamento tradizionale (l'importatore e il fornitore), ma entrerebbero nella nuova regolamentazione figure quali il "rappresentante autorizzato", il "fornitore dei servizi di logistica" e il "fornitore di piattaforme online".

L'estensione della legittimazione passiva all'azione da prodotto a questi ultimi due operatori economici consentirebbe, secondo la Commissione, di far fronte nell'era digitale ai problemi posti dalla circolazione massiva di prodotti insicuri introdotti nel mercato unico attraverso l'apporto facilitatore delle piattaforme del commercio elettronico. D'altra parte, ai sensi del sesto comma dell'art. 7 della proposta, gli intermediari digi-

tali sono normativamente tenuti a rispondere del danno solo in via sussidiaria ed alla stessa stregua di un qualsivoglia fornitore dell'apparato distributivo tradizionale. L'unica responsabilità che graverebbe su tali soggetti sarebbe, dunque, quella riconnessa alle ipotesi del tutto marginali in cui il distributore non comunichi, entro un mese dalla richiesta, l'identità di colui che gli abbia fornito il prodotto.

Più in dettaglio, leggendo il solo sesto comma dell'art. 7 "i fornitori di piattaforme online" sembrerebbero chiamati a rispondere del danno cagionato dal prodotto difettoso in ipotesi ancora più residuali rispetto a quelle che attivano il circuito della responsabilità dei distributori tradizionali. Per essere equiparate ad un distributore e rispondere allo stesso titolo di tale operatore economico, gli attori digitali devono aver presentato «informazioni specifiche» o aver reso «altrimenti possibile l'operazione specifica in questione in modo tale da indurre un consumatore medio a ritenere che [...] il prodotto [...] oggetto dell'operazione» fosse fornito «dalla piattaforma stessa o da un destinatario del servizio che agisce sotto la sua autorità o il suo controllo»: le medesime condizioni che rendono inapplicabile l'esenzione (condizionata) da responsabilità prevista in via generale per i fornitori di servizi di *hosting* ai sensi del terzo comma dell'art. 6 del regolamento sui servizi digitali¹²¹.

La reale portata innovativa della riforma assume un significato parzialmente diverso ove si prenda in considerazione un altro operatore economico assente nella normativa del 1985, il "fornitore dei servizi di logistica". Se, infatti, il secondo comma dell'art. 7 rende responsabili importatori e rappresentanti autorizzati per l'ipotesi di beni difettosi prodotti al di fuori del mercato unico, il terzo comma della medesima norma prevede che, nell'evenienza in cui anche questi ultimi non abbiano sede nell'Unione, a rispondere del danno arrecato al consumatore sarà chiamato il "fornitore dei servizi di logistica".

La definizione di “fornitore dei servizi di logistica” - ossia qualsiasi persona fisica o giuridica che offre, nel corso dell’attività commerciale, almeno due dei seguenti servizi: «immagazzinamento, imballaggio, indirizzamento e spedizione¹²²» - è tale da includere anche quegli attori del commercio elettronico che, non limitandosi a mettere in contatto i due versanti del mercato, offrono servizi aggiuntivi relativi all’effettivo raccordo spaziale e temporale tra venditori e acquirenti. Nella definizione elaborata dalla Commissione la figura del “fornitore dei servizi di logistica” è, infatti, costruita intorno ai servizi ulteriori (a contenuto materiale) talora prestati dagli intermediari del commercio elettronico. Un ulteriore dato di rilievo è che la responsabilità di tale soggetto è espressamente sganciata dalla titolarità del prodotto fonte di pregiudizio, non rilevando, ai fini delle connesse responsabilità, il fatto di essere «proprietar[i] dei prodotti interessati».

Dal combinato disposto del terzo e del sesto comma dell’art. 7 della proposta di direttiva discende, pertanto, un circuito di attivazione della responsabilità per danno da prodotto delle piattaforme del commercio elettronico atto a coprire molte delle ipotesi considerate nello studio per fattispecie prima compiuto con riferimento al modello statunitense.

Allo stesso tempo, le differenze con il modello nordamericano restano significative. A differenza di quanto avviene negli Stati Uniti, nel progetto di riforma della Commissione l’attenzione rimane ancora una volta polarizzata sul produttore, e non anche sul sistema distributivo, chiamato ad assumere anacronisticamente una posizione ancillare nei rapporti con l’industria. Solamente nell’ipotesi prevista dal terzo comma dell’art. 7 la responsabilità è assimilabile a quella del fabbricante del prodotto difettoso, ed il fornitore dei servizi di logistica è chiamato a rispondere alla stessa stregua del produttore e in via primaria e solidale con quest’ultimo soggetto.

Di minore intensità è, invece, la responsabilità espressamente prevista per “i fornitori di piattaforme online” che, pur non espletando servizi di logistica - e non rientrando, pertanto, nel novero degli operatori responsabili ai sensi del terzo comma dell’art. 7 -, abbiano comunque indotto i consumatori all’acquisto. Si è visto che in tali ipotesi la responsabilità - coperta dal sesto comma dell’art. 7 - è solo sussidiaria ed è subordinata alla circostanza che l’operatore digitale non comunichi entro un mese dalla relativa richiesta del danneggiato l’identità dell’operatore economico subito a monte nella catena distributiva. Non trovano, pertanto, copertura quelle evenienze - poste in luce dalla casistica statunitense su cui prima si è appuntata la riflessione¹²³ - che si pongono nelle ipotesi in cui l’anello della catena distributiva cui la piattaforma abbia dato accesso al mercato, benché identificabile, non compaia in giudizio o non sia solvibile¹²⁴.

Inoltre, l’imputabilità del fornitore di piattaforme online è ricollegata non tanto ad un generale potere di controllo esercitato sullo scambio, quanto a due ipotesi ben circostanziate: l’aver presentato «informazioni specifiche» o l’aver reso «altrimenti possibile l’operazione specifica in questione in modo tale da indurre un consumatore medio a ritenere che [...] il prodotto [...] oggetto dell’operazione» fosse fornito «dalla piattaforma stessa o da un destinatario del servizio che agisce sotto la sua autorità o il suo controllo¹²⁵». La prima ipotesi costituisce un’evenienza tutto sommato residuale posto che tra le piattaforme del commercio elettronico aperte all’apporto di venditori terzi, sono quasi sempre venditori e consumatori a fornire le informazioni necessarie allo scambio. Quanto alla seconda ipotesi, sembra potersi sostenere che essa sia di limitato ausilio per il danneggiato: la proposta di direttiva è, infatti, ancorata alla verifica del fatto che l’intermediario abbia fornito al consumatore medio l’impressione che il prodotto «specifico» fosse fornito dalla piattaforma stessa o da un agente del mercato da questa

controllato¹²⁶. Non hanno trovato, dunque, espressa contemplazione, le modalità concrete - ben comprese dalla giurisprudenza californiana su cui si è incentrata la riflessione nelle pagine precedenti di questo studio¹²⁷ - attraverso cui gli intermediari digitali “catturando” una enorme platea di consumatori e persuadendoli all’acquisto¹²⁸ (al di là del *concreto* affidamento ingenerato su un soggetto *determinato* con riferimento ad un’operazione *specificata*) finiscono con l’alimentare il rischio di una circolazione incontrollata di beni insicuri¹²⁹.

Del resto si è rilevato che i concreti affidamenti di soggetti determinati non hanno «alcuna ragione d’essere nella logica della responsabilità extracontrattuale¹³⁰». Tanto ciò è vero che il regime del danno da prodotto «non solo consente di ritenere responsabile il produttore pur quando egli non abbia venduto il bene all’utente finale, ma altresì legittima ad agire per il risarcimento tutti coloro che siano stati danneggiati dal prodotto difettoso¹³¹»; consumatori e non.

8. Osservazioni conclusive

Possiamo concludere che l’emergere di nuovi attori del mercato e la profonda ridefinizione della filiera di produzione e commercializzazione dei beni, siano state le ragioni principali a sostegno di un intervento legislativo di ampio respiro, che stabilisca un regime di responsabilità delle piattaforme del commercio elettronico.

Sembra questa la direzione imboccata dalla Commissione europea con la proposta di direttiva sulla responsabilità da prodotti esitata il 28 settembre 2022. L’espressa contemplazione, tra i legittimati passivi all’azione per danno da prodotto, dei “fornitori di piattaforme online” si accompagna, infatti, ad altre ipotesi di coinvolgimento in via principale di nuovi attori del mercato (inclusi anche quelli digitali) allorché ricorra la du-

plíce circostanza che essi offrano almeno due tra i servizi di logistica normativamente contemplati - immagazzinamento, imballaggio, indirizzamento e spedizione - e che importatori e rappresentanti autorizzati non abbiano sede dell'Unione.

D'altra parte, l'estensione operata dalla Commissione europea si muove prevalentemente nell'orbita di una sola delle funzioni tradizionalmente svolte dall'impresa che produce il servizio commerciale: il fungere da raccordo, temporale e spaziale, tra industria e consumatori. Solo nel caso della prestazione dei servizi di logistica, infatti, la responsabilità delle piattaforme digitali si aggiunge in ogni caso a quella del produttore che abbia sede all'estero. Mentre la Commissione non sembra aver prestato adeguata attenzione alle altre funzioni assolte nel momento distributivo dalle piattaforme del commercio elettronico - ridurre le asimmetrie informative tra le parti dello scambio e il sostenere la fiducia all'interno del mercato - allorché si è trattato di decidere sia relativamente al titolo della loro responsabilità sia alle modalità del loro coinvolgimento. Con riguardo al titolo della responsabilità, infatti, i fornitori di piattaforme online sono chiamati a rispondere del danno solo in via sussidiaria, quando l'anello precedente della catena produttiva-distributiva non sia identificabile. La loro responsabilità è accostata, dunque, alle responsabilità non di chi concorre alla immissione del prodotto dannoso nel mercato unico - importatori e rappresentanti autorizzati - ma a quella di chi ne agevola l'ulteriore circolazione, ossia il distributore.

Con riguardo alle condizioni di attivazione del circuito della responsabilità, calibrate sui compiti assolti nell'espletare il servizio distributivo, la proposta si è fermata a considerare ipotesi marginali.

Relativamente alla funzione informativa, infatti, l'evenienza contemplata dal progetto di riforma riguarda esclusivamente il caso in cui l'intermediario digitale fornisca "informazioni spe-

cifiche”. Non è stata presa in esame, invece, l’ipotesi più tipica che contraddistingue il servizio commerciale nell’economia di piattaforma: vale a dire, il caso in cui le informazioni siano prestate indirettamente ed in maniera a-professionale dall’operatore digitale tramite l’apporto dei propri utenti-consumatori.

Relativamente alla creazione di un sistema di fiducia nel mercato, la proposta di direttiva è, invece, ancorata alla verifica del fatto che l’intermediario abbia fornito al consumatore medio l’impressione che il prodotto *specifico* fosse fornito dalla piattaforma stessa o da un agente del mercato da questa controllato.

Una più attenta valutazione della logica della responsabilità extracontrattuale e, al tempo stesso, delle funzioni complessivamente assolte dalla distribuzione, avrebbero forse dovuto indirizzare la Commissione a riferirsi non tanto allo specifico e concreto affidamento riposto da un consumatore determinato sulla sicurezza del singolo acquisto («l’operazione specifica in questione», secondo la formulazione letterale della norma richiamata dall’ultimo comma dell’art. 7 della proposta di direttiva), quanto all’aumento del rischio ricollegabile al complessivo clima di fiducia che alcune piattaforme riescono a costruire a proprio vantaggio pur non adempiendo al compito - svolto invece dal servizio commerciale tradizionale - di ostacolare l’introduzione nel mercato di prodotti insicuri o di bassa qualità¹³². Il forte disallineamento in termini di sicurezza tra acquisti *online* e *offline* è ricollegabile anche alla circostanza che la “disintermediazione” operata dalle piattaforme digitali ha ridotto i passaggi che separano il produttore dall’acquirente, facilitando - in assenza di controlli - l’arrivo massivo di prodotti esteri sul mercato europeo. Nel tentativo di rendersi attraenti nei confronti di una rete di acquirenti e venditori sempre più ampia, gli intermediari digitali hanno spesso eliminato quelle barriere all’ingresso che la filiera tradizionale garantiva¹³³.

L'imputabilità della piattaforma avrebbe potuto trovare dunque la sua giustificazione non nel concreto affidamento rimasto deluso, ma nell'aumento del rischio che beni insicuri siano introdotti nel mercato. Tali ragioni avrebbero forse potuto indurre ad una maggiore latitudine della responsabilità degli attori digitali della distribuzione rispetto a quella racchiusa nel progetto di riforma della direttiva 85/374/CEE.

Note di chiusura

¹ L'articolo è stato pubblicato su "Danno e responsabilità", 1/2023, 8 ss. Sono riferibili a Rosario Petruso i paragrafi 3, 4.2, 4.4, 5, 6, 7. Sono riferibili a Guido Smorto i paragrafi 1, 2, 4, 4.1, 4.3, 8.

² Proposta di Direttiva del Parlamento europeo e del Consiglio sulla responsabilità per danno da prodotti difettosi, COM/2022/495 final del 28 settembre 2022.

³ Così il considerando n. 5 della proposta. Ai sensi dell'art. 17 della proposta, la direttiva 85/374/CEE risulterebbe abrogata e continuerebbe ad applicarsi esclusivamente in relazione ai prodotti immessi sul mercato prima della data di entrata in vigore della nuova disciplina.

⁴ Direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi.

⁵ Così l'Impact Assessment Report (Commission staff working document) che accompagna la proposta di direttiva, SWD(2022) 316 final, 28.9.2022, specialmente, 11.

⁶ Ex articolo 95 del Trattato che istituisce la Comunità europea, ex articolo 100 del Trattato che istituisce la Comunità economica europea. L'articolo 114 è subito richiamato nel testo della proposta di direttiva, ancor prima dei considerando.

⁷ Il primo comma dell'art. 114 TFUE così dispone: «Salvo che i trattati non dispongano diversamente, si applicano le disposizioni seguenti per la realizzazione degli obiettivi dell'articolo 26. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria e previa consultazione del Comitato economico e sociale, adottano le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno».

⁸ Cfr. la relazione di accompagnamento della proposta di direttiva, COM/2022/495 final del 28 settembre 2022, specialmente, 10.

⁹ Cfr. il Regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti; cfr. anche la decisione n. 768/2008/CE del Parlamento europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti.

¹⁰ Regolamento (Ue) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

¹¹ Proposta di direttiva del Parlamento europeo e del Consiglio, relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale), COM/2022/496 final del 28 settembre 2022.

¹² Proposta di regolamento del parlamento europeo e del consiglio sui prodotti macchina, COM/2021/202, final, del 21 aprile 2021.

¹³ Proposta di regolamento del Parlamento europeo e del Consiglio, relativo alla sicurezza generale dei prodotti, che modifica il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 87/357/CEE del Consiglio e la direttiva 2001/95/CE del Parlamento europeo e del Consiglio, COM(2021) 346 final del 30 giugno 2021.

¹⁴ Come si evince dai considerando n. 8 e n. 9 e dall'art. 3.

¹⁵ In particolare, l'art. 3, rubricato "Livello di armonizzazione" prevede testualmente: «Salvo altrimenti disposto dalla presente direttiva, gli Stati membri non mantengono o adottano nel loro diritto nazionale disposizioni divergenti da quelle stabilite dalla presente direttiva, incluse disposizioni più o meno rigorose per garantire al consumatore un livello di tutela diverso». Si noti che - almeno sino alle tre sentenze della Corte europea di giustizia rese il 25 aprile 2002 nei casi C-154/00, C-52/00 e C-183/00 - era condivisa in letteratura l'idea che l'obiettivo primario dell'intervento normativo europeo fosse quello della protezione della salute e dalla sicurezza dei consumatori (sul punto, cfr. ad esempio, F. CAFAGGI, *La responsabilità dell'impresa per prodotti difettosi*, in *Diritto privato europeo*, a cura di N. Lipari, Padova, 1997, II, 1002 s.) e che fosse, dunque, possibile per i legislatori nazionali (in omaggio a questa vocazione pro-consumeristica) prevedere, nelle rispettive normative di recepimento, una disciplina di maggiore favore per il danneggiato. In quelle pronunce, invece, la Corte di giustizia ha valorizzato la circostanza che la base giuridica dell'atto fosse l'art. 95 del Trattato che istituisce la Comunità europea. La direttiva 85/374/CEE è stata presentata, pertanto, come una misura di mercato interno, che si prefigge di instaurare un equilibrio tra la tutela dei consumatori e le responsabilità dei produttori, eliminando le distorsioni della concorrenza dovute alla esistenza di diversi regimi in materia di responsabilità e agevolando la libera circolazione dei beni. Per una critica delle sentenze del 25 aprile 2002, cfr. G. PONZANELLI, *Difetti del prodotto e del diritto privato europeo*, in *Il Foro. It.*, I, 295 ss.

¹⁶ Cfr. considerando n. 16 e 18.

¹⁷ Secondo un rilevamento del 2022, promosso e pubblicato dal sito Jungle-scout, due tra le piattaforme di e-commerce più adoperate dai consumatori nel mercato statunitense - *Amazon* e *Walmart* - sono in gran parte affollate da venditori terzi: il mercato di *Amazon* è composto per l'82% da venditori indi-

pendenti; i venditori indipendenti sulla piattaforma di *Walmart* si fermano invece al 79%. I risultati di questo studio sono pubblicati anche su *Retailcustomerexperience.com* in un articolo del 27 ottobre 2022 dal titolo “*Amazon beating Walmart online on several fronts*”.

¹⁸ Così vengono denominati i nuovi canali distributivi al terzo considerando della proposta di direttiva.

¹⁹ Tale intendimento si ricava dal proposito, più volte messo in luce nella relazione di accompagnamento alla direttiva, che «esista sempre un soggetto con sede nell’UE responsabile per i prodotti difettosi acquistati da produttori» stabiliti fuori dal mercato unico: cfr. la relazione di accompagnamento, cit., specialmente 2, 9 e 14.

²⁰ Giova dire che - ai sensi dell’art. 4 della proposta - si intende: per “immissione sul mercato”, la prima messa a disposizione di un prodotto sul mercato dell’Unione; per “messa a disposizione sul mercato”, la fornitura di un prodotto per la distribuzione, il consumo o l’uso sul mercato dell’Unione nel corso di un’attività commerciale, a titolo oneroso o gratuito; per “messa in servizio”, il primo utilizzo di un prodotto nell’Unione nel corso di un’attività commerciale, a titolo oneroso o gratuito, nei casi in cui il prodotto non è stato immesso sul mercato anteriormente al suo primo utilizzo.

²¹ Definito dall’art. 4 comma 1 n. 12 come quella «persona fisica o giuridica stabilita nell’Unione che ha ricevuto da un fabbricante un mandato scritto che la autorizza ad agire per suo conto in relazione a determinati compiti».

²² Definito dall’art. 4 comma 1 n. 13 come quella «persona fisica o giuridica stabilita nell’Unione che immette sul mercato dell’Unione un prodotto originario di un paese terzo».

²³ Sono espressamente esclusi i fornitori di alcuni servizi: i fornitori di «servizi postali definiti all’articolo 2, punto 1, della direttiva 97/67/CE»; i fornitori di «servizi di consegna dei pacchi come definiti all’articolo 2, punto 2, del regolamento (UE) 2018/644»; i fornitori di «qualsiasi altro servizio postale o di trasporto merci».

²⁴ Norma che disciplina una di quelle evenienze in cui non si applicherebbe l’esenzione (condizionata) da responsabilità prevista in via generale per i fornitori di servizi di *hosting* dal regolamento (Ue) 2022/2065.

²⁵ Così A. GENOVESE, voce “*Responsabilità del produttore*”, in *Dig. disc. priv.*, sez. civ., Torino, 2013, 607; M. COGNOLATO, *Azione contrattuale ed extracontrattuale per il risarcimento del danno da prodotto difettoso nelle “vendite a catena”*, in *Nuova giur. civ.*, 2003, 350.

²⁶ Cfr., in particolare, l’allegato I alla decisione n. 768/2008/CE cit., art. R1 comma 1, n. 4 e art. R3.

²⁷ Cfr. i considerando nn. 13 e 18 e l'art. 4 del regolamento (Ue) 2019/1020, cit.

²⁸ Cfr. la lett. h) dell'art. 3 del regolamento (UE) 2022/2065, cit., ove la «piattaforma online» è definita come quel fornitore di servizi «di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità del presente regolamento».

²⁹ F. GALGANO, *Grande distribuzione e responsabilità per prodotti difettosi*, in *Contratto e impresa*, 1992, 7 ss. Più in generale, sul fatto che i rapporti di forza tra industria e distribuzione non debbano inequivocabilmente essere pensati a favore della prima, cfr. L. PELLEGRINI, *Le trasformazioni in corso nella distribuzione: implicazioni settoriali e intersettoriali*, in AA. VV., *I contratti della distribuzione commerciale*, Milano, 1993, 146. L'impostazione della direttiva è stata confermata dalla giurisprudenza della Corte europea di giustizia: cfr. *Skov Æg c. Bilka Lavprisvarehus A/S*, 10 gennaio 2006, C-402/03. Si legge infatti nella pronuncia (cfr. p. 29) che «dopo aver ponderato i ruoli rispettivi dei vari operatori economici che intervengono nelle catene di fabbricazione e di commercializzazione è stata operata la scelta di imputare in linea di principio al produttore, e unicamente in taluni casi delimitati all'importatore e al fornitore, l'onere della responsabilità per i danni causati dai prodotti difettosi nel regime giuridico istituito dalla direttiva». Più in particolare, con riferimento alla responsabilità sussidiaria dei fornitori, si osserva (cfr. p. 28) a che «pur riconoscendosi che la possibilità di far sorgere la responsabilità del fornitore di un prodotto difettoso secondo le modalità previste dalla direttiva faciliterebbe le azioni giudiziarie intentate dal danneggiato, viene osservato che tale facilitazione sarebbe pagata a caro prezzo in quanto, obbligando tutti i fornitori ad assicurarsi contro tale responsabilità, essa condurrebbe ad un notevole rincaro dei prodotti. Inoltre, tale facilitazione condurrebbe ad una moltiplicazione dei ricorsi, dato che il fornitore si rivolgerebbe a sua volta contro il proprio fornitore risalendo sino al produttore. Dato che, nella grande maggioranza dei casi, il fornitore si limita a rivendere il prodotto così come acquistato e che solo il produttore ha la possibilità di agire sulla qualità di quest'ultimo, si ritiene opportuno concentrare la responsabilità per danno dei prodotti difettosi sul produttore».

³⁰ Sul diverso trattamento giuridico riservato alla produzione e alla distribuzione nell'ambito della direttiva 85/374/CEE, cfr. G. COMANDÈ, *Product liability in Italy*, in *European Product liability, An Analysis of the State of Art in the Era of New Technologies*, Pitř Machnikowski (ed), 2016, 292.

³¹ Principio che ha trovato conferma nella decisione n. 768/2008/CE, cit. Nell'ambito dei principi generali enucleati dall'art. 1 si legge, infatti, al comma 2 che «All'atto dell'immissione di prodotti sul mercato comunitario, gli operatori economici, in funzione dei loro rispettivi ruoli nella catena di fornitura, sono responsabili della conformità dei loro prodotti a tutta la normativa applicabile».

³² Maggiori responsabilità che si riscontrano anche in relazione agli obblighi gravanti sugli importatori sulla base della disciplina sulla conformità dei prodotti: cfr. l'allegato I alla decisione n. 768/2008/CE, cit., il cui articolo R4 prevede al comma 6 che «Ove ritenuto opportuno alla luce dei rischi presentati da un prodotto, gli importatori, per proteggere la salute e la sicurezza dei consumatori, eseguono prove a campione dei prodotti commercializzati, esaminano i reclami e, se del caso, mantengono un registro dei reclami, dei prodotti non conformi e dei richiami di prodotti e informano i distributori di tale monitoraggio». Di contro, sui distributori non grava alcun obbligo di eseguire prove a campione dei prodotti commercializzati.

³³ Cfr. U. CARNEVALI, *Prodotto composto difettoso e regresso tra produttori responsabili. Il criterio delle «dimensioni del rischio»*, in *Resp. civ. prev.*, 2015, 360; più in generale, M. FRANZONI, *Fatti illeciti*, Bologna, 2020, 548. Come notato in dottrina (cfr. G. STELLA, *La responsabilità del produttore per danno da prodotto difettoso nel nuovo codice del consumo*, in *Resp. civ. e prev.*, 2006, 1589), infatti, il danneggiato conserva sempre il diritto di rivolgersi al produttore nelle ipotesi in cui l'azione nei confronti dell'importatore si riveli impossibile, perché, ad esempio, questi all'epoca dell'azione è fallito. V. anche S. DELLA BELLA, *La responsabilità dell'importatore di fuochi d'artificio*, in *Resp. civ. e prev.*, 2006, 136.

³⁴ Come si evince dal considerando n. 27 della proposta di direttiva, tali attori - che non corrispondono esattamente alla definizione del soggetto preposto, nel diritto dell'Unione, alla immissione di un prodotto sul mercato unico - svolgono molte delle stesse funzioni assolte dagli importatori.

³⁵ Cfr. *Greenman v. Yuba Power Prods., Inc.*, 377 P.2d 897, 900 (Cal. 1963).

³⁶ Occorre sottolineare che Oltreoceano la responsabilità da danno da prodotto non è oggetto di disciplina federale e la regolamentazione della materia è affidata all'iniziativa dei singoli Stati dell'Unione, i quali hanno fissato una normativa statutaria o, altre volte, hanno lasciato la materia all'evoluzione del *common law*. Nell'uno e nell'altro caso, non constano ad oggi all'interno dei singoli Stati dell'Unione iniziative legislative volte ad adeguare la disciplina - statutaria o di *common law* - sulla responsabilità da prodotto alle inedite condizioni di mercato. Due progetti di legge californiani - cfr. Assem. Bill. 3262, 2019-2020 Reg. Sess. (Cal. 2020) e Assem. Bill. 1182, 2021-2022 Reg. Sess. (Cal. 2021) - sono stati, infatti, abbandonati sul nascere dopo che il *common law* si è

fatto carico di questa ulteriore estensione dei confini della responsabilità da prodotto: ci si riferisce in particolare alla sentenza *Bolger v. Amazon.com* 53 Cal. App.5th 431 (2020).

Per una panoramica di sintesi delle posizioni adottate dai Singoli Stati in materia di danno da prodotto, cfr. E. J. JANGER - A. D. TWERSKI, *The Heavy Hand of Amazon: A Seller Not a Neutral Platform*, in 14 *Brook. J. Corp. Fin. & Com. L.*, 2020, 259, nonché S. M. BENDER, *Product Liability's Amazon Problem*, in 4 *J.L. & Tech. Tex.*, 2021, 109 ss.

³⁷ Cfr. Restatement (Second) of Torts § 402A (1965), ove la legittimazione passiva all'azione da prodotto difettoso è estesa a «any person engaged in the business of selling products for use or consumption». In giurisprudenza v. *Vandermark v. Ford Motor Co.*, 391 P.2d 168 (Cal. 1964) e, più di recente, *Brooks v. Beech Aircraft Corp.*, 1995- NMSC 043, 120 N.M. 372, 376, 902 P.2d 54 (1995). In dottrina, cfr., invece, W. L. PROSSER, *The Assault Upon the Citadel (Strict Liability to the Consumer)*, in 69 *Yale L.J.*, 1099, 1122-1123 (1960). Sul punto, cfr. anche CAVICO JR., *The Strict Tort Liability of Retailers, Wholesalers, and Distributors of Defective Products*, in 12 *Nova L.Rev.*, 213, 221-222 (1987); M. S. SHAPO, *Millennial Torts*, in 33 *Ga. L. Rev.* 1999, 1021, spec. 1026; C. M. SHARKEY, *Holding Amazon liable as a seller of defective goods: a convergence of cultural and economic perspectives*, in 115 *Nw. L. Rev.*, 339 (2020).

³⁸ *Fox v. Amazon.com, Inc.*, 930 F.3d 415 (6th Cir. 2019).

³⁹ *Oberdorf v. Amazon.com, Inc.*, 936 F.3d 136 (3rd Cir. 2019).

⁴⁰ *Bolger v. Amazon.com, Inc.*, 53 Cal.App.5th 431 (Cal. Ct. App. 2020).

⁴¹ *Stiner v. Amazon.com*, 164 N.E.3d 394 (Ohio 2020).

⁴² Per un primo approccio a questa giurisprudenza, cfr. Z. GILLIES, *Amazon Marketplace and Third-Party Sellers: The Battle over Strict Product Liability*, in 54 *Suffolk U. L. Rev.* 87 (2021), specialmente 89 e ss. nonché A. DOYER, *Who Sells? Testing Amazon.com for Product Defect Liability in Pennsylvania and beyond*, in 28 *J.L. & Pol'y*, 719 (2020).

⁴³ Come si legge in *Loomis v. Amazon.com LLC* (63 Cal. App. 5th 466), 471 «Amazon describes its marketplace as “an online mall” which provides an “online storefront” to third party sellers»; analogamente, in *Gartner v. Amazon.com, Inc.*, 433 F. Supp. 3d 1034, 1042 (S.D. Tex. 2020) si legge: «[Amazon] contends that its marketplace is much like an auctioneer as they play only an incidental role in a product's placement in the stream of commerce».

⁴⁴ Letteralmente, «a business model that is not title dependent»: cfr. *Amazon.com, Inc. v. McMillan*, 625 S.W.3d 101, 112.

⁴⁵ Cfr. *Eberhart v. Amazon.com, Inc.*, 325 F. Supp. 3d 393 (S.D.N.Y. 2018), 398, ove si legge «regardless of what attributes are necessary to place an entity

within the chain of distribution, the failure to take title to a product places that entity on the outside»; *Erie Ins. Co. v. Amazon.com, Inc.*, 925 F.3d 135, 141 (4th Cir. 2019), ove lo stesso concetto è espresso nei termini che seguono: «Insofar as liability in Maryland for defective products falls on “sellers” and manufacturers (who are also sellers), it is imposed on owners of personal property who transfer title to purchasers of that property for a price»; *Philadelphia Indem. Ins. Co. v. Amazon.com, Inc.*, 425 F. Supp. 3d 158 (E.D.N.Y. 2019); Cfr. anche *Wallace v. Tri-State Assembly, LLC*, 201 A.D.3d 65, 68 (App. Div. 1st Dept. 2021); *State Farm Fire & Cas. Co. v. Amazon.com, Inc.*, 835 F. App'x 213, 216 (9th Cir. 2020).

⁴⁶ In *Allstate N.J. Ins. Co. v. Amazon.com, Inc.*, No. Civil Action No. 17-2738 (FLW) (LHG), 2018 WL 3546197, 34 si legge che, nel determinare se un soggetto possa essere chiamato a rispondere del danno da prodotto, «control over the product is the touchstone». Considerazioni analoghe sono alla base delle decisioni rese nei casi *Fox v. Amazon.com, Inc.*, 930 F.3d 415, 424-425 (6th Cir. 2019) e *Carpenter v. Amazon.com, Inc.*, N.D. Cal. No. 17-cv-03221, 2019 U.S. Dist. (19 marzo 2019) e da ultimo nel caso *Stiner v. Amazon.com*, 164 N.E.3d 394, 400.

⁴⁷ *Stiner v. Amazon.com*, cit., 394.

⁴⁸ Cfr. *Allstate N.J. Ins. Co. v. Amazon.com, Inc.*, No. Civil Action No. 17-2738 (FLW) (LHG), 2018 WL 3546197, 34; *Stiner v. Amazon.com, Inc.*, 398, da cui si apprende testualmente «While these factors may demonstrate the degree of control that Amazon seeks to exert in its relationship with sellers, they do not establish that Amazon exercised control over the product itself sufficient to make it a ‘supplier’ under the Act».

⁴⁹ Cfr. *Bolger v. Amazon.com, Inc.*, cit., ove Amazon è descritta come «an integral part of the overall producing and marketing enterprise that should bear the cost of injuries resulting from defective products»; v. anche *Oberdorf v. Amazon.com Inc.*, 930 F.3d 136, specialmente 146, ove si legge che «Although Amazon does not have direct influence over the design and manufacture of third-party products, Amazon exerts substantial control over third-party vendors».

⁵⁰ *Stiner v. Amazon.com*, 164 N.E.3d 394.

⁵¹ *Loomis v. Amazon.com LLC*, 63 Cal. App. 5th 466.

⁵² *Amazon.com, Inc. v. McMillan*, 625 S.W.3d 101.

⁵³ Cfr. *McMillan v. Amazon.com, Inc.*, United States Court of Appeals for the Fifth Circuit, 983 F.3d 194, 196 (5th Cir. 2020).

⁵⁴ Questo il testo del quesito interpretativo sottoposto alla Corte statale dal giudice federale: «May Amazon be held liable as a “seller” under Texas products-liability law for third-party products sold on Amazon’s website and handled through Amazon’s Fulfillment by Amazon program?».

⁵⁵ Cfr. § 82.001 e § 82.003 Tex. Civ. Prac. & Rem. Code. Tex. Civ. Prac. & Rem. Code.

⁵⁶ Cfr. la sezione 82 001 (3) ove il “seller” è definito come «a person who is engaged in the business of distributing or otherwise placing, for any commercial purpose, in the stream of commerce for use or consumption a product or any component part thereof».

⁵⁷ Si legge in sentenza (cfr. p. 109) che «our cases show that both sales and non-sale commercial transactions, at a minimum, involve sellers that hold or relinquish title in a product’s distribution chain».

⁵⁸ Letteralmente, nella pronuncia, «a business model that is not title dependent»: cfr. *McMillan v. Amazon.com*, 112, ove si legge anche che «Because McMillan obtained the remote through a transfer of title for a price, and Amazon did not hold or relinquish title at any point in the remote’s distribution chain, Amazon was not “engaged in the business of distributing or otherwise placing” the remote into the stream of commerce. On this record, therefore, Amazon is not a chapter 82 seller under Texas law».

⁵⁹ *Stiner v. Amazon.com*, cit.

⁶⁰ *Ohio Products Liability Act*, R.C. 2307.71.

⁶¹ *Ohio Products Liability Act*, cit., R.C. 2307.78(B).

⁶² Non a caso questa seconda parte della norma è definita in sentenza come una “catchall provision”.

⁶³ *Stiner v. Amazon.com*, cit. specialmente 398 e 399, ove si legge testualmente «But those persons do not become “suppliers” in the absence of control over the product, exhibited by actions such as the selection, possession, maintenance, and operation of the product».

⁶⁴ *Stiner v. Amazon.com*, cit., specialmente 399, ove si legge «According to Stiner, Amazon prevents sellers from contacting customers; retains sole discretion to determine the content, appearance, and design of its website; reserves the right to alter the content of product descriptions; and imposes restrictions on pricing».

⁶⁵ Solo nell’opinione concorrente del giudice Donnelly (cfr. *Stiner v. Amazon.com*, cit., 402) si mette in risalto sia l’obsolescenza di una legge costruita intorno ad una figura professionale (quella del fornitore che prestava servizi di distribuzione negli anni ’80 del secolo scorso) sia il paradosso cui essa dà luogo, consistente nel fatto che «la legge si applica anche a chi apponga un solo adesivo sul prodotto, ma non a chi controlla ogni singolo aspetto dell’immissione del prodotto nel flusso del commercio».

⁶⁶ *Loomis v. Amazon.com LLC*, cit.

⁶⁷ Il punto relativo alla derivazione giurisprudenziale del nostro istituto non è da sottovalutare, soprattutto nella regolamentazione dei mercati digita-

li dove è alto il rischio che l'intervento legislativo sia frutto della "cattura" del regolatore da parte delle pressioni e dell'influenza di gruppi ristretti, portatori di interessi specifici. Infatti, come notato da G. PRIEST, *La controrivoluzione nel diritto della responsabilità da prodotti negli Stati Uniti d'America*, in *Foro it.*, 1999, IV, 119 ss. negli Usa i «provvedimenti legislativi sembrano sempre particolarmente sospetti in quanto possono nascere sotto l'influenza di particolari interessi politici». Nei mercati digitali, il processo legislativo può essere oggetto di attività di *lobbying* da parte dei soggetti da regolare. Ed a soffrire le conseguenze negative di una normazione che non promuova l'interesse generale sono i consumatori. Per una prima panoramica sulle forme di condizionamento dei legislatori da parte di chi nel mercato (tradizionale o digitale) rivesta posizioni consolidate o dominanti, sia consentito rinviare a A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Milano, 2020, 75 ss. e 230 ss.

⁶⁸ In tale ottica è stata affermata la responsabilità di chi, produttore della materia prima (non difettosa) necessaria per realizzare tubature idrauliche, aveva agevolato in maniera capillare la penetrazione del prodotto finito nel mercato, assistendo i relativi produttori ad elaborare strategie di marketing, presentando informazioni a enti governativi, contattando associazioni di costruttori edili, organizzando seminari di formazione per ispettori idraulici (cfr. *Bay Summit Community Assn. v. Shell Oil Co.*, (1996) 51 Cal. App. 4th 762); ma anche di chi aveva autorizzato il produttore di munizioni per fucili da caccia, dietro concessione dei diritti di brevetto, a produrre i bossoli, fornendo personale qualificato e *know-how* per la relativa fabbricazione (cfr. *Kasel v. Remington Arms Co.* (1972) 24 Cal. App. 3d 711, 724) e pure del proprietario di una lavanderia a gettoni self-service, il quale - benché prestasse un mero servizio - aveva svolto «un ruolo tutt'affatto che marginale o secondario nella complessiva attività di commercializzazione del prodotto in questione» (cfr. *Garcia v. Halsett*, 3 Cal.App.3d 319 (1970), specialmente 326).

⁶⁹ Va debitamente segnalato che la comprensione della sentenza non può essere disgiunta dalla lettura del precedente *Bolger v. Amazon.com*, cit, cui la Court of Appeal rinvia più volte. La decisione appena citata costituisce il caso di "*first impression*" nel diritto californiano sulla responsabilità da prodotto difettoso delle piattaforme del commercio elettronico. Giova dire che, nella fattispecie caduta per prima sotto il riflettore dell'attenzione della Corte di secondo grado californiana, la piattaforma digitale, oltre ad aver fornito al venditore del prodotto difettoso servizi telematici, aveva prestato anche servizi di logistica: la riflessione in quel caso si era naturalmente incentrata anche sul controllo materiale che la piattaforma aveva potuto esercitare con riferimento al singolo bene venduto, fonte di pregiudizio.

⁷⁰ Le circostanze consistenti nei fatti che l'intermediario digitale non era entrato in contatto con il bene, non lo aveva posseduto, non lo aveva imballa-

to e non lo aveva spedito indussero il giudice di primo grado (cfr. *Kisha Loomis v. Forrinx Technology(Usa) Inc.*, Superior Court of Los Angeles County, No. BC632830, 19 marzo 2019) a ritenere che il ruolo svolto dalla piattaforma nella distribuzione dell'*hoverboard* difettoso fosse del tutto occasionale e marginale: la piattaforma, secondo questo ragionamento, non avrebbe avuto alcuna possibilità di esercitare un controllo sulle dinamiche di mercato, tale da poter influire sulle scelte effettuate a monte nella produzione. Sotto tale profilo, Amazon è, infatti, paragonata ad una casa d'aste o, più in generale, ad un rivenditore di beni usati: in entrambi i casi, mancherebbe quella relazione continuativa con la filiera di produzione che permetterebbe anche a tali attori del mercato di contribuire all'immissione in circolazione di prodotti sicuri.

⁷¹ Sul punto, la Corte richiama il proprio precedente *Bolger v. Amazon.com*, sviluppandone il ragionamento e rinviando ad esso: cfr. *Loomis v. Amazon.com*, cit., specialmente 471.

⁷² «Amazon “owns” the customer», era stato già osservato in *Bolger v. Amazon.com*, cit., 441.

⁷³ *Loomis v. Amazon.com*, cit., specialmente 472 e 484.

⁷⁴ La Court of Appeal ha osservato che, contrariamente alla tesi sostenuta dalla piattaforma al fine di dimostrare che non aveva esercitato un controllo sulla transazione (cfr. *Loomis v. Amazon.com*, cit., specialmente 479), Amazon non avrebbe potuto essere paragonata ad un “centro commerciale digitale”, che si fosse limitato a fornire neutralmente a terzi una vetrina elettronica: le circostanze di addebitare una commissione per ogni articolo venduto, di fungere da canale di pagamento per le transazioni realizzate e di gestire le comunicazioni tra compratori e venditori avrebbero allontanato l'intermediario da una sua possibile concettualizzazione nei termini suggeriti. Al contrario, le azioni intraprese dalla piattaforma (consistenti: nell'interagire con il cliente, nel ricevere ed elaborare l'ordine, nel riscuotere il pagamento, nel trattenere una percentuale del prezzo di vendita di ogni acquisto) sono, per la Court of Appeal, coerenti con le attività svolte da rivenditori e distributori di beni di consumo; soggetti, quest'ultimi, chiamati a sopportare oggettivamente i pregiudizi scaturenti dall'uso di un bene difettoso.

⁷⁵ *Loomis v. Amazon.com*, cit., specialmente 478.

⁷⁶ Pub. L. No. 104-104, 110 Stat. 137 (1996) (47 U.S.C. § 230). Tale necessità non si porrà nel prosieguo della trattazione con riferimento all'omologa disciplina europea prima racchiusa nell'art. 14 della direttiva 2000/31 ed ora nell'art. 6 del regolamento (Ue) 2022/2065. Nel Vecchio Continente, infatti, sulla base della giurisprudenza della Corte europea di giustizia (cfr. Corte europea di giustizia, 23 marzo 2010, C-236/08, C-237/08 e C-238/08, *Google France c. Louis Vuitton Mal-*

letier, *Google France c. Viaticum Luteciel e Google France c. CNRRH*. e Corte europea di giustizia, 12 luglio 2011, C-324/09, *L'Oréal SA e altri c. eBay International AG e a.*), si presuppone che, per beneficiare dell'esenzione da responsabilità, i prestatori dei servizi di *hosting* debbano operare come prestatori di servizi di ordine meramente tecnico, automatico e passivo. Nel caso che ci occupa, invece, pur nell'estrema eterogeneità e nell'irriducibilità ad un unico modello di organizzazione, le piattaforme del commercio elettronico oltre al semplice coordinamento di domanda e offerta, si differenziano per l'offerta di servizi complementari: logistica, immagazzinamento e consegna dei prodotti; gestione degli ordini e dei pagamenti; indicizzazione, selezione, organizzazione e promozione dei prodotti; modalità di presentazione delle offerte; filtraggio dei contenuti; sistemi di valutazione di prodotti e utenti; raccolta pubblicitaria; garanzie e strumenti di composizione delle controversie, con grandi differenze tra una realtà e un'altra. Tutti servizi, quelli appena ricordati, che farebbero venir meno, alla luce della giurisprudenza prima citata, lo scudo normativo previsto per i servizi di *hosting* dall'art. 6 del regolamento (Ue) 2022/2065 più volte menzionato.

⁷⁷ J. KOSSEFF, *The Twenty-six Words that Created the Internet*, Itacha-Londra, 2019.

⁷⁸ Per la formulazione di questa difesa da parte di Amazon v. Brief for Appellee, *Fox v. Amazon.com, Inc.*, cit., 39-40. In dottrina la tesi è sostenuta, tra gli altri, da A.E. Shehan, *Note, Amazon's Invincibility: The Effect of Defective Third-Party Vendors' Products on Amazon*, 53 *Ga. L. Rev.* 1215, 1234 (2019).

⁷⁹ Tale argomento è stato da ultimo esaminato con riferimento agli obblighi informativi che gravano sugli attori della distribuzione dalla sentenza resa l'11 marzo 2022 nel caso *Lee v. Amazon.com, Inc.*, 76 *Cal. App.* 5th 200.

⁸⁰ Cfr. *HomeAway.com Inc. et al v. City of Santa Monica*, No. 18-55367 (9th Cir. 2019); *Erie Ins. Co. v. Amazon.com, Inc.*, 925 F.3d 135, 140 (4th Cir. 2019); *Oberdorf v. Amazon.com, Inc.*, cit., 153.

⁸¹ Tale argomento è stato accolto principalmente dalle Corti di prossimità: cfr., ad esempio, la decisione di primo grado resa dalla United States District Court for the District of Maryland nel caso *Erie Ins. Co. v. Amazon.com, Inc.* (8:16-cv-02679-RWT), poi ribaltata, però, in grado di appello e, con lo stesso destino, *Oberdorf v. Amazon.com, Inc.*, 295 F. Supp. 3d 496. In dottrina, sul punto, E. Goldman, *Amazon Isn't Liable for Defective Marketplace Sale (No Thanks to Section 230)-Erie Insurance v. Amazon*, <https://blog.ericgoldman.org/archives/2019/05/amazon-isnt-liable-for-defective-marketplace-sale-no-thanks-to-section-230-erie-insurance-v-amazon.htm>

⁸² *Oberdorf v. Amazon.com, Inc.*, 936 F.3d 136 (3rd Cir. 2019), specialmente 151, ove si afferma che «The second issue in this appeal is whether Oberdorf's claims, both for negligence and for strict liability, including failure to

provide adequate warnings regarding the use of the dog collar, are barred by § 230 of the CDA. [...] this is a question of federal law. We conclude that the CDA bars some, but not all, of Oberdorf's claims».

⁸³ *Oberdorf v. Amazon.com, Inc.*, cit., specialmente 152-153.

⁸⁴ *State Farm Fire & Casualty Co. v. Amazon.com, Inc.* (W.D.Wis. 2019) 390 F. Supp.3d 964, 973 e 974, *Oberdorf v. Amazon.com, Inc.*, 936 F.3d 136 (3rd Cir. 2019), specialmente 153, ove si legge «While we recognize that Amazon exercises online editorial functions, we do not agree that all of Oberdorf's claims seek to treat Amazon as the publisher or speaker of information provided by another information content provider. As previously discussed, Amazon is a "seller" of products on its website, even though the products are sourced and shipped by third-party vendors such as The Furry Gang. Amazon's involvement in transactions extends beyond a mere editorial function; it plays a large role in the actual sales process. This includes receiving customer shipping information, processing customer payments, relaying funds and information to third-party vendors, and collecting the fees it charges for providing these services»; Cfr. anche *Papataros v. Amazon.com, Inc.*, 2019 U.S. Dist. LEXIS 144253; *Bolger v. Amazon.com* 53, cit. specialmente 465.

⁸⁵ Cfr. *Amazon.com, Inc. v. McMillan*, cit., 112.

⁸⁶ *Stiner v. Amazon.com*, cit., specialmente 400.

⁸⁷ *Loomis v. Amazon.com*, cit., specialmente 479.

⁸⁸ Cfr. A. RUBINSTEIN - A. WOLINSKY, *Middlemen*, in 102 *Quarterly Journal of Economics*, 1987, 581; CHUNG-YI TSE, *The Spatial origin of commerce*, in 52 *International Economic Review*, 2011, 349.

⁸⁹ Cfr. I. TREVISAN, *La funzione distributiva. I nuovi rapporti tra industria e distribuzione*, 1991, Milano, 3; L. PELLEGRINI, *Le trasformazioni in corso*, cit., 132. Sul punto, cfr. R. PARDOLESI, *I contratti di distribuzione*, Napoli, 1979, 6, ove la distribuzione commerciale viene intesa «alla stregua di complesso di attività relative al trasferimento (verso controprestazione in denaro) di beni e servizi dal produttore all'utilizzatore finale».

⁹⁰ Sul punto, cfr. R. PARDOLESI, *I contratti di distribuzione*, cit., 12.

⁹¹ Sul punto, cfr. D. F. SPULBER, *Market Microstructure and Intermediation*, in 10 *Journal of Economic Perspectives*, 1996, specialmente 143; I. TREVISAN, *La funzione distributiva*, cit., 50.

⁹² La distribuzione è chiamata ad assolvere questo compito indipendentemente dagli intervalli di arresto della produzione. Sul punto, cfr. R. CLOWER - A. LEJONHUFVUD, *The Coordination of Economic Activities: A Keynesian Perspective*, in 65 *American Economic Review*, 1975, 182 ss.

⁹³ Sul punto, cfr. G. LANCASTER - M. MASSINGHAM, *Essentials of marketing*, London, 1988, 14 s. e 58 s., ove gli Autori mettono in luce come il problema della distribuzione dal punto di vista dell'industria - relativamente alla selezione del canale di commercializzazione - si ponga, non in termini di "quale canale scegliere", ma di "quale canale ci sceglierà".

⁹⁴ A. RUBINSTEIN - A. WOLINSKY, *Middlemen*, cit., 583.

⁹⁵ Le caratteristiche peculiari e la qualità dei singoli prodotti immessi in mercato sono spesso difficili da osservare per i singoli consumatori. Al contrario, gli intermediari che fanno scorta dei prodotti hanno maggiori possibilità di distinguere i beni di qualità superiore da quelli di qualità inferiore. Sul punto, cfr. D. F. SPULBER, *Market Microstructure*, cit., 135 ss.

⁹⁶ Per una approfondita riflessione sul punto, cfr. R. PARDOLESI, *I contratti di distribuzione*, cit., 30.

⁹⁷ I. TREVISAN, *La funzione distributiva*, cit., 52.

⁹⁸ I. TREVISAN, *La funzione distributiva*, cit., 60 sottolinea come i produttori per poter vendere ai distributori debbano soddisfare «rigorosi standard relativi al controllo di qualità e alla frequenza e alla puntualità dei rifornimenti [...]». Questo significa, in pratica, che quelle imprese della distribuzione che costituiscono gli sbocchi più appetibili in un dato mercato preferiranno trattare solo con i produttori già affermati, la cui affidabilità è provata e che sono disponibili (e capaci) di assicurare un'elevata cooperazione in queste aree». Sulla necessità del canale distributivo di impiegare a tal fine personale qualificato, cfr. R. PARDOLESI, *I contratti di distribuzione*, cit., 78.

⁹⁹ Più in dettaglio, un circuito di operazioni ripetute lungo la filiera di commercializzazione sostiene la fiducia, dato che nei sistemi sociali in cui i partecipanti si incontrano ripetutamente venire meno agli accordi diventa più complicato: «la ripetizione comporta incentivi al rispetto degli impegni, favorendo la creazione di un quadro cognitivo comune entro il quale le parti agiscono - come si usa dire con espressione di successo - "all'ombra del futuro"». Sul punto sia consentito rinviare per un ulteriore approfondimento a G. SMORTO, *Reputazione, fiducia e mercati*, *Eur. e Dir. Priv.*, 2016, 199 ss.),

¹⁰⁰ D. F. SPULBER, *Market Microstructure*, cit., 135 e 146.

¹⁰¹ Sul punto, cfr. L. PELLEGRINI, *Le trasformazioni in corso*, cit., 133.

¹⁰² R. PARDOLESI, *I contratti di distribuzione*, cit., 78.

¹⁰³ L. PELLEGRINI, *Le trasformazioni in corso*, cit., 134.

¹⁰⁴ L. PELLEGRINI, *Le trasformazioni in corso*, cit., 134 e 146.

¹⁰⁵ L. PELLEGRINI, *Le trasformazioni in corso*, cit., 146.

¹⁰⁶ L'esigenza di soddisfare le preferenze del consumatore si è resa sempre più avvertita a causa dei repentini mutamenti che si registrano nella domanda. Cfr. R. PARDOLESI, *I contratti di distribuzione*, cit., 11. Giova anche porre in luce come attente analisi (cfr. M. R. BAYE - T. F. COSIMANO, *Choosing sides in matching games: Nash equilibria and comparative statics*, in 57 *Economica*, 1990, 283 ss.) abbiano dimostrato l'esistenza di una significativa probabilità di insuccesso degli scambi allorché siano possibili solo negoziazioni dirette. In effetti le transazioni che si realizzano per mezzo degli intermediari possono produrre rendimenti di scala dalla produzione e dalla distribuzione delle informazioni, consentendo la conclusione di nuovi contratti che altrimenti andrebbero persi a causa della sussistenza di asimmetrie informative tra i due versanti del mercato. I fabbricanti, infatti, non conoscono le idiosincrasie dei clienti e gli acquirenti sono incerti sulle caratteristiche dei prodotti.

¹⁰⁷ A mutare sotto l'influsso delle informazioni fornite dalla filiera distributiva sono, dunque, anche le stesse modalità attraverso cui l'industria produce. Sugli effetti perversi (nella produzione e nella commercializzazione dei beni) della asimmetrica distribuzione delle informazioni nel mercato, cfr. G. A. AKERLOF, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, in 84 *Q. J. Econ.* 488 (1970).

¹⁰⁸ I. TREVISAN, *La funzione distributiva*, cit, 69.

¹⁰⁹ Cfr. M. W. VAN ALSTYNE - G. G. PARKER, *Pipelines, Platforms, and the New Rules of Strategy*, in *Harvard Business Review*, 2016, 54 ss.

¹¹⁰ Questa è la rappresentazione tipica che proviene dalle piattaforme: cfr. *Loomis v. Amazon.com LLC*, cit., 471, ove si legge testualmente che «Amazon describes its marketplace as "an online mall" which provides an "online storefront" to third party sellers».

¹¹¹ Sul punto, sia consentito rinviare per ulteriori approfondimenti a G. SMORTO, *Reputazione*, cit., 199 ss.

¹¹² Restituisce l'idea della mole delle recensioni dei consumatori quanto si legge nella pagina web di Amazon (<https://www.aboutamazon.com/news/company-news/product-safety-and-compliance-in-our-store>), in cui la piattaforma rassicura gli acquirenti circa gli sforzi compiuti nell'appurare la veridicità di quanto pubblicato: «Every few minutes, our tools review [...] the tens of millions of customer reviews that are submitted weekly for signs of a concern and investigate accordingly».

¹¹³ L'importanza del "passaparola" sui canali digitali quale fonte di informazioni è dimostrata anche dalla circostanza che nel 2016, il Congresso degli Stati Uniti ha promulgato il *Consumer Review Fairness Act*, che vieta clausole

contrattuali che impediscano ai consumatori di pubblicare recensioni. Cfr. 15 U.S. Code § 45b - Consumer review protection.

¹¹⁴ Sui limiti delle informazioni che attingono alla c.d. “saggezza della folla”, cfr. N. BLICKSTEIN SHCHORY, *Information Asymmetries in E-Commerce: The Challenge of Credence Qualities*, 20 J. High Tech. L., 2020, 1. Sul sovraccarico di informazioni di cui è destinatario il consumatore che si serve dell’esperienza dei propri “pari”, cfr. D. VAN KNIPPENBERG - L. DAHLANDER - M. R. HAAS - G. GEORGE, *Information, Attention, and Decision Making*, in 58 *Academy of Mgmt. J.*, 2015, 649 ss.

¹¹⁵ Cfr. L. YOU- R. SIKORA, *Performance of Online Reputation Mechanisms under the Influence of Different Types of Biases*, in 12 *Information Systems and e-Business Management*, 2014, 418; C. NOSKO - S. TADELIS, *The Limits of Reputation in Platform Markets: An Empirical Analysis and Field Experiment*, NBER Working Paper Series, Working Paper 20830, 2015, <http://www.nber.org/papers/w20830>.

¹¹⁶ A detta di parte della letteratura, le recensioni dei consumatori avrebbero potuto costituire un potenziale ed efficace sostituto anche delle tradizionali tutele consumeristiche volte a correggere le asimmetrie informative tra produttori ed acquirenti: in tal senso, cfr. S. R. PEPPE, *Freedom of Contract in an Augmented Reality: The Case of Consumer Contracts*, in 59 *Ucla L. Rev.*, 676, 686 (2012); M. COHEN - A. SUNDARARAJAN, *Self-Regulation and Innovation in the Peer-to-Peer Sharing Economy*, in 82 *U. Chi. L. Rev. Online*, 116, 121 (2015); DO-HYUNG PARK - JUMIN LEE, *eWOM Overload and Its Effect on Consumer Behavioral Intention Depending on Consumer Involvement*, in 7 *Electronic Com. Res. & Applications*, 2008, 386. Critica questa impostazione J. DAMMANN, *Electronic Word of Mouth and Consumer Protection: A Legal And Economic Analysis*, in 94 *S. Cal. L. Rev.* 423.

¹¹⁷ Sul punto, cfr. S. HE - B. HOLLENBECK - D. PROSERPIO, *The Market for Fake Reviews* in 41 *Marketing Science*, 2022, 896, ove è accuratamente dimostrato come in diversi luoghi della rete (in particolare nei social network e nelle applicazioni di messaggistica) si realizzino vere e proprie compravendite di recensioni.

¹¹⁸ Il venditore, infatti, potrebbe avere interesse a stare sul mercato solo occasionalmente. Ecco allora che ha tutto l’interesse a manipolare l’informazione che passa sui canali digitali. Sulla facilità attraverso cui i sistemi reputazionali approntati dagli intermediari digitale possono essere pilotati, cfr. J. GRIMMELMANN, *The Virtues of Moderation*, in 17 *Yale Journal of Law & Technology*, 2015, 55, J. URIST, *Who’s Feeling Lucky? Skewed Incentives, Lack of Transparency, and Manipulation of Google Search Result Under the DMCA*, in 1 *Brook. J. Corp. Fin. & Com. L.*, 2006, 220.

¹¹⁹ Che il problema sia difficilmente fronteggiabile in autonomia dagli stessi operatori dei mercati digitali è dimostrato dalla recente iniziativa pro-

cessuale intrapresa da *Amazon* contro gli organizzatori di decine di migliaia di gruppi *Facebook* nati per sollecitare recensioni non veritiere. Del risvolto processuale della vicenda ne dà atto un articolo di I. SIMONETTI, apparso sul *New York Times* il 19 luglio 2022, dal titolo “*Amazon sues leaders of more than 10,000 Facebook groups it says churn out fake reviews*”.

¹²⁰ Circostanze ampiamente documentate dal *New York Times* in un articolo a firma di G. SUTHIVARAKOM, apparso l’11 febbraio 2020 con il titolo *Welcome to the Era of Fake Products*.

¹²¹ Regolamento (Ue) 2022/2065, cit.

¹²² Cfr. il primo comma dell’art. 4 (n. 14) della proposta di direttiva.

¹²³ Ci si riferisce, in particolare, al caso *Loomis v. Amazon.com*, cit., ove, come si ricorderà, la piattaforma non aveva prestato servizi di logistica e il fornitore, benché formalmente identificabile, era di fatto irraggiungibile.

¹²⁴ Giova dire che questo aspetto era stato segnalato alla Commissione europea dal *Bureau Européen des Unions de Consommateurs* (BEUC), in sede di risposta alla *Consultazione pubblica dal titolo “Responsabilità civile - adeguare le norme in materia di responsabilità all’era digitale e all’intelligenza artificiale”* (lanciata il 18 ottobre 2021 e conclusasi il 10 gennaio 2022). In quell’occasione il BEUC aveva posto in luce la necessità che la responsabilità degli intermediari digitali dovesse scattare non solo nell’ipotesi in cui il distributore non fosse individuabile, ma anche nel caso in cui quest’ultimo non avesse intrapreso iniziativa alcuna per compensare il danno sofferto dal singolo.

¹²⁵ Si noti che potrebbero assumere rilievo, al fine di accertare se l’intermediario abbia indotto il consumatore medio a ritenere che il bene acquistato sia fornito da un destinatario del servizio che agisce sotto la sua autorità o il suo controllo, le “*Model Rules on Online Platforms*”, elaborate dall’*European Law Institute*, alcune delle quali dedicate alle responsabilità (contrattuali) dei gestori della piattaforma che esercitano una “influenza predominante” sulla fornitura del servizio sottostante. L’articolo 20 dell’articolato normativo proposto dall’*European Law Institute*, rubricato “*Liability of the Platform Operator with Predominant Influence*” così, infatti, dispone: «1. If the customer can reasonably rely on the platform operator having a predominant influence over the supplier, the customer can exercise the rights and remedies for the non-performance available against the supplier under the supplier-customer contract also against the platform operator. When assessing whether the customer can reasonably rely on the platform operator’s predominant influence over the supplier, the following criteria may be considered in particular: a) The supplier-customer contract is concluded exclusively through facilities provided on the platform; b) The platform operator withholds the identity of

the supplier or contact details until after the conclusion of the supplier-customer contract; c) The platform operator exclusively uses payment systems which enable the platform operator to withhold payments made by the customer to the supplier; d) The terms of the supplier-customer contract are essentially determined by the platform operator; e) The price to be paid by the customer is set by the platform operator; f) The marketing is focused on the platform operator and not on the suppliers; or g) The platform operator promises to monitor the conduct of suppliers and to enforce compliance with its standards beyond what is required by law».

¹²⁶ Anche su questo specifico fronte, la tutela appare di limitato ausilio per il consumatore: la piattaforma ha la possibilità di evitare di indurre falsi affidamenti semplicemente avvertendo il consumatore del fatto che la transazione sarà conclusa con un venditore terzo che opera in maniera indipendente. Obbligo peraltro previsto dal comma 7 dell'art. 30 del regolamento (Ue) 2022/2065 sui servizi digitali. La norma, rubricata "Tracciabilità degli operatori commerciali", prevede che «Il fornitore della piattaforma online che consente ai consumatori di concludere contratti a distanza con operatori commerciali mette a disposizione dei destinatari del servizio, sulle sue piattaforme online, le informazioni di cui al paragrafo 1, lettere a), d) ed e) in modo chiaro, facilmente accessibile e comprensibile. Tali informazioni devono essere disponibili almeno sull'interfaccia online della piattaforma online dove appaiono le informazioni sul prodotto o sul servizio». Le informazioni in questione sono quelle di contatto dell'operatore commerciale (nome, indirizzo, numero di telefono e indirizzo di posta elettronica), quelle relative alla sua eventuale iscrizione in un registro delle imprese (il registro presso il quale è iscritto e il relativo numero di iscrizione o mezzo equivalente di identificazione contemplato in detto registro) e «un'autocertificazione da parte dell'operatore commerciale con cui quest'ultimo si impegna a offrire solo prodotti o servizi conformi alle norme applicabili del diritto dell'Unione».

¹²⁷ Cfr. *Loomis v. Amazon.com*, cit.

¹²⁸ Il fatto stesso che un qualsiasi prodotto sia disponibile sulla piattaforma veicola all'insieme dei potenziali acquirenti (fidelizzati alla piattaforma da offerte speciali e programmi in abbonamento che permettono l'accesso a offerte esclusive) il messaggio rassicurante che, proprio perché inserito in quell'assortimento virtuale, sia, come tutti gli altri beni che ne fanno parte, sicuro e commerciabile.

¹²⁹ Da questo punto di vista, la responsabilità aquiliana sarebbe chiamata ad incentivare la prevenzione del danno. In generale, sulla responsabilità civile come puntello per incentivare l'investimento in misure preventive di sicurezza, cfr. P. G. Monateri, *La responsabilità civile*, Milano, 2006, 20 ss. e 39 ss.; sul

punto, cfr. anche M. Grondona, *La responsabilità civile tra libertà individuale e responsabilità sociale. Contributo al dibattito sui «risarcimenti punitivi»*, Napoli, 2017, 70 ss. Più in generale, e sulla presa d'atto anche nella giurisprudenza italiana di vertice, del carattere polifunzionale della responsabilità civile, cfr. A. Palmieri, R. Pardolesi, *I danni punitivi e le molte anime della responsabilità civile*, in *Il Foro it.*, I, 2017, 2630 ss.

¹³⁰ A. ALBANESE, *La responsabilità civile per i danni da circolazione di veicoli ad elevata automazione*, in *Europa e Diritto Privato*, 2019, 995.

¹³¹ A. ALBANESE, *La responsabilità*, cit., 995.

¹³² Non muta la sostanza di quanto si sta dicendo l'inciso, contenuto nel considerando n. 28 della proposta di direttiva (e in termini parzialmente diversi nel comma 6° dell'art. 7), a tenore del quale le piattaforme online, «quando svolgono il ruolo di [...] importatore o distributore di un prodotto difettoso, dovrebbero essere responsabili alle stesse condizioni di tali operatori economici». Ancora una volta, infatti, si ripropone il problema di fondo segnalato in questo studio, legato all'impostazione anacronistica (sia della direttiva da superare sia della nuova proposta), di considerare la filiera commerciale solo in funzione servente rispetto all'industria produttrice. Ove, poi, il significato da attribuire all'inciso contenuto nel considerando n. 28 (e nella parte corrispondente del comma 6° dell'art. 7) fosse quello di prevedere per l'attore digitale regimi di responsabilità più rigorosi nel caso in cui abbia assunto le vesti di altri operatori economici, la direttiva sconterebbe il limite che si propone di superare: il fatto, cioè, di delegare *ex ante* alla concretizzazione giudiziale l'individuazione delle condizioni alla cui stregua definire se l'intermediario digitale si sia comportato di fatto alla stregua di «importatore o distributore» del prodotto difettoso.

¹³³ Si è contribuito, così, ad accrescere il rischio per il consumatore di acquistare prodotti poco sicuri. Sul punto, cfr. J. EMONT, *Amazon's Heavy Recruitment of Chinese Sellers Puts Consumers at Risk*, *Wall St. J.*, 11 novembre 2019.

Tutela della persona e limitazione dell'errore umano tra *Advanced Driver Assistance Systems* e guida automatizzata di livello 3

ENRICO AL MUREDEN

SOMMARIO: 1. La sicurezza stradale e l'obiettivo "zero vittime" nei principi sovranazionali. - 2. Il contenimento dell'errore umano tra ADAS e guida assistita di livello. - 3. La crescente rilevanza del danno da difetto del prodotto e la persistente attualità dell'art. 2054, comma 4 c.c. - 4. Il danno da veicolo autonomo "conforme" tra responsabilità del produttore e nuove forme di indennizzo.

1. La sicurezza stradale e l'obiettivo "zero vittime" nei principi sovranazionali

L'esigenza di garantire un'effettiva tutela dell'integrità delle persone a fronte dei rischi scaturenti dalla circolazione dei veicoli costituisce da sempre un obiettivo perseguito a livello globale dalle Nazioni Unite e si iscrive, nel contesto attuale, entro gli Obiettivi della Agenda ONU 2030¹. In quest'ottica la risoluzione *Improving Road Safety*² individua l'obiettivo di ridurre in misura pari ad almeno il 50% il numero dei decessi e delle lesioni scaturenti dal traffico stradale entro il 2030. La finalità di limitare il numero di sinistri e le loro conseguenze riferite tanto agli occupanti delle automobili, quanto ai cosiddetti utenti deboli della strada, ossia ai pedoni e ciclisti, riecheggia anche le linee programmatiche che caratterizzano l'azione dell'Unione Europea e quella del legislatore nazionale.

In un simile scenario, l'opportunità di superare gli ostacoli posti dalla concezione tradizionale della guida e di creare i presupposti

per consentire una transizione rapida, affidabile e sicura verso la diffusione di veicoli a guida automatizzata è stata posta in luce dalla Commissione Europea che, nell'ambito del c.d. GEAR 2030³, ha delineato una *Roadmap for Automated Driving*⁴ e da un successivo *report* commissionato dal Parlamento Europeo nel quale è stata posta in evidenza l'opportunità di una revisione sistematica di molteplici discipline attualmente vigenti e dell'introduzione di regole concepite in funzione delle specificità che caratterizzano i nuovi rischi scaturenti dalla circolazione di veicoli individuando in essa il volano di una crescita economica⁵; crescita che, invero, dovrà necessariamente coinvolgere una vasta rete di rapporti che vedono interessati molteplici settori collegati alla circolazione stradale compendiate nella *Platform for the Deployment of Cooperative Intelligent Transport Systems in the European Union (C-ITS)*⁶.

Il percorso intrapreso dall'Unione Europea, pertanto, è teso all'individuazione di regole uniformi capaci di promuovere la sperimentazione e la successiva diffusione delle auto altamente automatizzate in un quadro giuridico armonizzato funzionale a ridurre nella massima misura possibile le divergenze delle singole legislazioni nazionali in tutti i contesti che concorrono a regolare la circolazione dei veicoli, così da garantirne l'affidabilità nelle molteplici situazioni nelle quali l'assunzione di decisioni tradizionalmente imputabili all'essere umano costituiranno il frutto di un'interazione tra esso ed i meccanismi automatizzati o talvolta risulteranno totalmente devolute a questi ultimi.

Queste considerazioni, del resto, trovano piena corrispondenza nell'attuale Piano Nazionale Sicurezza Stradale 2030, che individua nell'incremento della sicurezza stradale uno dei pilastri del sistema di mobilità sostenibile. Proprio in questo contesto viene ulteriormente sottolineata la fondamentale importanza rivestita dai dispositivi ADAS, che determinano una riconduzione della condotta umana dentro gli standard di sicurezza previsti dal legislatore e sorvegliano l'effettività di questo processo attraverso

*l'Event Data Recorder*⁷. Sotto questo profilo emerge l'opportunità della diffusione di strumenti capaci di incrementare il livello di conformità della guida del veicolo rispetto alle regole che governano la sicurezza della circolazione stradale attraverso il contenimento di quel fattore di soggettività sintetizzato nell'espressione del cosiddetto "errore umano". L'introduzione di un pacchetto di ADAS che riportano la conduzione del veicolo entro gli standard legali limita significativamente la possibilità di errori; al tempo stesso la possibilità di affidare tutte le operazioni di guida a sistemi automatizzati soggetti solamente alla sorveglianza del responsabile contribuisce ad elevare ulteriormente il livello di standardizzazione della circolazione dei veicoli e di conseguenza la conformità alle discipline legali. Cionondimeno occorre sottolineare che anche in un contesto destinato a contenere l'incidenza dell'errore umano il ruolo della persona che assume la veste di conducente continuerà a rivestire un'importanza fondamentale, in quanto nello scenario della guida di livello 2 l'azione del conducente, ancorché circoscritta entro le limitazioni imposte dal funzionamento degli ADAS, resta l'elemento predominante della guida; anche nel secondo scenario, ossia quello della guida di livello 3, la condotta umana conserva una fondamentale rilevanza, in quanto è comunque rimessa ad un'operazione decisa dal conducente l'attivazione dei meccanismi di guida automatizzata i quali richiedono una continua reperibilità del conducente e quindi una sua capacità di essere sempre pronto ad intervenire in modo appropriato al fine di evitare sinistri.

2. Il contenimento dell'errore umano tra ADAS e guida assistita di livello 3.

In un contesto ormai caratterizzato dalla rapida transizione da un modello di guida tradizionale incentrato sul fondamentale ruolo del conducente ad uno basato sulla guida assistita, si regi-

stra l'ingresso nel sistema normativo di due rilevanti novità che, operando sinergicamente, contribuiranno ad imprimere una significativa svolta verso la progressiva affermazione degli *Advanced Driver Assistance Systems* (ADAS) e la guida assistita di livello 3.

Il 14 luglio 2022, infatti, segna la data dell'entrata in vigore del nuovo art. 34-*bis* della Convenzione di Vienna sulla circolazione stradale del 1968, rubricato "guida autonoma". L'introduzione di una simile previsione nella Convenzione ONU che regola plurimi aspetti della circolazione stradale nell'Unione Europea ed in una molteplicità di Paesi aderenti rimuove il principale ostacolo alla diffusione di veicoli altamente automatizzati equipaggiati con *Advanced Driver Assistance Systems* di livello 3⁸, ossia di vetture che – pur richiedendo la presenza di un conducente che svolga attività di monitoraggio e sia in grado di intervenire in caso di necessità – dispongono della capacità di viaggiare autonomamente e controllare ogni aspetto connesso alla guida in ambienti mappati⁹.

La possibilità di considerare «soddisfatto il requisito della presenza di un conducente in ogni veicolo (...) in movimento» quando esso «utilizza un sistema di guida autonoma conforme» ai «regolamenti tecnici nazionali, e a qualsiasi strumento giuridico internazionale» (art. 34-*bis*, lett. a, Convenzione di Vienna), o «alla legislazione nazionale che regola il funzionamento del veicolo» (art. 34-*bis*, lett. b, Convenzione di Vienna) dà la facoltà ai legislatori dei singoli Stati aderenti di operare un intervento di riforma che, introducendo nei sistemi nazionali previsioni conformi al principio espresso nella Convenzione, consentirà alla auto di livello 3 – già disponibili allo stato della tecnica – di esprimere tutte le loro potenzialità sulle strade destinate alla circolazione pubblica¹⁰. Con particolare riferimento all'ordinamento italiano si delinea l'esigenza di una modifica dell'art. 46 del Codice della Strada il cui testo attuale dispone che «si intendono per veicoli tutte le macchine di qualsiasi spe-

cie, che circolano sulle strade guidate dall'uomo». Questa profonda trasformazione consentirà un avvicinamento del nostro sistema a quelli di molti ordinamenti statunitensi e più in generale a quelli che, non aderendo alla Convenzione di Vienna, hanno potuto ammettere già da tempo la circolazione generalizzata di veicoli altamente automatizzati¹¹.

L'apertura del legislatore verso forme di circolazione nelle quali la guida può essere in larga misura affidata a sistemi automatizzati e richiedere un intervento solo eventuale del pilota costituisce il tassello di un più articolato disegno nel quale si iscrive anche un altro intervento del legislatore dell'Unione Europea che – oltre ad introdurre immediatamente significative innovazioni applicabili ai veicoli dotati di dispositivi di livello 2 – costituisce un importante viatico nell'ottica della diffusione delle auto di livello 3.

Infatti il Reg. (UE) 2019/2144 entrato in vigore il 6 luglio 2022 – sottolineando l'esigenza di valorizzare l'impiego delle nuove tecnologie al fine di «migliorare ulteriormente le prestazioni di sicurezza dei veicoli nell'ambito di un approccio integrato alla sicurezza stradale e allo scopo di proteggere meglio gli utenti vulnerabili della strada» – ha disposto l'obbligo di equipaggiare i veicoli di nuova immatricolazione con una serie di dispositivi ADAS funzionali ad innalzarne la sicurezza attiva e passiva (sistemi avanzati di adattamento intelligente della velocità; interfaccia di installazione di dispositivi di tipo *alcock*; avviso della disattenzione e della stanchezza del conducente; avviso avanzato di distrazione del conducente; segnalazione di arresto di emergenza; rilevamento in retromarcia) ed a monitorare le fasi della guida attraverso l'introduzione del registratore di dati di evento (c.d. *Event Data Recorder*; art. 6, lett. g), Reg. 2019/2144/UE)¹².

L'operare sinergico di strumenti funzionali ad incrementare la sicurezza dei veicoli e di quello destinato a registrare gli eventi (c.d. *Event Data Recorder*) consentirà di differenziare le auto di nuova omologazione ed immatricolazione non solo sot-

to il profilo della maggiore sicurezza, ma anche sotto quello della accresciuta idoneità a ricostruire in modo puntuale e tendenzialmente inequivocabile le dinamiche dei sinistri.

Il combinarsi delle recenti modifiche del quadro legislativo può essere osservato come la manifestazione di una progressiva transizione dal modello di guida tradizionale, integralmente affidato all'azione del conducente, ad una guida assistita e parzialmente automatizzata nella quale assume una crescente rilevanza il sistema che governa la conduzione del veicolo. L'introduzione da parte del Reg. (UE) 2019/2144 di nuovi ADAS che assistono il pilota nelle operazioni di guida ed incidono sulla sua condotta inducendola a conformarsi alle regole che governano la sicurezza stradale, unitamente all'*Event Data Recorder*, che registra le fasi precedenti ai sinistri rendendo possibile la puntuale ricostruzione della loro dinamica, consentono di estendere in via generalizzata il livello di automazione 2, e, in altri termini, di introdurre sistemi capaci di contenere gli errori umani ed incanalare la condotta del pilota entro gli standard di conformità alle norme di sicurezza che tradizionalmente erano affidati alle sue abilità e alla sua disciplina.

La recente integrazione della convenzione di Vienna mediante l'inserimento del nuovo art. 34-bis, rimuovendo la previsione che imponeva un costante coinvolgimento del conducente nella guida, crea i presupposti affinché i singoli ordinamenti aderenti alla Convenzione istituiscano un quadro normativo favorevole al diffondersi di veicoli dotati di dispositivi di automazione di livello 3, ossia capaci di circolare in modalità autonoma nell'ambito di ambienti mappati, richiedendo un intervento del conducente solo nell'ipotesi in cui il sistema automatizzato non sia in grado di funzionare autonomamente in modo affidabile.

In definitiva, osservando i due provvedimenti nel loro complesso, si può intravedere la transizione da un sistema nel quale la conformità della guida alle regole che governano la sicurezza

stradale era integralmente affidata alla condotta del conducente ad uno nel quale la discrezionalità e le conseguenti possibilità di errore nella guida tradizionale vengono significativamente contenuti dall'operare di ADAS di livello 2 – obbligatoriamente installati sui veicoli di nuova immatricolazione – e dal progressivo incedere di veicoli dotati di dispositivi di automazione di livello 3 che determinerà un graduale affermarsi di una guida automatizzata la cui sicurezza appare garantita dall'operatività di un sistema programmato per conformarsi integralmente alle regole della circolazione stradale. Il passaggio dal livello 2 a livello 3 può essere osservato proprio sotto la prospettiva della centralità della figura del conducente umano che, persiste nel livello 2, seppur coadiuvata dai dispositivi ADAS per degradare, nel livello, 3 al ruolo di “sorvegliante” chiamato ad intervenire nelle ipotesi in cui il sistema automatizzato richieda un coinvolgimento della persona¹³.

3. La crescente rilevanza del danno da difetto del prodotto e la persistente attualità dell'art. 2054, comma 4 c.c.

La prospettiva di una costante diffusione di veicoli dotati di dispositivi che consentiranno di accedere alla guida di livello 2 e di livello 3 pone delicate questioni interpretative con riferimento alla persistente attualità dei principi e delle regole dettati per il governo delle conseguenze degli incidenti cagionati dalla circolazione stradale.

Un primo ordine di questioni – che attualmente si pone con riferimento ai veicoli automatizzati di livello 2 – consiste nell'esigenza di una rimodulazione del rapporto tra responsabilità del conducente e responsabilità del produttore negli incidenti provocati dal veicolo nei frangenti in cui operino i dispositivi automatizzati di assistenza alla guida (ADAS)¹⁴. Il problema di una transizione da un sistema *driver focused* ad uno nel quale

assumeranno una crescente rilevanza le funzioni assolute da meccanismi automatizzati – generale e comune a tutti gli ordinamenti – si pone con specifico riguardo al contesto nazionale nella prospettiva di verificare la persistente adeguatezza della disciplina originariamente concepita dal legislatore del 1942 e tuttora vigente, la quale prevede che il proprietario del veicolo (o, in sua vece, l'usufruttuario o l'acquirente con patto di riservato dominio) ed il conducente siano «responsabili dei danni derivati da vizi di costruzione o da difetto di manutenzione del veicolo» (art. 2054, comma 4, c.c.)¹⁵. Alla responsabilità di questi soggetti deve aggiungersi quella del fabbricante che, fino all'introduzione della disciplina sul danno da prodotto, rispondeva sulla base della generale regola codificata all'art. 2043 c.c. e che – a seguito del radicale mutamento, derivante dal recepimento della dir. 85/374/CEE ad opera del d.p.r. n. 224 del 1988 – è soggetto ad un regime di responsabilità fondato sulla nozione di «prodotto difettoso». Nell'attuale contesto normativo, pertanto, il fabbricante risponde per i danni cagionati all'utilizzatore sulla base delle norme contenute negli artt. 114 ss. del codice del consumo; tale forma di responsabilità assume particolare rilievo per quanto concerne i danni subiti dal conducente del veicolo, che, fino all'introduzione della disciplina in materia di danno da prodotto, poteva conseguire un risarcimento solamente ricorrendo alla tutela generica offerta dall'art. 2043 c.c.¹⁶. La crescente diffusione di auto dotate di dispositivi che consentono una guida assistita riconducibile al livello 2 determina una situazione nella quale il prodotto svolge funzioni di guida tradizionalmente assolute dal conducente, ponendo così il problema di una transizione da un modello di responsabilità (*driver focused*) che alloca su quest'ultimo il costo risarcitorio derivante dell'incidente ad uno *product focused*, che pone detto costo sul produttore dei dispositivi su cui il pilota poteva fare affidamento. In questa prospettiva, ad esempio, l'incidente nel quale ven-

ga danneggiato un pedone durante una fase di parcheggio effettuata utilizzando i sistemi avanzati quali quelli di adattamento intelligente della velocità [art. 6, lett. a), Reg. UE 2019/2144] potrebbe fuoriuscire dall'ambito applicativo dell'art. 2054, comma 1, c.c. per ricadere nelle diverse previsioni che basano la responsabilità sul difetto del prodotto ponendo i costi risarcitori che da questo scaturiscono in capo al proprietario del veicolo (art. 2054, comma 4, c.c.)¹⁷ o al suo fabbricante (art. 114 c. cons.). Considerazioni analoghe potrebbero ripetersi con riferimento ad incidenti causati durante l'operatività di dispositivi quale l'*Automated Lane Keeping System (ALKS)*¹⁸ che, condizioni la traiettoria del veicolo ed ostacoli il conducente nell'effettuare una manovra volta ad evitare un incidente. L'analisi di tali problematiche effettuata in un accurato studio condotto con riferimento al sistema tedesco ha posto in luce in primo luogo che, qualora i dispositivi automatizzati presuppongano una costante interazione con il pilota, riveste fondamentale importanza la consapevolezza di quest'ultimo rispetto alle caratteristiche del veicolo, dei suoi sistemi di guida autonoma e dei loro limiti. Tale presupposto, infatti, riveste carattere indefettibile al fine di adottare la condotta più appropriata sotto il profilo del monitoraggio e dell'intervento in caso di necessità. In questo nuovo contesto, pertanto, le capacità del pilota continuano ad assumere una rilevanza centrale, anche se l'incedere dell'automazione determina una loro parziale modificazione ed un diverso e maggiore coinvolgimento del produttore. Poiché l'ottimale conduzione del veicolo dipenderà dalla capacità del pilota di interagire con sistemi automatizzati, sembra possibile affermare che le attuali regole in materia di responsabilità del conducente per i danni cagionati dalla circolazione mantengano in termini generali la loro validità¹⁹, ma debbano essere al contempo lette in una prospettiva di sempre maggiore complementarità rispetto alle norme che regolano la responsabilità del produttore.

Sotto questo profilo, pertanto, sono destinate ad assumere una rilevanza crescente le informazioni fornite dal produttore nel libretto di istruzioni ed anche quelle comunicate attraverso gli strumenti pubblicitari²⁰; esse, infatti, non devono essere formulate con modalità tali da indurre il conducente a sovrastimare le *performance* del sistema automatizzato e ad abbassare il livello di attenzione richiesto dalla guida²¹.

Queste considerazioni sembrano destinate a conservare la loro validità anche con riferimento alla circolazione delle auto dotate di meccanismi di automazione di livello 3. In particolare, nel momento in cui saranno operativi i sistemi capaci di sostituire il guidatore e condurre il veicolo autonomamente, appare verosimile ritenere che la responsabilità per i danni cagionati dal veicolo ricada entro la previsione dell'articolo 2054, comma 4, c.c. Ciò non esclude, tuttavia, la persistenza di una rilevante responsabilità del conducente che, sebbene non direttamente coinvolto nella guida, deve continuare a rimanere vigile e pronto ad intervenire non appena il sistema lo richieda. Sotto questo profilo si pongono delicate questioni concernenti il funzionamento dei dispositivi che assolvono alla funzione della cosiddetta *human machine interface*, ossia di mantenere una comunicazione costante tra il veicolo il conducente in modo da richiamare prontamente ed efficacemente l'attenzione di quest'ultimo ed indurlo a riprendere i comandi dell'auto.

4. Il danno da veicolo autonomo “conforme” tra responsabilità del produttore e nuove forme di indennizzo

La totale implementazione della guida assistita di livello 2 e di quella parzialmente automatizzata di livello 3 dovrebbe condurre, secondo gli studi maggiormente accreditati, ad una significativa riduzione del numero degli incidenti. In tale contesto permarranno comunque sinistri dovuta a difetti di

funzionamento del veicolo, ad imperfezioni della struttura stradale o a comportamenti anomali delle persone. Altra parte dei sinistri, tuttavia, potrebbe essere cagionata da veicoli conformi, ossia operanti nella modalità autonoma secondo protocolli predeterminati e validati dagli standard legislativi che ne definiscono la sicurezza. Il primo genere di incidenti, ossia quelli provocati da difetti del prodotto o delle infrastrutture, nonché da condotte umane anomale, potrebbe continuare ad essere disciplinato ricorrendo alle regole che attualmente governano la responsabilità del fabbricante, quella del gestore delle strade e quella degli utenti della strada.

La seconda tipologia di sinistri – ossia gli incidenti cagionati da veicoli conformi agli standard legislativi –, invece, pone il problema dell’allocazione dei costi scaturenti da attività esercitate in piena aderenza rispetto agli standard normativi che definiscono livelli di sicurezza valutati come ragionevoli dal legislatore.

Si pone, così, il problema di dar vita ad un quadro normativo idoneo a fornire un sufficiente livello di certezza e di prevedibilità riguardo alle responsabilità scaturenti dalla commercializzazione e dalla circolazione di veicoli altamente automatizzati ed un’efficiente allocazione dei costi degli incidenti cagionati dalla loro circolazione. In quest’ottica sono state prospettate nel sistema statunitense diverse soluzioni interpretative in una prospettiva *de iure condendo* ormai verosimilmente prossima a concretizzarsi.

Una visione fortemente favorevole a conseguire nel più breve tempo possibile una drastica riduzione degli incidenti mediante la sostituzione dei veicoli tradizionali con quelli automatizzati ha individuato una soluzione interpretativa basata su una lettura coordinata delle norme federali in materia di sicurezza dei veicoli con quelle statali concernenti la responsabilità civile. In questa prospettiva riveste un ruolo fondamentale la *preemption doctrine* in ragione della quale la conformità di un

veicolo agli standard federali delineati dalla *National Highway Traffic Safety Agency* (NHTSA) costituisce un limite oltre il quale non è configurabile una responsabilità civile in capo al produttore che abbia immesso sul mercato un veicolo conforme²². Detto principio – formatosi sulla base della costante interpretazione del *National Traffic and Motor Vehicle Safety Act* del 1966 con riferimento ai veicoli tradizionali – dovrebbe estendersi, secondo questa visione, anche alla futura legislazione federale in materia di veicoli altamente automatizzati.

In definitiva la lettura appena illustrata consentirebbe di attribuire alla *regulatory compliance* il rango di una *complete defense* e di promuovere la rapida diffusione di una tecnologia capace di garantire un più elevato livello di sicurezza. In una simile prospettiva la responsabilità del produttore si potrebbe configurare solo in presenza di una non conformità rispetto agli standard federali. In questo modo il *regulatory-compliant autonomous vehicle* dovrebbe comportare una responsabilità del produttore circoscritta ai soli incidenti cagionati dal malfunzionamento, dell'auto, del suo *hardware* (*strict product liability*) o dall'assenza di adeguati avvertimenti forniti dal produttore al fine di consentire un uso ragionevolmente sicuro del veicolo in condizioni normali²³.

In un simile disegno l'estensione della responsabilità civile del produttore non subirebbe significative alterazioni rispetto al contesto attuale ed il costo degli incidenti provocati dai veicoli automatizzati conformi agli standard federali continuerebbe a gravare in prevalenza sull'utilizzatore il quale sopporterebbe gli oneri risarcitori derivanti dai danni provocati a terzi in virtù della sua qualità di proprietario o conducente del veicolo. Anche per quanto concerne le c.d. *one car collision* – nelle quali per effetto di una manovra correttamente effettuata da un veicolo automatizzato conforme dovessero prodursi danni in capo al proprietario-conducente – opererebbe la *preemption doctrine* come causa di limitazione della responsabilità del fabbricante e

dovrebbe quindi escludersi in linea di principio la risarcibilità del danno subito dall'utilizzatore del veicolo conforme.

Una simile lettura appare in linea con le soluzioni che attualmente governano la responsabilità per danno da prodotto conforme in molti contesti merceologici²⁴.

In prima approssimazione questo approccio potrebbe apparire favorevole per i produttori in quanto limiterebbe la loro responsabilità ai soli casi di danni provocati da prodotti difettosi, ossia non conformi agli standard legislativi. Cionondimeno questa soluzione può rivelarsi controproducente in quanto non idonea a infondere nel consumatore quel sentimento di fiducia necessario a vincere la diffidenza alimentata dal cosiddetto *bias dello status quo*²⁵.

Una diversa lettura del fenomeno della diffusione delle *driverless cars* pone in rilievo l'esigenza di socializzare i costi dei nuovi incidenti causati dall'automazione della circolazione stradale e a tal fine lumeggia l'introduzione di un sistema denominato *Market Enterprise Responsibility* (MER), il quale presupporrebbe l'istituzione di un fondo alimentato dagli stessi produttori funzionale a creare le risorse a cui attingere per far fronte al risarcimento dei danni eventualmente cagionati²⁶. In questo modo si realizzerebbe una copertura di tipo latamente indennitario a favore degli occupanti, dei pedoni e di ogni tipo di *bystander* che consentirebbe di allocare tutti i costi derivanti dagli incidenti causati dai veicoli di *driverless*. Il sistema della *Market Enterprise Responsibility* (MER) consentirebbe, inoltre, di allocare i costi degli incidenti provocati dai veicoli automatizzati secondo una modalità caratterizzata da un elevato livello di sostenibilità economica combinandosi con il meccanismo della *market share liability*. Con questa formula, che consente la ripartizione della responsabilità civile e degli obblighi risarcitori che ne conseguono in proporzione alle quote di mercato riferibili ai singoli danneggiati, sarebbe infatti possibile porre su ciascun

produttore un onere di contribuzione al finanziamento del fondo destinato alla compensazione delle vittime degli incidenti direttamente proporzionale alle quote di mercato conseguite. Il contributo fornito da ciascun produttore risulterebbe così proporzionale all'entità del rischio introdotto nella società quantificato mediante il numero di veicoli venduti.

Un simile criterio, tuttavia, dovrebbe essere integrato da un ulteriore variabile che consenta di valorizzare le scelte delle imprese che investono sul miglioramento dei requisiti di sicurezza dei propri veicoli. L'entità del contributo dovuto da ciascun produttore al fine di alimentare le risorse destinate a compensare le vittime, infatti, dovrebbe essere determinata combinando il parametro delle quote di mercato con quello del "coefficiente di sicurezza" dei veicoli commercializzati. Proprio quest'ultimo criterio costituirebbe un efficace incentivo a produrre e commercializzare auto caratterizzate da elevate capacità di evitare gli incidenti (sicurezza attiva) e di mitigarne le conseguenze (sicurezza passiva).

La prospettiva di un sistema di tipo indennitario nel quale le risorse necessarie al fine di garantire una pronta e adeguata compensazione economica alle vittime vengano alimentate da un contributo dei produttori giustificato in funzione delle quote di mercato conseguite ed anche del coefficiente di sicurezza del prodotto consente di cogliere il fondamentale il ruolo assoluto dall'*Event Data Recorder*. Infatti i dati conseguiti attraverso l'operare di questo strumento, osservati nel loro complesso, consentiranno di effettuare puntuali *ratings* riguardo alla sicurezza dei singoli modelli e, di conseguenza, creeranno le condizioni per poter premiare i produttori che, investendo nella ricerca e nella fabbricazione di veicoli caratterizzati da un elevato livello di sicurezza, potranno essere chiamati a contribuire al fondo destinato alle vittime degli incidenti in una misura inversamente proporzionale alla capacità dei loro veicoli di evitare gli incidenti e di contenerne le conseguenze dannose.

Un simile approccio si pone nel solco di una condivisibile tendenza a valorizzare l'assunzione di decisioni fondata sulla disponibilità e sull'analisi di una significativa quantità di dati (*data driven decisions*). A tale fine, pertanto, appare imprescindibile rendere ancora più intenso il rapporto di sinergia e complementarietà tra le diverse discipline facendo sì che i dispositivi deputati alla raccolta dei dati vengano regolati e concepiti in funzione di una raccolta di dati sempre più funzionale a ricostruire in ogni singolo dettaglio le complesse relazioni tra conducente e dispositivi di assistenza ed automazione della guida (*Human Machine Interface*)²⁷.

Note di chiusura

¹ J. WISMANS, S. SELPI, M. THYNELL, G. LINDBERG, *Economics of Road Safety - What does it imply under the 2030 Agenda for Sustainable Development?*, cit.

² L'Assemblea generale delle Nazioni Unite ha adottato, il 31 agosto 2020, la A / 74 / L.86 e Add.1, in <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/226/30/PDF/N2022630.pdf?OpenElement>.

³ La Commissione Europea ha istituito l'*High Level Group on the Competitiveness and Sustainable Growth of the Automotive Industry in the European Union (GEAR 2030)* nell'ottobre del 2015 al fine di compendiare le diverse istanze sottese alla circolazione stradale. Il gruppo annovera rappresentanti degli stati membri e *stakeholders* che riflettono le istanze dell'industria, dei consumatori, della tutela ambientale e della sicurezza stradale al fine di delineare le politiche da adottare nella prospettiva che si pone come orizzonte temporale il 2030.

⁴ Cfr. il documento *Prioritising the Safety Potential of Automated Driving in Europe*, pubblicato dall'*European Transport Safety Council (ETSC)*, in <https://etsc.eu/>.

⁵ Nel documento *A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment Accompanying the European Parliament's legislative own-initiative report (Rapporteur: Mady Delvaux)*, in <https://op.europa.eu/it/publication-detail/-/publication/df658667-20f1-11e8-ac73-01aa75ed71a1>, p. 5, viene chiarito che l'affermarsi di strumenti idonei ad elevare il livello di automazione della guida dovrà condurre verso una revisione dell'attuale quadro normativo e, in particolare, della disciplina che governa i profili assicurativi (dir. 2009/103/CE) e di quella in materia di responsabilità del produttore (dir. 85/374/CEE).

⁶ In proposito, si rinvia al documento *Study on the Deployment of C-ITS in Europe: Final Report*, in <https://transport.ec.europa.eu>, nel quale sono compendiate le esigenze emerse all'esito della consultazione di una variegata platea di *stakeholders*.

⁷ Il Piano è consultabile all'indirizzo <https://www.mit.gov.it/node/15908>.

⁸ Sotto questo profilo assume una rilevanza fondamentale la classificazione dei cinque livelli di automazione operata dalla *Society of Automotive Engineers International* (ente di normazione nel campo dell'industria aerospaziale, automobilistica e veicolistica che elabora standard tecnici funzionali alla fabbricazione di prodotti ed allo svolgimento di attività). Essa contempla un livello 0, che designa l'auto tradizionale in cui la conduzione è interamente devoluta al pilota; un livello 1 in cui sono presenti dispositivi (*Stability Control*;

Cruise Control; *Lane Correction Technology*) ormai diffusi sulla grande maggioranza dei veicoli più recenti; un livello 2 che designa i veicoli nei quali i dispositivi automatici controllano sia le funzioni di sterzata, sia quelle di accelerazione e decelerazione nell'ambito di scenari predeterminati, ma non permettono di escludere la permanente necessità di mantenere un costante controllo da parte del pilota umano. I successivi livelli di automazione, ancorché pienamente conseguiti dal punto di vista tecnico, riguardano veicoli che attualmente stanno attraversando – nel panorama complessivo di una pluralità di ordinamenti caratterizzati da discipline differenziate – la fase della sperimentazione sia in contesti appositamente ideati a tal fine sia nelle condizioni reali della circolazione stradale. Così, le auto rientranti nel livello 3 dispongono di meccanismi capaci di controllare ogni aspetto connesso alla guida in ambienti mappati (*mapped environment*), ma al tempo stesso richiedono la costante presenza a bordo di un pilota che svolga attività di monitoraggio e sia in grado di intervenire nelle ipotesi in cui lo scenario prefigurato nella mappatura si modifichi rendendo necessarie operazioni che non potevano essere programmate sulla base delle informazioni disponibili *ex ante*. Al livello 4 di automazione si collocano i veicoli nei quali la presenza di un pilota umano risulta del tutto superflua in ogni condizione; la presenza di strumenti che consentano la guida da parte di una persona, pertanto, si giustifica solo in ragione dell'eventualità che sia necessario utilizzare l'auto in ambienti e condizioni in cui la guida automatizzata sia impossibile o qualora il pilota decida di dedicarsi personalmente alla guida. L'ultimo livello (5) include le auto che, discostandosi completamente dall'attuale concezione di veicolo, svolgono le funzioni di guida in modo completamente autonomo escludendo ogni intervento umano e che, pertanto, sono prive degli strumenti (sterzo, pedali) attraverso i quali questo tipicamente si realizza.

⁹ Nell'Unione Europea lo scenario normativo (per un'accurata illustrazione delle soluzioni che si stanno delineando nei diversi ordinamenti dell'UE cfr. *Automated Driving Roadmap*, redatta dal ERTRAC Working Group, pubblicata il 29 maggio 2017, http://www.ertrac.org/uploads/images/ERTRAC_Automated_Driving_2017.pdf) si caratterizzava infatti per la presenza di significativi ostacoli allo sviluppo delle *autonomous driving cars* che scaturivano dalle previsioni della Convenzione di Vienna del 1968, la cui originaria formulazione imponeva ad «ogni veicolo in movimento o ogni complesso di veicoli in movimento» di «avere un conducente» (art. 8, comma 1) dotato delle «cognizioni e l'abilità necessarie per la guida del veicolo» (art. 8, comma 4) e che mantenesse «costantemente il controllo del proprio veicolo» (art. 8, comma 5) restando in ogni circostanza «padrone del proprio veicolo, in modo da potersi conformare

alle esigenze della prudenza e da essere costantemente in grado di effettuare tutte le manovre che gli competono». Sulla scorta delle indifferibili esigenze di incentivare il processo che dovrà condurre alla futura automazione della guida è stata come detto attuata una revisione della Convenzione di Vienna – il cui art. 8 contempla nella sua formulazione attuale la possibilità che il conducente non tenga le mani sullo sterzo e si limiti a sorvegliare il veicolo mentre esso procede in modalità autonoma, conservando costantemente la capacità di riassumere senza indugio il controllo del veicolo (cfr. I. FERRARI, *Analisi comparata in tema di responsabilità civile legata alla circolazione dei veicoli a guida autonoma*, in *Smart Roads e driverless cars: tra diritto, tecnologie, etica pubblica*, a cura di SCAGLIARINI, Torino, 2019, p. 99. M. TAMPIERI, *L'intelligenza artificiale: una nuova sfida anche per le automobili*, in *Contr. impr.*, 2020, p. 732) – e del Regolamento UNECE R 79, che all'art. 5.16.1, consente di attivare lo sterzo con comando automatico entro il limite di velocità dei 12 km/h (v. I. FERRARI, *Analisi comparata in tema di responsabilità civile legata alla circolazione dei veicoli a guida autonoma*, cit., p. 99; A. DI ROSA, *Il legal framework internazionale ed europeo*, in *Smart Roads e driverless cars: tra diritto, tecnologie, etica pubblica*, cit., p. 65.). In questo scenario, il costante incedere delle innovazioni tecnologiche che imprimono rilevanti trasformazioni alla circolazione veicolare sta conducendo, inevitabilmente, verso un periodo di graduale transizione nel quale ai veicoli tradizionali si affiancheranno in misura crescente veicoli automatizzati con caratteristiche sempre più prossime a quelle dell'automazione totale dando vita ad un contesto nel quale emergerà una nuova tassonomia degli incidenti (v. K. S. ABRAHAM, R. L. RABIN, *Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era* (April 9, 2018), in *Virginia Law Review*, Vol. 105, 2019, Forthcoming; Stanford Public Law Working Paper, SSRN: <https://ssrn.com/abstract=3159525>, p. 44; M. GEISTFELD, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, in 105 *Calif. L. Rev.* 1611 (2018), p. 1635. A. ALBANESE, *La responsabilità civile per i danni da circolazione di veicoli ad elevata automazione*, in *Eur. e dir. priv.*, 2019, p. 995). A quelli che vedranno coinvolti veicoli tradizionali, si aggiungeranno quelli tra veicoli tradizionali e veicoli automatizzati, quelli tra soli veicoli automatizzati, quelli in cui i veicoli automatizzati provocheranno danni a pedoni e ciclisti, infine quelli in cui il veicolo automatizzato arrecherà un danno solamente ai suoi occupanti (c.d. *one-car collision*).

¹⁰ Cfr. V. ILKOVÁ, A. ILKA, *Legal aspects of autonomous vehicles - An overview*, in *21st International Conference on Process Control (PC)*, 2017, pp. 428 ss.

¹¹ J. WISMANS, S. SELPI, M. THYNELL, G. LINDBERG, *Economics of Road Safety - What does it imply under the 2030 Agenda for Sustainable Development?*, in <https://>

www.uncrd.or.jp/content/documents/4903Final%20background%20paper%20for%20EST%20Plenary%20Session%2010.pdf

¹² L'entrata in vigore delle disposizioni contenute nel Reg. UE 2019/2144 del Parlamento europeo e del Consiglio del 27 novembre 2019 comporta l'obbligo di dotare i veicoli a motore di sistemi avanzati quali quelli di adattamento intelligente della velocità [art. 6 lett. a) Reg. UE 2019/2144], interfaccia di installazione di dispositivi di tipo *alcolock* [art. 6, lett. b), Reg. UE 2019/2144], avviso della disattenzione e della stanchezza del conducente [art. 6, lett. c), Reg. UE 2019/2144], avviso avanzato di distrazione del conducente [art. 6, lett. d), Reg. UE 2019/2144], segnalazione di arresto di emergenza [art. 6, lett. e), Reg. UE 2019/2144], rilevamento in retromarcia [art. 6, lett. f), Reg. UE 2019/2144], e, infine, del registratore di dati di evento [art. 6, lett. g), Reg. (UE) 2019/2144]. Una simile dotazione si diffonderà nel parco circolante progressivamente in quanto in una prima fase, a partire dal 6 luglio 2022, essa diverrà obbligatoria per le auto ed i veicoli commerciali leggeri di nuova omologazione, quindi, dal 7 luglio 2024 sarà obbligatoria su auto e veicoli commerciali leggeri di nuova immatricolazione, infine nel 2029 interesserà anche i c.d. mezzi pesanti. Si aprirà, pertanto, una lunga fase transitoria nel corso della quale coesisteranno veicoli caratterizzati da livelli assai differenziati di sicurezza e di affidabilità in ordine alla possibilità di fornire la prova della dinamica degli incidenti. Il progressivo rinnovamento del parco circolante, attualmente composto da veicoli tradizionali, vedrà accrescersi nel tempo il numero di veicoli dotati dei dispositivi contemplati dall'art. 6 Reg. (UE) 2019/2144) e dall'*Event Data Recorder*. In argomento E. AL MUREDEN, *Event data recorder e advanced driver assistance systems: la "spinta gentile" verso la mobilità del futuro*, in questa Rivista, 2022, pp. 390 ss.

¹³ V. ancora I. FERRARI, *Analisi comparata in tema di responsabilità civile legata alla circolazione dei veicoli a guida autonoma*, cit., p. 99; M. TAMPIERI, *L'intelligenza artificiale: una nuova sfida anche per le automobili*, cit., p. 732; A. DI ROSA, *Il legal framework internazionale ed europeo*, cit., p. 65.

¹⁴ Il problema, analizzato nel contesto europeo già a partire dal 2005 (VAN WEES, BROOKHUIS, *Product liability for ADAS; legal and human factors perspectives*, EJTIIR, 5, no. 4 (2005), p. 357), ha assunto in tempi recenti una crescente rilevanza con riferimento all'ordinamento statunitense (cfr. K. S. ABRAHAM, R. L. RABIN, *Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era*, cit., p. 8), in cui si pone in luce l'esigenza di far fronte ad un significativo periodo di transizione nel quale la persistente prevalenza di automobili con guida tradizionale condurrà a mantenere inalterate le attuali regole che governano la responsabilità civile; regole che – secondo gli

AA. – dovranno costituire oggetto di una profonda revisione solo nel momento in cui la circolazione di veicoli automatizzati e raggiungerà una misura pari al 25% del parco circolante.

¹⁵ Sulla previsione contenuta nell'ultimo comma dell'art. 2054 c.c. e sui complessi rapporti intercorrenti tra la responsabilità del proprietario e quella del fabbricante G. ALPA, *Costruzione di autoveicoli, clausole di esonero e responsabilità dell'impresa. Per una diversa lettura dell'articolo 2054, ultimo comma, codice civile*, cit., 1975, I, c. 751, il quale – nell'ambito di un'analitica ricostruzione della disciplina, della sua *ratio* e delle modificazioni complessive del quadro normativo in materia di risarcimento dei danni provocati dalla circolazione stradale – giunge a delineare una «responsabilità a carico dell'impresa» per gli incidenti cagionati dai difetti del veicolo, anticipando a metà degli anni Settanta gli approdi che trovarono una definitiva consacrazione solo alla fine degli anni Ottanta a seguito dell'intervento del legislatore attraverso l'attuazione della disciplina in materia di responsabilità del produttore (d.p.r. 24 maggio 1988, n. 224, attuativo della dir. 85/374/CEE). Per una ricostruzione dei rapporti tra la responsabilità *ex artt.* 2054, ult. comma, c.c. e la disciplina in materia di responsabilità del produttore C. CASTRONOVO, *La nuova responsabilità civile*, 4^a ed., Milano, 2018, p. 758; M. FRANZONI, *Dei fatti illeciti. Artt. 2043-2059*, in *Comm. cod. civ. Scialoja-Branca*, a cura di G. DE NOVA, Bologna-Roma, 2020, p. 465.

¹⁶ E. AL MUREDEN, *Sicurezza "ragionevole" degli autoveicoli e responsabilità del produttore nell'ordinamento italiano e negli Stati Uniti*, in *Contr. impr.*, 2012, p. 1505.

¹⁷ In questo senso appare condivisibile la riflessione di COLOMBA, *Driverless cars e intelligenza artificiale. Una questione di ordine pubblico: la liceità del brevetto*, in *Smart Roads e driverless cars: tra diritto, tecnologie, etica pubblica*, cit., p. 87, in part. p. 93, laddove osserva che «il perimetro della responsabilità civile sarebbe il meno colpito e potrebbe, anche *rebus sic stantibus*, fare faticosamente fronte a questo radicale mutamento d'assetto, richiamandosi a principi già affermati in materia».

¹⁸ La disciplina tecnica armonizzata che governa i requisiti di sicurezza di questo dispositivo è dettagliatamente compendiate nell'Addendum 156 – UN Regulation No. 157 *Date of entry into force as an annex to the 1958 Agreement: 22 January 2021 Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems (ECE/TRANS/WP.29/2020/81)*.

¹⁹ K. S. ABRAHAM, R. L. RABIN, *Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era*, cit., p. 5.

²⁰ Sotto questo profilo riveste particolare interesse la vicenda che sta interessando la commercializzazione dei veicoli Tesla (<https://www.tomshw.it/>

[automotive/tesla-guida-autonoma-la-vittoria-in-tribunale-in-germania/](#)) e la definizione di alcune funzionalità che ricorrendo ai termini *Autopilot* e *Full Self-Driving*, Possono ingenerare l'erronea convinzione dell'utilizzatore di poter fare affidamento su un sistema di guida completamente automatizzato ed affidabile.

²¹ In definitiva, pertanto, si può affermare che il ricorso a sistemi parzialmente automatizzati non presenta dal punto di vista legale profili di differenziazione rispetto alle situazioni nelle quali sono utilizzati sistemi di assistenza al guidatore (servofreno, servosterzo, ABS) in quanto permane in ogni caso la necessità di un costante monitoraggio e di interventi correttivi in caso di errori. In questo senso M. GEISTFELD, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, cit., p. 1636; J. LEVY, *No Need to Reinvent the Wheel: Why Existing Liability Law Does Not Need to Be Preemptively Altered to Cope with the Debut of the Driverless Car*, in *J. Bus. Entrepreneurship & L.*, 2015, p. 360; K. S. ABRAHAM, R. L. RABIN, *Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era*, cit., p. 40, affermano che nel prossimo futuro il problema della diffusione di veicoli con livello di automazione 3 potrà porre principalmente problemi legati ad un malfunzionamento dell'algoritmo deputato a richiamare l'attenzione del conducente e a sollecitare un suo intervento. Poiché la responsabilità del produttore risulterebbe configurabile solo sotto questo profilo, è possibile concludere che anche nell'ottica della diffusione di veicoli di livello 3 non sia necessario procedere ad una modifica radicale delle norme che attualmente governano la responsabilità civile. Nel contesto italiano il problema di individuare regole capaci di rispondere alle nuove esigenze generate dalla transizione dal modello di circolazione fondato sulla guida della persona a quello della guida automatica è analizzato da U. RUFFOLO, *Self-driving car, auto driverless e responsabilità*, in *Intelligenza artificiale e responsabilità*, a cura di U. RUFFOLO, Milano, 2017, p. 39, il quale lusinga la possibilità di ricorrere alla disciplina contemplata all'art. 2050 c.c. in materia di attività pericolose sottolineando i profili di pericolosità specifica che caratterizzano la guida altamente automatizzata. In senso contrario A. DAVOLA e R. PARDOLESI, *In viaggio col robot: verso nuovi orizzonti della r.c. auto ("driverless")?*, in *Danno e resp.*, 2017, p. 625, escludono la possibilità di dare applicazione all'art. 2050 c.c. in quanto, aderendo a questa lettura, «si finirebbe per qualificare come pericolosa un'attività (la guida automatizzata), la quale, se conforme alle regole della tecnica, è paradossalmente più sicura della normale attività di guida "umana"»; considerazioni in parte analoghe riecheggiano in I. FERRARI, *Analisi comparata in tema di responsabilità civile legata alla circolazione dei veicoli a guida autonoma*, cit., p. 110, la quale osserva che, eccezion fatta

per il Regno Unito, «negli Stati in cui è stata autorizzata per via normativa la sperimentazione dei veicoli a guida autonoma sono stati sensibilmente incrementati i massimali assicurativi». Una simile scelta viene osservata non tanto nella prospettiva del «riconoscimento di maggior pericolosità dei veicoli autonomi», ma, piuttosto, alla stregua di una misura volta a facilitare l'accettazione della sperimentazione da parte della collettività.

²² Sulla *preemption*, ossia sulla prevalenza delle norme federali rispetto a quelle nazionali, v. T. O. MCGARITY, *The Preemption War: When Federal Bureaucracies Trump Local Juries*, New Haven London, 2008; A. UNTEREINER, *The preemption defense in tort actions: Law Strategy and Practice* Washington D.C., 2008; J. O'REILLY, *Federal Preemption of State and Local Law*, cit.; V. D. DINH, *Rassessing the law of Preemption*, 88 *Geo L.J.* 2085 (2000); J. GOLDSMITH, *Stature Foreign Affairs Preemption*, *Sup. Ct. Rev.* 175 (2000); C. M. SHARKEY, *Products Liability Preemption: an Institutional Approach*, 76 *Geo. Wash. L. Rev.*, 449 (2008); M. J. DAVIS, *On Restating Products Liability Preemption*, 74 *Brooklyn L. Rev.* 759 (2009).

²³ M. GEISTFELD, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, in 105 *Calif. L. Rev.* 1611 (2018), p. 1674, sottolinea la necessità di mettere le imprese che effettuano ingenti investimenti in questa tecnologia nella condizione di calcolare con adeguata precisione i costi e i margini di convenienza delle attività da avviare.

²⁴ Per una più diffusa in illustrazione del problema del danno da prodotto conforme E. AL MUREDEN, *Product safety e product liability nella prospettiva del danno da prodotto conforme*, in *La responsabilità del produttore*, a cura di ALPA, Milano, 2019, p. 489.

²⁵ G. CALABRESI e E. AL MUREDEN, *Driverless cars. Intelligenza artificiale futuro della mobilità*, Bologna, 2021, p. 123.

²⁶ K. S. ABRAHAM, R. L. RABIN, *Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era*, cit., p. 8.

²⁷ Con riferimento all' *Event Data Recorder* (art. 6, lett. g), Reg. 2019/2144/UE) è previsto un rinvio al reg. UN ECE R 160 nel quale sono indicati i parametri che devono essere registrati, unitamente a parametri tecnici come periodo di registrazione, risoluzione e accuratezza del dato, frequenza di campionamento, e intervallo minimo. Sebbene questo dettagliato elenco contenga una serie di parametri concernenti il funzionamento di ABS, airbag, pretensionamento delle cinture, attivazione del freno di servizio, angoli di beccheggio e rollio, angolo di sterzo, nonché dati antropometrici relativi a guidatore e passeggero, limitatamente a corporatura e peso, non viene fatto alcun riferimento ad altri rilevanti parametri quali quelli relativi a veicoli terzi o ad infra-

strutture, ad eventuali passeggeri posteriori o a pedoni. Non compaiono, inoltre, dati sulla diagnostica di bordo quali quelli relativi alla pressione e temperatura gomme, stato degli organi motore e distribuzione, deformazioni meccaniche, ecc. A queste osservazioni deve aggiungersi che il periodo di registrazione indicato dalla disciplina normativa consente l'osservazione di una finestra temporale di soli 10 secondi polarizzata sullo scontro: gli ultimi 5 secondi prima dello scontro e i primi 5 successivi. Alla luce di queste osservazioni, pertanto, appare auspicabile un ulteriore sviluppo del sistema dell' *Event Data Recorder* che consenta di osservare una maggiore quantità di parametri, di registrare interazioni maggiormente complesse e, in definitiva, di consentire un'interazione tra tecnica e disciplina legislativa improntata ad un rapporto di efficace sinergia.

Sostenibilità e innovazione nell'attività bancaria: il conto base come soluzione per chi abbia ridotte capacità cognitive

MARCO CARLIZZI

SOMMARIO: 1. Premessa. - 2. La trasformazione digitale delle banche. - 3. L'aumento del numero degli anziani ed il loro rapporto col digitale. - 4. Sostenibilità e finanza: a) dall'Agenda 2030 ai Regolamenti 2019/1288, 2020/852 e 2022/1288. - 5. *Segue*: - b) la sostenibilità nell'attività bancaria e le *Guidelines on Loan Origination and Monitoring* EBA. - 6. Il "Conto di base" *ex art- 126-noviesdecies* TUB. - 7. Conclusioni: il "Conto di base" come possibile strumento per banche socialmente sostenibili.

1. Premessa

"Il maggiore ricorso alle innovazioni tecnologiche potrà apportare significativi benefici agli operatori, agli intermediari e, in prospettiva, a imprese e famiglie".

Questa frase, che si attaglia invero a moltissimi settori industriali, è invece da attribuire al Governatore della Banca d'Italia ed è stata pronunciata nell'ultimo intervento all'ASSIOM Forex il 12 febbraio 2022; è, infatti, uno dei *leitmotiv* del settore bancario degli ultimi dieci anni, nei quali le trasformazioni imposte dal cambiamento tecnologico e in particolare dall'innovazione digitale hanno profondamente modificato gli assetti organizzativi di queste imprese, nonché le forme di distribuzione dei loro servizi finanziari¹.

A questo tema si affianca normalmente l'analisi dei problemi che ciò ha comportato, dalla *cyber security* alla concentrazione in poche mani dei sistemi informativi bancari, ossia della tecnologia necessaria per tutte le operazioni bancarie (c.d. *core*

banking system)², mentre raramente si affronta il tema dell'impatto che tale trasformazione ha avuto ed ha sul popolo degli utenti e dei consumatori con ridotte capacità cognitive, come gli anziani³, che sono statisticamente meno alfabetizzati tecnologicamente e che hanno di conseguenza grandi difficoltà di utilizzo dei servizi bancari digitali.

È bene chiarire, sin da principio, che il tema non si pone solo per gli “anziani” perché riguarda chiunque si trovi ad avere una ridotta capacità cognitiva (ad es. a seguito di un trauma o una malattia) e non riguarda nemmeno tutte le persone anziane perché è stato provato che almeno un 52 per cento⁴ di quest'ultime sono in realtà in certi casi pienamente in grado di affrontare le sfide che la tecnologia mette loro davanti.

In generale, però, il tema è molto grave, dato che la popolazione anziana in Italia è in continuo aumento e che è nozione di comune esperienza che l'accesso a tutti i servizi offerti dagli intermediari finanziari *on line*, o attraverso applicazioni proprietarie della singola banca, è diventata una necessità e abbisogna di una capacità cognitiva e di attenzione che con l'età man mano si perde.

D'altra parte, con l'oramai nota Agenda 2030 delle Nazioni Unite per lo sviluppo sostenibile del 25 settembre 2015 e il conseguente Accordo di Parigi del 12 dicembre 2015 sul cambiamento climatico⁵, i governi di tutto il mondo si sono assunti impegni precisi a favore dell'obiettivo di un'economia e una società più sostenibili, individuando 17 nuovi Obiettivi per lo Sviluppo Sostenibile (*Sustainable Development Goals*, “SDG”) con i 169 traguardi ad essi associati⁶.

All'interno della suddetta Risoluzione dell'Assemblea Generale delle Nazioni Unite, in diverse occasioni si fa riferimento agli anziani come una delle categorie di persone che si trovano in una situazione di maggior bisogno e poi all'interno dell'obiettivo n. 8 (“lavoro dignitoso e crescita economica”) si afferma che uno dei traguardi da raggiungere è quello di: “Rafforzare la capacità degli

istituti finanziari interni per incoraggiare e aumentare l'utilizzo di servizi bancari, assicurativi e finanziari *per tutti*" [corsivo nostro].

Ecco dunque che la cerniera tra sistema bancario, soggetti vulnerabili e SDG si chiude e mostra come il tema debba essere necessariamente trattato.

Invero il legislatore, prima europeo e poi domestico, si era già posto il problema della necessità di rendere accessibile a talune categorie di consumatori i conti di pagamento, inserendo nel 2017 all'interno del Testo Unico Bancario, il Capo II-ter "Disposizioni particolari relative ai conti di pagamento" disciplinando in particolare, dall'art. 126-*noviesdecies* in poi, il cosiddetto "Conto di base", un conto di pagamento denominato in euro che è - a determinate condizioni - un vero e proprio diritto del consumatore.

Con il seguente lavoro si intende affermare che il Conto di base può essere una soluzione per coniugare l'obbiettivo della sostenibilità - come sopra intesa - con i diritti dei correntisti con ridotte capacità cognitive⁷, diritti da esercitarsi nelle forme di volta in volta individuate dall'inarrestabile evoluzione tecnologica nell'usufruire dei servizi bancari e finanziari.

2. La trasformazione digitale delle banche

Il mondo dei servizi bancari - per quel che qui interessa⁸ - si è sicuramente caratterizzato negli ultimi anni per due fenomeni: la chiusura di sportelli e filiali in tutta Italia e la spersonalizzazione della sua attività con i correntisti attraverso un uso massiccio di servizi *on line*.

I dati mostrano innanzitutto come negli ultimi 10 anni gli sportelli e dipendenti delle banche italiane si sono drasticamente ridotti⁹. In particolare dal 2012 al 2021 c'è stato un calo di dipendenti di 45.613 unità (da 315.238 a 269.625) pari al 14,47 per cento mentre - ancor più impressionante - nel medesimo periodo, si è passati da 32.881 sportelli operativi a 21.650 (circa il 50 per cento

dei quali appartenenti a banche di maggiore dimensione) con una perdita quindi di “punti vendita” pari a 11.231, ossia più del 34 per cento¹⁰; tutto ciò ha fatto il paio con la riduzione del numero delle banche che sono passate da 740 nel 2001 a 456 al 3.12.2021 ossia circa il 38 per cento delle banche in meno¹¹.

Il contesto è dunque chiaro: c'è stata una riorganizzazione del modello distributivo dei prodotti e servizi bancari che ha comportato – sempre per quel che qui interessa – una riduzione di circa un terzo delle filiali e dunque un allontanamento “fisico” delle banche dai propri correntisti. I clienti della banca, dunque, hanno per così dire “subito” questa riorganizzazione, dovendosi adattare al nuovo stato di fatto e non potendo (ovviamente) in nessun modo opporsi ad esso.

Nello stesso tempo l'ICT (*Information and Communication Technology*) è diventato il vero cuore pulsante delle banche e ciò forse ha anche in parte causato quel fenomeno di concentrazione che abbiamo sopra descritto¹².

L'impatto dell'innovazione e della tecnologia sul sistema bancario è stato radicale: già oltre vent'anni fa la Banca Centrale Europea analizzava approfonditamente il tema affermando che l'ICT nelle banche avrebbe, da un lato, ridotto i costi associati alla gestione delle informazioni attraverso processi automatizzati che avrebbero sostituito i sistemi basati sul lavoro manuale e sui documenti cartacei e, dall'altro, modificato il modo attraverso il quale la clientela avrebbe avuto accesso ai servizi e prodotti dell'istituto finanziario, ossia andando verso l'accesso da remoto a tali servizi (c.d. “*remote banking*”)¹³.

Ciò ha comportato, anche a livello regolatorio, la presa di coscienza dell'importanza del tema e, nel 2015, veniva aggiunto alla circolare 285 del 17 dicembre 2013 (Parte Prima, Titolo IV) il nuovo capitolo “Il sistema informativo” (Capitolo 4), nel quale ora vengono disciplinati nel dettaglio i compiti che su tale tema ha l'organo con funzioni di supervisione strategica e l'organo

con funzioni di gestione e, al contempo, si precisa l'organizzazione della funzione ICT, della sicurezza informatica e del rischio informatico (c.d. "IT Governance")¹⁴.

Ciò che qui interessa mettere in luce è proprio lo sviluppo del cosiddetto *remote banking*, ossia quella modalità di accesso e generale utilizzo del proprio conto corrente che avviene da remoto, attraverso un accesso *internet*, ovvero attraverso una applicazione proprietaria della banca che poi a sua volta dà accesso a diverse funzionalità della posizione personale. Ciò avviene, com'è esperienza comune, attraverso delle credenziali di accesso che sono spesso la combinazione di più codici di autenticazione attraverso i quali il sistema riconosce il titolare del conto¹⁵.

Il percorso non ha origini particolarmente recenti ma è iniziato con l'introduzione delle prime *Automated Teller Machine* (ATM) negli anni Sessanta, per poi proseguire negli anni novanta con l'avvio dei sistemi di trading *on line*, la diffusione dell'*internet banking* a partire dagli anni duemila¹⁶ per poi approdare all'ultima frontiera dell'*Open Banking*¹⁷, che ha avuto pieno dispiegamento con la Direttiva PSD2¹⁸.

D'altra parte, l'importanza per le banche della tecnologia appare evidente dall'analisi della Banca d'Italia, *Indagine Fintech nel sistema finanziario italiano*¹⁹, che ha rilevato come la spesa in tecnologie *fintech* è passata in questi anni da 233 milioni (2017-2018) a 456 milioni (2019-2020) fino a 530 milioni (2021-2022) e ciò vuol dire che in 6 anni l'importo degli investimenti si sono più che raddoppiati²⁰.

3. L'aumento del numero degli anziani ed il loro rapporto col digitale

Al 1° gennaio 2022 gli individui residenti in Italia dai 65 anni di età in su ammontavano a 14 milioni e 46 mila pari al 23,8 per cento del totale della popolazione²¹ e si registra un costante

trend di crescita²², in parte correlato anche al costante aumento della speranza di vita alla nascita²³, insieme alla oramai cronica ridotta fecondità degli italiani²⁴.

Sempre ai fini che qui interessa, va segnalato che nel 2018, sul totale degli anziani, circa uno su tre viveva da solo (in aumento rispetto al 2017) e oltre tre anziani soli su quattro avevano un titolo di studio che non superava la licenza media: la quota dei poco istruiti raggiungeva l'80,7 per cento tra le donne e l'85 per cento tra coloro che avevano più di 75 anni²⁵. Quello degli anziani con un basso livello di istruzione è invero un *trend* in diminuzione: infatti, nel 2020 meno di un anziano su due aveva un titolo di studio molto basso che non superava la licenza elementare²⁶.

Avvicinandoci poi al tema che ci occupa, e tenendo a mente che l'apprendimento permanente durante tutto l'arco della vita (c.d. *lifelong learning*) assume sempre maggiore importanza soprattutto in relazione ai forti cambiamenti in atto nella nostra società (e rientra infatti tra gli obiettivi strategici di Europa 2020), se si considera la classe di età 65 -74enni il coinvolgimento in attività formative arriva all'1,9 per cento e dunque ad un tasso particolarmente basso²⁷.

Viene dunque qui in rilievo il cosiddetto *digital divide* “che contraddistingue la popolazione anziana, sostanzialmente quasi esclusa dai benefici derivanti dall'applicazione di tecnologie informatiche in un numero crescente di campi”²⁸.

Insomma, quello che emerge molto chiaramente è che, da un lato, il numero degli anziani in Italia è un numero considerevole della popolazione italiana e per di più in continuo aumento e, dall'altro, proprio gli anziani (*rectius*: i soggetti con ridotta capacità cognitiva) sono tra i soggetti che più hanno difficoltà a stare al passo con l'innovazione tecnologica.

D'altra parte, tanti sono gli studi sul rapporto tra *internet* e l'età anagrafica degli individui²⁹ ed in particolare sull'uso di *internet* da

parte degli anziani che dimostra un “divario marcato tra le generazioni”³⁰, tanto da poter dire che, se ci si focalizza sulle famiglie di soli anziani, ovvero di quelle composte da persone di 65 anni e più, ben il 67,4 per cento di loro non sa usare *internet*³¹.

Sempre con riferimento all'utilizzo di *internet*, altri studi ci informano che il numero delle famiglie italiane che lo usano nell'ambito delle scelte economico-finanziarie oscilla tra l'8 per cento nel caso della negoziazione di cripto-valute e il 52 per cento per l'*online banking*³²: il rapporto tra il depositante-correntista-investitore e la propria banca è dunque disintermediato e i clienti, grazie ai sistemi di accesso a distanza al proprio conto, possono operare direttamente sui propri fondi effettuando tutte le operazioni di cui hanno bisogno³³.

A fronte di questi dati, però, non sembra ci sia altrettanta attenzione sul rapporto tra gli anziani e le banche, sulla loro capacità di interfacciarsi con quella sopra descritta “trasformazione digitale” che ha interessato il sistema bancario e che è destinata in futuro ad aumentare.

4. Sostenibilità e finanza: a) dall'Agenda 2030 ai Regolamenti 2019/2088, 2020/852 e 2022/1288

Come è noto, con l'Accordo di Parigi del 2015 sul cambiamento climatico³⁴ e l'Agenda 2030 delle Nazioni Unite per lo sviluppo sostenibile³⁵, si è cercato a livello globale di dare una risposta ai cambiamenti climatici, oramai oggettivi, il tutto attraverso una transizione verso un'economia a basse emissioni di carbonio, con l'obiettivo di mantenere l'aumento della temperatura media mondiale ben al di sotto di 2° C rispetto ai livelli preindustriali³⁶.

Ebbene, la finanza è stata individuata come una delle leve principali che i governi possono utilizzare per mettere in atto l'Accordo di Parigi, visto che la messa a disposizione di prodotti finanziari che perseguono obiettivi ecosostenibili è un modo ef-

ficace di incanalare gli investimenti privati verso le attività sostenibili³⁷.

Possiamo dire che dal punto di vista normativo, da un lato, abbiamo assistito a una proliferazione della normativa sulla finanza sostenibile e quindi sulla c.d. tassonomia di tale finanza e, dall'altro, ma non con la stessa velocità, anche ad un coinvolgimento delle banche in questo percorso attraverso orientamenti in materia di concessione e monitoraggio dei prestiti (le c.d. *Guidelines on Loan Origination and Monitoring* del 29 maggio 2020 dell'EBA)³⁸.

Partendo però dalla Finanza Sostenibile, che certamente è quella che più di tutti è stata oggetto di questo processo regolatorio, il punto di partenza è stata la constatazione che la mancanza di regole comuni provoca certamente divergenza degli standard di informativa, distorsioni della concorrenza e confusione tra gli investitori finali, oltre a quella che viene comunemente definita come “*greenwashing*”³⁹, ossia una pratica che consiste “nell’ottenere un vantaggio sulla concorrenza in modo sleale, commercializzando un prodotto finanziario come eco-compatibile quando in realtà gli standard ambientali di base non sono soddisfatti”⁴⁰.

Invero, il percorso di gestazione di questa normativa è stato piuttosto lungo. Ricordiamo infatti che nel 2016, la Commissione Europea ha incaricato un gruppo di esperti in materia di finanza sostenibile perché predisponesse un elenco di raccomandazioni rivolte al settore finanziario, con l’obiettivo principale di condurre uno studio sullo stato dell’arte della finanza etica all’interno della cornice eurounitaria e, di riflesso, di sostenere la transizione verso un’economia a basse emissioni di carbonio⁴¹. La relazione finale, presentata il 31 gennaio 2018, ha delineato le sfide e le opportunità che l’UE doveva affrontare nell’elaborazione di una nuova politica per la finanza sostenibile; in particolare, il *report* individuava i modi in cui il settore finanziario poteva entrare nuovamente in contatto con l’economia reale per soste-

nere la transizione verso un'economia definita "circolare" e più efficiente sotto il profilo della gestione delle sue risorse⁴².

Interessante notare che l'accento è posto proprio sulla necessità che tutti gli investimenti "sostenibili" siano concepiti come azioni "a lungo termine", essendo il rischio di danni irreparabili massimo laddove, a fronte di scelte di investimento sostenibile, si opti nel breve-medio periodo per bruschi cambi di direzione e stravolgimento delle politiche sino a quel momento realizzate. Peraltro, secondo gli esperti, orientare i flussi di investimento verso progetti sostenibili a lungo termine consentirebbe anche un miglioramento della stabilità del sistema finanziario.

Ebbene, se tutto questo era previsto nel *Final Report* dell'*High Level Expert Group*, la Commissione Europea, l'8 marzo 2018 ha proposto un *Action Plan on sustainable finance*⁴³, una strategia dell'Unione in materia di finanza sostenibile, delineando i lavori e le iniziative future nelle quali coinvolgere tutti i soggetti interessati del sistema finanziario ed indicando esplicitamente delle scadenze per ciascuna "azione" da intraprendere.

Il primo punto sottolineato sia dal *Final Report* che dall'*Action Plan* era quello di creare un linguaggio comune per la finanza sostenibile, ovvero un sistema unificato di classificazione dell'UE o "tassonomia" per definire ciò che è sostenibile e identificare gli ambiti in cui gli investimenti sostenibili possono incidere maggiormente: ciò che è stato fatto con i Regolamenti (UE)2019/2088, (UE)2020/852 e (UE)2022/1288.

Con il Regolamento (UE) 2019/2088 del Parlamento Europeo e del Consiglio del 27 novembre 2019 relativo all'informativa sulla sostenibilità nel settore dei servizi finanziari⁴⁴, si è inteso implementare un'informativa destinata agli investitori finali sui rischi di sostenibilità e sulla considerazione degli effetti negativi per la sostenibilità degli investimenti, cercando di evitare divergenza degli standard di informativa, distorsioni della concorrenza e confusione tra gli investitori finali.

Innanzitutto, il Regolamento definisce il «rischio di sostenibilità» ossia “un evento o una condizione di tipo ambientale, sociale o di governance che, se si verifica, potrebbe provocare un significativo impatto negativo sul valore dell’investimento”⁴⁵.

L’obiettivo finale del regolamento 2088 è quindi quello di rafforzare la protezione degli investitori finali migliorando l’informativa a loro destinata: l’obiettivo di raggiungere un’economia in linea con gli obiettivi dell’Agenda 2030 è dunque declinata nella finanza sostenibile attraverso una attenta e dettagliata informazione ai risparmiatori.

Gli operatori devono quindi specificare nelle loro politiche in che modo integrano i rischi di sostenibilità e pubblicare dette politiche: per *rischio di sostenibilità* si intende un evento o una condizione di tipo ambientale, sociale e di governance che, se si verifica, potrebbe provocare un significativo impatto negativo sul valore dell’investimento.

Fondamentale nel Regolamento 2088 è la declinazione di quelli che vengono chiamati “livelli di ambizione”: partendo dalla constatazione che ad oggi ci sono diversi prodotti con diversi livelli di ambizione, il Regolamento 2088 distingue tra (i) Prodotti finanziari che *promuovono caratteristiche ambientali e sociali* e (ii) Prodotti finanziari che *hanno come obiettivo quello di produrre effetti positivi per l’ambiente e la società*.⁴⁶

Per i primi, va comunicato in che modo l’indice designato sia quello della sostenibilità e sia allineato a dette caratteristiche ovvero come, per i prodotti che non hanno un indice, vengano rispettate le caratteristiche di sostenibilità dei prodotti finanziari; per i secondi, i partecipanti ai mercati finanziari devono comunicare il parametro di riferimento utilizzato per misurare le prestazioni in termini di sostenibilità nonché, laddove non ci sia un parametro di riferimento, spiegare come viene conseguito l’obiettivo di sostenibilità.

Fondamentale, ai fini di quanto qui interessa, va ricordata proprio la definizione prevista dall'art. 2 lett. 17 di «investimento sostenibile»: investimento in un'attività economica che contribuisce a un *obiettivo ambientale*, misurato, ad esempio, mediante indicatori chiave di efficienza delle risorse concernenti l'impiego di energia, l'impiego di energie rinnovabili, l'utilizzo di materie prime e di risorse idriche e l'uso del suolo, la produzione di rifiuti, le emissioni di gas a effetto serra nonché l'impatto sulla biodiversità e l'economia circolare o un investimento in un'attività economica che contribuisce a un *obiettivo sociale*, in particolare un investimento che contribuisce alla lotta contro la disuguaglianza, o che promuove la coesione sociale, l'integrazione sociale e le relazioni industriali, o un investimento in *capitale umano* o in comunità economicamente o socialmente svantaggiate, il tutto *a condizione che tali investimenti non arrechino un danno significativo* a nessuno di tali obiettivi e che le imprese che beneficiano di tali investimenti rispettino prassi di buona governance, in particolare per quanto riguarda strutture di gestione solide, relazioni con il personale, remunerazione del personale e rispetto degli obblighi fiscali.

Come si vede, quindi, è definito sostenibile anche quell'investimento che contribuisce alla lotta contro la disuguaglianza o comunque un investimento in comunità economicamente o socialmente svantaggiate.

Ecco dunque un punto che vale la pena sottolineare: un investimento che abbia come obiettivo quello di integrare la comunità dei soggetti con ridotte capacità cognitive all'interno della più ampia collettività dei "normodotati", potrebbe definirsi un investimento sostenibile ai sensi del regolamento 2088 e dunque attrarre capitali a ciò destinati.

Successivamente, con il Regolamento (UE)2020/852 del Parlamento Europeo e del Consiglio del 18 giugno 2020, relativo all'istituzione di un quadro che favorisca gli investimenti soste-

nibili e recante la modifica del Regolamento (UE)2019/2088, il legislatore europeo ha inteso definire ciò che si può considerare un'attività economica ecosostenibile al fine di individuare il grado di ecosostenibilità di un investimento⁴⁷.

Stabiliti gli obblighi di trasparenza degli investimenti ecosostenibili e di prodotti finanziari che promuovono caratteristiche ambientali delle informazioni precontrattuali e delle relazioni periodiche di regolamento, il Regolamento specifica, per tutti gli obiettivi ambientali, il significato del contributo sostanziale a ciascuno di essi, così come individua quale sia il “danno significativo agli obiettivi ambientali” (l'assenza del quale abbiamo visto essere il requisito essenziale dell'”investimento sostenibile”) e quali siano le garanzie minime di salvaguardia e i requisiti dei criteri di vaglio tecnico.

A chiudere il cerchio su questa materia è quindi stato emesso il Regolamento delegato (EU) 2022/1288 della Commissione del 6 aprile 2022⁴⁸, che integra il regolamento 2019/2088 per quanto riguarda le *norme tecniche di regolamentazione* che specificano: a) i dettagli del contenuto e della presentazione delle informazioni relative al principio “non arrecare un danno significativo” (così detto *do no significant harm*, DNSH), b) il contenuto, le metodologie e la presentazione delle informazioni relative agli indicatori di sostenibilità e gli effetti negativi per la sostenibilità e c) il contenuto e la presentazione delle informazioni relative alla promozione delle caratteristiche ambientali o sociali e degli obiettivi di investimento sostenibile nei documenti contrattuali, sui siti *web* e nelle relazioni periodiche.

Come espressamente dichiarato nel Regolamento, l'intento è sempre lo stesso: conseguire gli obiettivi dell'accordo di Parigi e ridurre in maniera significativa i rischi e gli impatti dei cambiamenti climatici.

Invero, il regolamento, molto complesso, è strutturato in cinque capi: (i) le disposizioni generali, (ii) la trasparenza circa gli ef-

fetti negativi sui fattori di sostenibilità (*Adverse Impacts on Sustainability Factors* - a sua volta suddiviso tra i partecipanti ai mercati e consulenti finanziari), (iii) l'informativa precontrattuale sul prodotto (a sua volta suddiviso tra la *promozione* delle caratteristiche ambientali e sociali e l'*obiettivo* di investimento sostenibile richiama a tal uopo gli artt. 8 e 9 del Regolamento 2019/2088, nonché prodotti con l'opzione di investimento), (iv) l'informativa sul prodotto pubblicata su web (anche qui distinte tra i prodotti finanziari che promuovono caratteristiche ambientali e sociali e quelli che hanno come obiettivo investimenti sostenibili), (v) l'informativa sul prodotto nelle relazioni periodiche (sempre con le medesime distinzioni di prodotto suddette) e quindi le disposizioni finali con una serie di allegati con i modelli di informativa da fornire⁴⁹.

5. *Segue*: b) la sostenibilità nell'attività bancaria e le *Guidelines on Loan Origination and Monitoring* EBA

Se questo è in estrema sintesi il panorama della complessa normativa sulla Finanza Sostenibile (che come visto include sia gli aspetti ambientali sia quelli della *governance* e dei diritti umani), diverso è stato lo sviluppo normativo per quanto riguarda gli obblighi ESG delle banche.

Per le banche, infatti, si è arrivati soltanto nel 2020 agli orientamenti dell'Associazione Bancaria Europea (EBA)⁵⁰ in materia di concessione e monitoraggio dei prestiti, c.d. *Guidelines on Loan Origination and Monitoring* del 29 maggio 2020, entrate in vigore a giugno 2021 con un periodo di transizione fino a giugno 2024⁵¹.

Gli orientamenti definiscono quindi la posizione dell'EBA in merito alle adeguate prassi di vigilanza all'interno del Sistema europeo di vigilanza finanziaria o alle modalità di applicazione del diritto dell'Unione in un particolare settore; nel caso di specie gli orientamenti trovano il loro prodromo nell'articolo 16 del regolamento (UE) n. 1093/2010⁵².

Le Guidelines, che si applicano a tutti gli istituti finanziari⁵³, seppur secondo il Principio di proporzionalità in relazione alle dimensioni dell'istituto e ai prodotti erogati⁵⁴, hanno adottato un approccio c.d. “ex-ante”, ossia il raggiungimento degli obiettivi della regolamentazione viene perseguito anzitutto “by design”, imponendo prassi gestionali che minimizzino il rischio di una nuova risalita degli stock dei c.d. *Non Performing Loans*. Insomma, il regolatore europeo, dopo anni di attenzione alla riduzione dei crediti deteriorati detenuti dalle banche (conseguenti alla grave crisi finanziaria del 2008), ha iniziato a studiare regolamenti volti a ridurre il rischio dell'attività creditizia svolta dagli istituti di credito ponendo grande attenzione sia alla fase di concessione dei prestiti che al loro successivo monitoraggio.

Oltre a notare che queste Guidelines sono in realtà molto prescrittive (“*rule-based*”) rispetto ai normali standard delle Guidelines EBA, quel che qui interessa sottolineare è l'introduzione dei fattori ESG all'interno delle politiche creditizie, sviluppata poi lungo tutto il processo, ossia dalla valutazione del rischio alle politiche creditizie e poi ancora alle politiche commerciali, alla concessione del credito e quindi alla gestione e monitoraggio: dunque lungo tutto il processo di valutazione e gestione del credito⁵⁵.

All'interno del paragrafo 4.3 (Politiche procedure relative al rischio di credito), in particolare al paragrafo 4.3.5, vengono quindi citati i fattori ESG partendo da questa premessa: “Gli enti dovrebbero incorporare i fattori ESG e i rischi ad essi associati nella loro propensione al rischio di credito, nelle politiche di gestione dei rischi e nelle politiche e procedure relative al rischio di credito, adottando un approccio olistico”.

La normativa bancaria, dunque, arriva ai fattori ESG attraverso gli orientamenti dell'EBA, inserendo d'imperio all'interno del processo del credito e della valutazione del merito creditizio i rischi di sostenibilità.

Vediamo però qui subito i limiti di questa normativa, perché nello stesso paragrafo dedicato ai “Fattori ESG” (e dunque in teoria a tutti e tre gli aspetti della sostenibilità: ambientale, sociale e di governo) si legge che: “Gli enti dovrebbero tenere conto dei rischi associati ai fattori ESG per le condizioni finanziarie dei mutuatari, e in particolare del potenziale impatto dei *fattori ambientali e del cambiamento climatico*, nella loro propensione al rischio di credito e nelle politiche e procedure ad esso relative. I *rischi del cambiamento climatico* per le performance finanziarie dei clienti possono materializzarsi principalmente sotto forma di rischi fisici, come quelli che derivano dagli effetti tangibili del cambiamento climatico, compresi i rischi di responsabilità civile per aver contribuito al cambiamento climatico stesso, o i rischi di transizione, ad esempio quelli che derivano dalla transizione verso un’economia a basse emissioni di carbonio e resistente ai cambiamenti climatici. Inoltre, possono verificarsi altri rischi, quali cambiamenti delle preferenze del mercato e dei consumatori e rischi legali, che potrebbero influire sull’andamento delle attività sottostanti.”

Lo stesso paragrafo poi analizza il prestito sostenibile dal punto di vista ambientale (4.3.6) affermando che: “Gli enti che emettono o prevedono di emettere linee di credito sostenibili dal punto di vista ambientale dovrebbero indicare, nell’ambito delle loro politiche e procedure relative al rischio di credito, i dettagli specifici delle loro politiche e procedure di prestito sostenibile dal punto di vista ambientale, con riferimento alla concessione e al monitoraggio di tali linee di credito”; e, ancora, laddove nei paragrafi 5.2.5 e 5.2.6 relativi ai Prestiti a microimprese e piccole imprese e poi alle Medie e grandi imprese afferma che: “Gli enti dovrebbero valutare l’esposizione del cliente ai fattori ESG, *in particolare ai fattori ambientali* e all’impatto sul cambiamento climatico, e l’adeguatezza delle strategie di mitigazione, come specificate dal cliente”.

In conclusione, se è vero che gli obiettivi dell'Agenda 2030 ed i cosiddetti Fattori ESG sono entrati anche nel mondo delle banche attraverso queste Guidelines EBA, è altresì vero che la declinazione delle stesse, di fatto, punta solo e soltanto sui rischi climatici e ambientali tralasciando aspetti, anch'essi fondamentali, come il rispetto dei *diritti umani* in tutta la filiera produttiva o l'utilizzo di una *better governance* intesa non solo come insieme di regole di organizzazione degli organi sociali, ma anche come attenzione ad una gestione "giornaliera" dell'impresa che sia etica e sostenibile: insomma, non va analizzato solo *cosa* fa l'impresa ma anche *come* lo fa⁵⁶.

6. Il "Conto di base" ex art. 126-*noviesdecies* TUB

Analizzato dunque il fenomeno dei soggetti con ridotte capacità cognitive e del loro rapporto con le banche e avendo, in rapida sintesi, esposto i principi e le regole della finanza sostenibile e dei *Principi ESG* come enucleati all'interno della recente normativa bancaria europea (con tutti i limiti suesposti), è il momento qui di analizzare uno specifico strumento a disposizione delle banche italiane che, forse, interpretato alla luce dei *Principi ESG* sopra esposti, può essere il grimaldello attraverso il quale dare una soluzione ai problemi esposti in premessa.

In attuazione della direttiva 2014/92/UE (cosiddetta "PAD", *Payment Accounts Directive*) sulla "comparabilità delle spese relative al conto di pagamento, sul trasferimento del conto di pagamento e sull'accesso al conto di pagamento con caratteristiche di base", nonché in linea con le politiche europee di riduzione dell'uso del contante ai fini di una riduzione dei costi per la pubblica amministrazione e per agevolare la lotta all'evasione fiscale, con il decreto legislativo 15 marzo 2017, n. 37, sono stati introdotti all'interno del decreto legislativo 1° settembre 1993, n. 385 (Testo Unico Bancario - TUB), gli artt. 126-*decies* e ss. fa-

centi parti del Capo II-ter “Disposizioni particolari relative ai conti di pagamento”⁵⁷.

Con il decreto legislativo 37/2017, come implementato dal D.M. 3 maggio, 2018, n. 70, è stato dunque introdotto nel nostro ordinamento l’obbligo per le “banche, la società Poste italiane S.p.a. e gli altri prestatori di servizi di pagamento abilitati ad offrire servizi a valere su un conto di pagamento [...] un conto di pagamento denominato in euro con caratteristiche di base, «conto di base»”⁵⁸.

Viene dunque imposto ai prestatori di servizi di pagamento l’obbligo di avere tra i loro prodotti, e di conseguenza di offrirlo a chi ne faccia richiesta, anche il «conto di base» che abbia alcune caratteristiche.

Le caratteristiche di base consistono nell’includere, a fronte di un canone annuale onnicomprensivo, un numero di operazioni annue (definito dalla legge) effettuabili senza addebito di ulteriori spese.

Individuati, con il decreto attuativo, i profili di clientela ai quali il conto di base è destinato, un numero di operazioni sufficiente a coprire l’uso personale da parte del consumatore e le operazioni e i servizi inclusi nel conto di base (con espressa esclusione di aperture di credito e sconfinamenti), il TUB si premura di affermare che: “il titolare del conto di base può eseguire le operazioni avvalendosi, senza maggiori costi, dei *canali telematici* disponibili presso il prestatore di servizi di pagamento per i conti analoghi”⁵⁹.

Fin qui, dunque, si tratta di un obbligo per gli istituti bancari di mettere a disposizione della clientela uno speciale conto corrente che di fatto è limitato nell’operatività, ma è vantaggioso da un punto di vista economico in quanto prevede solo un canone annuale onnicomprensivo.

Ancora più interessante ai nostri fini è però l’art. 126-*vicies quater* del TUB, rubricato “Conti di base per particolari catego-

rie di consumatori”, attraverso il quale il legislatore obbliga gli istituti finanziari ad offrire il conto di base completamente senza spese a determinate “fasce di clientela socialmente svantaggiate e ai titolari di trattamenti pensionistici”.

Il D.M. 70/2018 ha poi individuato le fasce di clientela svantaggiate e titolari di trattamenti pensionistici utilizzando a tal uopo un parametro meramente economico, ossia richiamando per i primi un ISEE in corso di validità inferiore ad euro 11.600,00 e per i secondi un importo lordo annuo della pensione di euro 18.000,00⁶⁰.

Come si vede, tutta la normativa è improntata a favorire i soggetti meno abbienti, facilitandoli nell'uso di mezzi di pagamento tracciabili (perché una delle motivazioni se non la principale era questa) attraverso un conto di base che sia per i più bisognosi addirittura gratuito⁶¹; il legislatore si premura di specificare che, qualora il titolare del conto voglia avvalersi di canali telematici, questi non devono avere dei costi aggiuntivi, ma al contempo dimentica di prevedere che quei servizi di pagamento e quei canali telematici debbano essere accessibili al titolare del conto.

Lo stesso decreto ministeriale, però, nell'indicare la possibilità per gli istituti di pagamento di prevedere addebiti ulteriori per le operazioni non comprese o eccedenti il limite previsto, richiama espressamente il “rispetto dei criteri di ragionevolezza e coerenza con finalità di *inclusione finanziaria*” previsti dal medesimo atto⁶².

L'inclusione finanziaria è quindi espressamente prevista nel testo del decreto anche se viene declinata solo e soltanto da un punto di vista economico, mentre più opportuno sarebbe stato allargarne il senso includendo anche coloro che, seppur inizialmente presenti nel “mondo finanziario”, ne sono stati, loro malgrado, successivamente esclusi⁶³.

Eppure, la direttiva faceva riferimento ad una “economia moderna e più inclusiva” e alle “esigenze dei consumatori più vulnerabili”; ancora, al 3° considerando, affermava che: “Il corretto funzionamento del mercato interno e lo sviluppo di un'e-

conomia moderna e socialmente inclusiva dipende sempre più dalla prestazione universale di servizi di pagamento. La nuova legislazione in materia deve rientrare nell'ambito di una strategia economica intelligente per l'Unione, che deve efficacemente tenere conto delle esigenze dei consumatori più vulnerabili⁶⁴”.

Dunque la normativa europea parlava di “consumatori più vulnerabili”, non parlava soltanto di soggetti meno abbienti e, proprio per far sì che l'Europa arrivi a costruire “un'economia moderna e socialmente inclusiva” – per riprendere le parole della direttiva PAD –, non è pensabile che vengano esclusi dai servizi bancari i soggetti con ridotte capacità cognitive.

7. Conclusioni: il “Conto di base” come possibile strumento per banche socialmente sostenibili

Come abbiamo visto in apertura, l'attività bancaria ha subito nell'ultimo decennio una profonda trasformazione e ciò sia in relazione alla organizzazione interna sia in relazione al rapporto con la propria clientela. I *software* gestionali stanno man mano permeando tutte le funzioni aziendali tanto che la stessa normativa di vigilanza (la Circolare 285/2013) ha disciplinato appositamente il “sistema informativo” e il “rischio informatico (o ICT)”, affidando, ad esempio, all'organo con funzioni di supervisione strategica il compito di approvare le strategie di sviluppo del sistema informativo e il modello di riferimento per l'architettura del sistema informativo.

Questa informatizzazione dell'attività bancaria ha innanzitutto riguardato i processi interni della banca (dal processo del credito al sistema dei controlli), ma ha poi riguardato anche i rapporti con la clientela spostando sempre di più la relazione con il depositante *on line*, intermediata da un sito internet o una “app” che permette agli utenti dei servizi bancari di svolgere in autonomia le operazioni che prima faceva allo sportello.

Questo ha innanzitutto comportato, complici anche i processi di concentrazione societaria avvenuti, una riduzione negli ultimi 10 anni di più del 30 per cento degli sportelli presenti sul territorio italiano, ma soprattutto, per quel che qui interessa, la necessità per chiunque abbia un conto in banca di avere confidenza e capacità di gestire un computer o uno smartphone per poter essere “riconosciuti” dalla banca/sportello *on line* o poter operare sul proprio conto (con i meccanismi che oramai ben conosciamo di password da modificare periodicamente, di combinazioni tra password e OTP-*One Time Password* generate da token o da “app” dedicate, ecc.) facendo sì che coloro che, a causa delle ridotte capacità cognitive prodotte ad esempio dall'età, non siano riusciti ad adattarsi a queste modalità, sono oramai impossibilitati ad esercitare i propri diritti provenienti dal contratto bancario da loro a suo tempo sottoscritto e quindi impediti ad operare sul proprio conto.

Negli stessi anni, però, un lungo processo di analisi e presa di coscienza delle conseguenze dei cambiamenti climatici si è chiuso con un documento delle Nazioni Unite che pone degli obiettivi di sostenibilità a tutti gli Stati e che – con riferimento al tema qui trattato – ha affermato: “Le persone più deboli devono essere supportate. Tutti coloro che si trovano in una situazione di maggior bisogno vengono inclusi nell'Agenda: si tratta di bambini, giovani, persone diversamente abili [...], persone affette da HIV/AIDS, *anziani*, popolazioni indigene, rifugiati, sfollati e migranti” (n.23 delle dichiarazioni introduttive dell'Agenda 2030 per lo Sviluppo Sostenibile del 2015). Accanto al tema ambientale viene dunque posta l'attenzione ai temi della *Governance* delle società e dell'economia in generale e al tema *Social*, ossia l'attenzione alle persone e all'impatto non economico che ha un'azione economica (come abbiamo visto anche la categoria degli “anziani”).

Infatti, all'interno dell'Obiettivo 8 dell'Agenda 2030 “Incentivare una crescita economica duratura, inclusiva e sostenibile, un'occupazione piena e produttiva ed un lavoro dignitoso per

tutti” si legge, al punto 8.10: “Rafforzare la capacità degli *istituti finanziari* interni per incoraggiare e aumentare l'utilizzo di servizi bancari, assicurativi e finanziari *per tutti*”.

Con riferimento alle banche, questo processo di adattamento all'Agenda 2030 delle Nazioni Unite è passato prima attraverso la normazione della c.d. “finanza sostenibile”, in particolare col Regolamento SFDR (*Sustainable Finance Disclosure Regulation*, Regolamento (UE) 2019/2088) e quindi con le Linee Guide EBA, *Guidelines on Loan Origination and Monitoring*, che obbligano le banche a valutare il c.d. “Rischio ESG” nelle proprie politiche di credito e dunque, a cascata, a richiedere i dati ESG ai propri clienti e potenziali affidati, così mettendo in moto il meccanismo virtuoso, per tutti gli operatori di mercato, di valutare il proprio impatto ambientale, sociale e di governo.

Le conclusioni che vorremmo cercare di tirare a questo punto, al fine di coniugare l'innovazione che ha investito le banche con la sostenibilità “sociale” dettata dall'Agenda 2030, è la necessità di rileggere gli artt. 126-*noviesdecies* e segg. TUB in un'ottica diversa, non più solo quale strumento di inclusione finanziaria per i meno abbienti, ma altresì quale conto dedicato anche ai soggetti con minori capacità cognitive e agli anziani (quindi ugualmente uno strumento di inclusione finanziaria ma anche sociale).

La normativa sul Conto di base va infatti ora letta alla luce dei Principi ESG come declinati per l'attività bancaria dagli Orientamenti EBA (che riguardano in particolar modo i rischi di sostenibilità ambientale all'interno del processo del credito e dell'analisi del merito creditizio), dal Regolamento SFDR che nel definire «investimento sostenibile» (art. 2, lett. 17) cita gli investimenti “in *capitale umano* o in comunità economicamente o socialmente svantaggiate” e, ancor prima, dalla PAD (*Payment Accounts Directive*), Direttiva 2014/92/UE che, come abbiamo visto, parla di “consumatori più vulnerabili” e di una “economia moderna e socialmente inclusiva”⁶⁵.

Il Conto di Base deve dunque avere caratteristiche tali da renderlo accessibile e utilizzabile anche a tutti coloro (già clienti o meno) che abbiano capacità cognitive inferiori alla media, agli anziani: in questo senso le banche dovranno prevedere sistemi differenziati di accesso a questo tipo di conto, ad esempio utilizzando modelli di riconoscimento e autenticazione ad immissione vocale (c.d. impronta vocale⁶⁶) o in generale sistemi di riconoscimento biometrico o, ancora, prevedere per questo conto un rafforzamento dell'assistenza telefonica.

Così interpretato e implementato, il Conto di base potrebbe dunque essere lo strumento attraverso il quale l'innovazione viene coniugata alla sostenibilità nell'attività bancaria.

Note di chiusura

¹ In <https://www.bancaditalia.it/pubblicazioni/interventi-governatore/integov2022/FOREX-12-febbraio-2022-Visco.pdf>.

² Ma si pensi anche ai problemi della finanza decentralizzata – anche attraverso l'utilizzo della tecnologia dei registri distribuiti (Distributed Ledger Technology, DLT) e degli *smart contract* che consentono l'esecuzione di transazioni senza ricorrere a un intermediario o a un processo “centralizzato”, tema altresì trattato dal Governatore nell'intervento citato.

³ Diverse sono le definizioni di anziano che si trovano in letteratura; si va da quella “storica” che individua la soglia di 65 anni di età e che viene attribuita – probabilmente in maniera errata – a Otto Von Bismarck, a quella che divide le persone con più di 65 anni tra chi è in buone condizioni di salute, ha un buon inserimento sociale e disponibilità di risorse e dunque appartiene alla cosiddetta “terza età”, da coloro che invece dipendono da altri e si trovano in una condizione di decadenza fisica e che vengono quindi ricompresi nella cosiddetta “quarta età”; o ancora esiste una definizione di anzianità che distingue quattro sottogruppi, i “giovani anziani” (persone tra i 64 e i 74 anni), gli anziani (persone tra i 75 e gli 84 anni), i “grandi vecchi” (persone tra gli 85 e i 99 anni) ed infine i centenari. Si ricorda che a livello europeo i diritti degli anziani sono tutelati dalla Carta dei diritti fondamentali dell'Unione Europea che all'art. 25 afferma che: “*L'Unione riconosce e rispetta il diritto degli anziani di condurre una vita dignitosa e indipendente e di partecipare alla vita sociale e culturale*”; è chiaro che in questa “partecipazione” rientra anche quello allo sviluppo tecnologico.

Nel 2018, la Società Italiana di Gerontologia e Geriatria avanzò l'idea di aggiornare il concetto di anzianità, portando a 75 anni l'età ideale per definire una persona come “anziana”. “*Un 65enne di oggi*” – affermava la SIGG – “*ha la forma fisica e cognitiva di un 40-45enne di 30 anni fa e un 75enne quella di un individuo che aveva 55 anni nel 1980*”. Si può leggere l'intero paper, nel quale vengono fornite ampie motivazioni anche comparatistiche, all'indirizzo https://www.sigg.it/wp-content/uploads/2018/12/News_Quando-si-diventa-anziani.pdf.

⁴ Nel 2018, la quota di utenti regolari di Internet nella popolazione UE-28, tra 65 e 74 anni, era del 52 per cento. In Italia, nello specifico, il 34 per cento. Fonte: Rapporto Annuale 2019 – Approfondimento Gli anziani e le nuove tecnologie, p. 161, consultabile all'indirizzo <https://www.istat.it/storage/rapporto-annuale/2019/capitolo3.pdf>.

⁵ Cfr. [https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:22016A1019\(01\)](https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:22016A1019(01)).

⁶ Sulla scia dell'Agenda 2030, si è sviluppato un ampio dibattito che ha visto protagonista anche la categoria dei grandi imprenditori. Si veda ad es. *Transforming Capitalism for Sustainability*, K. SAKURADA, CEO, Sompo Holdings, Inc., Time, 7 febbraio, 2022 e più nel dettaglio, dello stesso autore, *Bushido Capitalism, the cold Hugh Read fine business for a Sostenibile Future*, LID Publishing, 2021, dove l'Autore esprime le tre vie attraverso le quali gestire un business che dovrà essere “good for the seller, good for buyer, good for the society”. L'Autore afferma che andrà guardato non solo l'interesse degli shareholders ma anche quello dei multi-stakeholders: se è vero che nel 2021 la capitalizzazione delle prime cinque società del mercato americano era pari a quella delle 2170 società del first Section of Tokyo Stock Exchange (dove ad esempio ci sono società di assistenza sanitaria), questo fa capire come non è possibile che il valore di quelle cinque società sia superiore al valore di tutte le società del Giappone. Ed invero, per valutare il valore della società, bisognerà includere delle metriche che riguardano come quella società faccia crescere la comunità e non soltanto i profitti finanziari. Sulla stessa scia e forse ancor prima (in considerazione del fatto che lo stesso manager già aveva scritto nel 2018 e nel 2019 nella “Dichiarazione della Business Round-table”), va segnalata la lettera aperta di L. FINK, Presidente e CEO di Blackrock, il più grande fondo di investimento al mondo, che nella sua ultima Larry Fink's 2022 Letter to CEOs, *The Power of Capitalism*, ha affermato che “A company must create value for and be valued by its full range of stakeholders in order to deliver long-term value for its shareholders”. Invero, il tema è antico più ampio e riguarda il fatto che le concentrazioni di ricchezza sono fonti non solo di potere economico, ma anche di potere politico, come già chiariva e analizzava B. LIBONATI, *Politica e società*, in *Riv. Soc.*, 1961, pp. 1096-1102, ora anche in *Id.*, *Scritti giuridici*, Vol. I, Milano, 2013. Più in generale su questi temi, E. BARCELLONA, *La Sustainability Corporate Governance nelle proposte di riforma del diritto europeo: a proposito dei limiti strutturali del c.d. stakeholderism*, in *Riv. Soc.*, 2022, 1.

⁷ Spesso, nel presente lavoro, ci riferiremo alla categoria degli “anziani”; ben consapevoli però che il medesimo discorso vale per tutti coloro che non hanno più quelle capacità cognitive necessarie per esercitare i diritti provenienti da un rapporto di conto corrente o di servizi di investimento, che pure erano stati a loro tempo contrattualizzati.

⁸ Per un'analisi invece della trasformazione del sistema bancario in termini di forme societarie ammesse e di riorganizzazione del mercato, mi sia permesso rinviare al mio *Osservazioni intorno alla riforma delle banche popolari*, in *Riv. dir. comm.*, 2016, II, p.43-79, nonché da ultimo *Ancora sulla riforma delle banche popolari (DL 3/2015): la lunga maratona giudiziaria* (appena cominciata), in *Riv. dir. comm.*, 2022, II, 17.

⁹ Banca d'Italia da qualche anno pubblica con cadenza annuale un report dettagliato "*Banche e istituzioni finanziarie: articolazione territoriale*". I dati indicati nel testo sono presi dall'ultimo report disponibile al momento in cui si scrive il presente, consultabile all'indirizzo: https://www.bancaditalia.it/pubblicazioni/banche-istfin/2022-banche-istfin/statistiche_STAATER_20220331.pdf.

¹⁰ Secondo una classificazione per gruppo istituzionale, le banche S.p.a. possedevano oltre 17.700 sportelli, pari al 75 per cento del totale nazionale, mentre le banche di credito cooperativo e le banche popolari erano rispettivamente il 18 per cento e il 6 per cento.

¹¹ Vale la pena ricordare che il fenomeno della concentrazione bancaria è stato un fenomeno guidato anche dal legislatore italiano che, negli ultimi 10 anni, ha introdotto radicali riforme in tema di disciplina dei modelli di banche mutualistiche; prima, nel gennaio del 2015, con la riforma delle banche popolari e, poi, nell'aprile del 2016 con la riforma – non meno importante – delle banche di credito cooperativo, ossia banche mutualistiche necessariamente ancorate ad un determinato territorio. Con riferimento alle popolari, l'art.1 del D.L. 24 gennaio 2015, n. 3 ("Misure urgenti per il sistema bancario e gli investimenti"), convertito con l. 24 marzo 2015, n. 33, il legislatore ha innanzitutto inserito un limite dimensionale patrimoniale per l'uso del modello banca popolare, in aggiunta ad una serie di modifiche alla *governance* di queste banche (voto maggiorato delle persone giuridiche, aumento delle deleghe di voto in assemblea e possibilità di avere amministratori non soci) e alle modalità di finanziamento delle stesse (possibilità di emettere strumenti finanziari partecipativi); per un commento mi sia permesso rinviare sul punto al mio *Osservazioni intorno alla riforma delle banche popolari del 2015. Un primo commento*, in *Riv. dir. comm.* 2016, p. 43 e da ultimo A. MIRONE, *Statuto delle banche popolari e riforma del credito cooperativo*, in *Giur. Comm.*, 2019, 211/I. Con riferimento invece alla Riforma delle BCC, con la legge n. 49 dell'8 aprile 2016, conversione in legge, con modificazioni, del decreto-legge 14 febbraio 2016, n. 18, "Recante misure urgenti concernenti la riforma delle banche di credito cooperativo, la garanzia sulla cartolarizzazione delle sofferenze, il regime fiscale relativo alle procedure di crisi e la gestione collettiva del risparmio", il legislatore ha previsto che ogni banca di credito cooperativo (di seguito "BCC") deve aderire ad un Gruppo Bancario Cooperativo: le BCC devono sottoscrivere un "contratto di coesione" che disciplina il funzionamento del Gruppo stesso e quindi il grado di direzione e coordinamento che la Capogruppo, della quale le medesime BCC aderenti detengono la maggioranza del capitale, esercita sulle singole banche del Gruppo. Per un commento della nuova normativa delle banche di credito cooperativo anche in ottica comparatistica, E. PAGANI, *La riforma del*

credito cooperativo in prospettiva comparata, in *Banca, Impresa e Società*, 2/2016, 203, la quale conclude affermando l'importanza di tutelare, anche attraverso questa riforma, la "biodiversità" del sistema bancario in Italia. Va detto che dal 2016 in avanti il legislatore non ha mai smesso di emendare la Riforma delle BCC, in particolare col c.d. Decreto "Mille Proroghe" (ossia la Legge 21 settembre, n. 108, di conversione, con modificazioni, del D.L. 91/2018), col c.d. "Decreto Fiscale" (ossia la Legge 17 dicembre 2018 n. 136 che converte, con modificazioni, il D.L. 23 ottobre 2018, n. 119) ed ancora con la Legge di Bilancio 2019 (ossia Legge 30 dicembre 2018, n. 145, in vigore dal 1° gennaio 2019).

¹² Tra i primi a mettere in luce in generale il valore della informatizzazione dei processi di produzione e dei prodotti/servizi nelle imprese ed i vantaggi competitivi che ne sarebbero derivati sono stati Porter e Millar, i quali con riferimento alle banche affermarono infatti che "*Banking and insurance [...] have always been information intensive. Such industries were naturally among the first and most enthusiastic users of data processing*", M. PORTER, V.E. MILLAR, *How information gives you competitive advantage*, in *Harvard Business Review*, 1985.

¹³ BCE, *The effects of Technology on the Eu Banking System*, 1999; <https://www.ecb.europa.eu/pub/pdf/other/techbnken.pdf>. Sul tema degli effetti dell'innovazione tecnologica nell'attività bancaria è tornato, da ultimo, il Governatore della Banca d'Italia Ignazio Visco al 29° Congresso ASSIOM FOREX del 4 febbraio 2023, affermando che: "*L'ampio ricorso all'esternalizzazione dei servizi informatici e l'elevata concentrazione che caratterizza questo mercato hanno fatto sì che nel 2022 la platea delle banche coinvolte da attacchi informatici sia aumentata rispetto all'anno precedente, sebbene il numero dei singoli eventi si sia ridotto*".

¹⁴ Premessa generale è che: "*Nell'ambito della generale disciplina dell'organizzazione e dei controlli interni, sono attribuiti agli organi e funzioni aziendali ruoli e responsabilità, relativi allo sviluppo e alla gestione del sistema informativo, nel rispetto del principio della separazione delle funzioni di controllo da quelle di supervisione e gestione*", così testualmente l'art. 1 del Capitolo 4.

¹⁵ L'importanza dell'*home banking* si coglie bene nel "Rapporto sulle scelte di investimento delle famiglie italiane 2021" presentato il 20 novembre 2022 da CONSOB, laddove si legge: "*L'utilizzo di internet da parte delle famiglie italiane nell'ambito delle scelte economico-finanziarie oscilla tra il 2 per cento nel caso della negoziazione di cripto-valute e il 44 per cento per l'online banking*", report reperibile all'indirizzo: https://www.consob.it/documents/1912911/1941479/rf2021_it.pdf/b37ab0b4-fdef-efe8-ce91-90a645760cc0.

¹⁶ Così l'intervento del V.D.G della Banca d'Italia, F. Panetta, *L'innovazione digitale nell'industria finanziaria italiana*, 26 settembre 2017: <https://www.ban->

caditalia.it/publicazioni/interventi-direttorio/int-dir-2017/Panetta_26092017.pdf.

¹⁷ Sul punto, vale la pena citare la prima indagine “*The Global Open Banking Report*” svolta dal CBI (l’associazione, oramai società consortile, che raggruppa molte delle banche italiane sui temi dell’innovazione tecnologica e della digitalizzazione dell’industria bancaria e finanziaria) in collaborazione con PWC, che fornisce una panoramica completa delle tendenze presenti nel sistema bancario nazionale e internazionale in tema di servizi innovativi in ambito bancario e finanziario, basati su modelli collaborativi tra diversi operatori del medesimo settore o anche di settori diversi, reperibile all’indirizzo: <https://www.cbi-org.eu/Home-en/The-Global-Open-Banking-Report-1>. L’open banking si basa, infatti, sulla condivisione di dati e informazioni tra i vari attori coinvolti (es. banche tradizionali, banche digitali, FinTech e Tech Provider), con l’obiettivo di sviluppare ed erogare servizi innovativi al cliente finale, quali Servizi di Account Information, Servizi di Payment Initiation e Servizi a Valore Aggiunto. Solo per fare qualche esempio, i servizi di Account Information sono principalmente guidati dall’aggregazione dei conti (in modo che il cliente possa avere una visione completa di tutti i suoi conti), e dal Personal Financial Management (che, ad esempio, elabora approfondimenti sui trend di spesa o sui piani di risparmio). Per quanto riguarda il servizio di Payment Initiation, i servizi più offerti sono il Peer-to-Peer (P2P) e i Pagamenti Istantanei, con un enorme sviluppo delle richieste di modi pratici, semplici ed economici di eseguire i pagamenti. Infine, sui Servizi a Valore Aggiunto, ampiamente diffusi sono la verifica del codice IBAN, che consente ai clienti di verificare la validità e la corretta titolarità di un IBAN prima di effettuare un pagamento, e l’Identità Digitale & Digital Onboarding, che fa leva sui dati dell’utente per facilitare l’*Onboarding* (così il Report citato pp. 49 ss.).

¹⁸ Il riferimento è alla Direttiva 2015/2366/(UE) del Parlamento Europeo e del Consiglio del 25 novembre 2015, sui servizi di pagamento nel mercato interno, entrata in vigore in Italia il 13 gennaio 2016 (c.d. “PSD2” *Payment System Directive 2*), ai sensi della quale con “Open Banking” si intende “*un ecosistema aperto e digitale che consente, anche senza la presenza di accordi prestabiliti, lo scambio di dati e informazioni, non solo finanziarie, tra gli operatori (bancari, finanziari e non) che ne fanno parte.*” La normativa europea è stata poi integrata con il Regolamento delegato 2018/389 della Commissione Europea del 27 novembre 2017, entrato in vigore alla fine del 2019. Interessanti, sul punto, i servizi offerti alla clientela dalle c.d. terze parti (Third Party Providers - TPP). Come abbiamo in parte anticipato, i TPP, nelle loro differenti tipologie, offrono: i) servizi di informazione sui conti di pagamento detenuti dal cliente presso uno o più prestato-

ri di servizi di pagamento (Servizio di Informazione sui Conti/Account Information Service – AIS); ii) servizi attraverso i quali il TPP dispone, su richiesta del cliente, un ordine di pagamento a valere su un conto di pagamento che il cliente detiene presso un altro prestatore di servizi di pagamento (Servizio di Disposizione di Ordini di Pagamento/Payment Initiation Service – PIS); iii) servizi di pagamento basati sulle carte, che richiedono una procedura di conferma fondi su un conto che il cliente detiene presso un altro prestatore di servizi di pagamento, non preventivamente associato tramite un accordo contrattuale alla carta di pagamento (Servizio di Conferma Fondi/Card Initiated Service – CIS). Per approfondimenti: *PSD2 e Open Banking: nuovi modelli di business e rischi emergenti* - Banca d'Italia, novembre 2021, reperibile all'indirizzo: <https://www.bancaditalia.it/compiti/vigilanza/analisi-sistema/approfondimenti-banche-int/2021-PSD2-Open-Banking.pdf>. Sul tema, F. FERRETTI, *L'“open banking” e le troppe zone grigie del conflitto tra la legislazione europea sui pagamenti e la tutela dei dati personali (The “open banking” and the too many gray areas of the conflict between the European legislation on payment services and the protection of personal data)*, in *Federalismi.it*, 2021, fasc. 10, pp. 69-99; F. MARASÀ, *Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR (The processing of personal data of payment service users between PSD2 and GDPR)*, in *Orizzonti del diritto commerciale*, 2020, fasc. 2, pp. 629-670; I. D'AMBROSIO, *La tutela del consumatore nei pagamenti elettronici e la nuova direttiva europea PSD2*, in *Notariato*, 2019, fasc. 6, pp. 676-68.

¹⁹ Terza indagine conoscitiva pubblicata il 22 novembre 2021 condotta da Banca d'Italia: una rilevazione che ha cadenza biennale e che ha coinvolto 59 gruppi bancari e 53 banche non appartenenti a gruppi. Consultabile all'indirizzo: <https://www.bancaditalia.it/publicazioni/indagine-fintech/2021/2021-FINTECH-INDAGINE.pdf>.

²⁰ Per progetti *fintech* si intendono quelle iniziative di investimento incentrate sull'innovazione tecnologico-finanziaria e capaci di generare nuovi processi, prodotti, servizi e modelli di business. Secondo Banca d'Italia: *“La diffusione delle tecnologie contribuisce a trasformare la struttura dell'industria finanziaria; assume spessore l'innovazione della filiera del credito e dei pagamenti, grazie ai progetti dedicati al mobile banking, al digital lending e all'erogazione di prodotti derivati dai servizi AIS e PIS”* [rispettivamente: Servizio di informazione sui conti/Account Information Service e Servizio di disposizione di ordini di pagamento/Payment Initiation Service, ndr], p.36. Per un'analisi più generale dello stato di digitalizzazione dell'economia europea e quindi della società, si vedano gli interessantissimi Digital Economy and Society Index (DESI) reports, che oramai dal 2014 la Commissione Europea emette. In particolare, per l'edizione 2021 dell'indice di digi-

talizzazione dell'economia e della società (DESI), l'Italia si colloca al 20° posto fra i 27 Stati membri dell'UE: l'Italia è significativamente in ritardo rispetto ad altri paesi dell'UE in termini di capitale umano. Rispetto alla media UE, registra infatti livelli di competenze digitali di base e avanzate molto bassi. Solo il 42 per cento delle persone di età compresa tra i 16 e i 74 anni possiede perlomeno competenze digitali di base (56 per cento nell'UE) e solo il 22 per cento dispone di competenze digitali superiori a quelle di base (31 per cento nell'UE). Per maggiori approfondimenti il report è consultabile sul sito internet del DESI all'indirizzo: <https://digital-strategy.ec.europa.eu/en/policies/desi>.

²¹ Rapporto annuale Istat 2022: https://www.istat.it/storage/rapporto-annuale/2022/Rapporto_Annuale_2022.pdf.

²² Nel 2009 sfioravano i 12 milioni e costituivano il 20,3 per cento della popolazione; se si va più indietro negli anni scopriamo che nel 1960 gli anziani erano 4,6 milioni ed erano pari al 9,3 per cento, negli anni 80 raggiungevano i 7,4 milioni ed erano pari al 13 per cento, mentre nel 2000 salivano a 10,3 milioni, pari quindi al 18,1 per cento. Quindi, in meno di 10 anni, gli anziani sono aumentati di 5 punti percentuale. Così: *Invecchiamento attivo e condizione di vita degli anziani in Italia* – Istat 2020 <https://www.istat.it/it/files//2020/08/Invecchiamento-attivo-e-condizioni-di-vita-degli-anziani-in-Italia.pdf>.

²³ La speranza di vita oggi fa registrare un livello superiore agli 80 anni per gli uomini e agli 85 anni per le donne; *Invecchiamento attivo*, cit.

²⁴ Va detto inoltre che, dalla seconda metà degli anni 70 in poi, le coppie italiane hanno smesso di tenere un comportamento riproduttivo in grado di garantire il cosiddetto “rimpiazzo delle generazioni” (due figli per donna); *Invecchiamento attivo*, cit.

²⁵ Rapporto annuale Istat 2019: <https://www.istat.it/storage/rapporto-annuale/2019/Rapportoannuale2019.pdf>.

²⁶ Rapporto annuale Istat 2022: https://www.istat.it/storage/rapporto-annuale/2022/Rapporto_Annuale_2022.pdf.

²⁷ La scarsa partecipazione alla formazione della popolazione anziana inattiva riveste una notevole importanza in considerazione del fatto che la quota di inattivi è predominante: sono circa due su tre – poco meno di 10 milioni di individui – la cui inclusione sociale e qualità della vita sono connesse anche alla partecipazione dell'iCloud Learning.

²⁸ Sempre, *Invecchiamento attivo e condizione di vita degli anziani in Italia* – Istat 2020 <https://www.istat.it/it/files//2020/08/Invecchiamento-attivo-e-condizioni-di-vita-degli-anziani-in-Italia.pdf>, p. 113.

²⁹ L'uso di internet nel nostro Paese rimane fortemente legato all'età, e solamente tra le persone di età maggiore di 65 anni laureate l'utilizzo della rete presenta valori simili a quelli registrati per la media italiana: il 61,3 per cento (Fondazione Ugo Bordoni, Istat, 2018) <https://www.fub.it/wp-content/uploads/2020/06/Internet@Italia-2018.pdf>. Occorre inoltre rammentare che, riguardo l'utilizzo regolare di internet da parte degli individui di 65-74 anni in Europa, l'Italia nel 2018 si trovava nella parte inferiore della graduatoria, lontano dalla media europea e ancor di più dalle prime posizioni, occupate da paesi dell'Europa del Nord, Fonte: Rapporto Annuale 2019 – Approfondimento Gli anziani e le nuove tecnologie, Figura 3.38, p. 161 <https://www.istat.it/storage/rapporto-annuale/2019/capitolo3.pdf>, in linea con EUROSTAT, *ICT usage in households and by individuals*.

³⁰ Nell'ultimo decennio la quota di utenti regolari di Internet nella popolazione europea (UE-28) tra 65 e 74 anni è più che triplicata, passando dal 16 per cento al 52 per cento; tale trend positivo si registra anche per l'Italia, con un incremento di 28 punti percentuali (passando dal 6 al 34 per cento). In Italia, nel complesso, la percentuale di utenti regolari di Internet di 65 anni e più è del 21,7 per cento. L'analisi per generazione consente di inquadrare meglio i cambiamenti intercorsi nel tempo a parità di età. Analizzando i profili di fruizione della rete si osserva un utilizzo regolare di Internet molto limitato per gli uomini e pressoché nullo per le donne nati prima del 1934 (che nel 2018 avevano 84 anni e più). A fronte di una diffusione costante dell'uso regolare di Internet per i nati a partire dal 1934, si osserva un divario marcato tra le diverse generazioni: i giovani anziani di 65-69 anni nel 2018 (nati tra il 1949 e il 1953) utilizzavano Internet regolarmente, molto più dei loro coetanei di quindici anni prima. Tale tendenza si è osservata sia tra gli uomini (44,7 contro 5,8 per cento dei nati tra il 1934 e il 1938), sia tra le donne (34,9 contro 0,7 per cento dei nati tra il 1934 e il 1938), con evidenti differenze di genere. Così il Rapporto Annuale 2019 – Approfondimento Gli anziani e le nuove tecnologie, p. 161 <https://www.istat.it/storage/rapporto-annuale/2019/capitolo3.pdf>. Altri studi affermano che i dati Istat, scorporati per età, ci aiutano a comprendere questo aspetto: i cittadini tra 55 e 59 anni che non usano Internet sono solo il 18,5 per cento, mentre tra gli over 75 sono l'82,8 per cento, <https://www.spazio50.org/50piu-e-fondazione-leonardo-al-cnel>.

³¹ Rapporto annuale Istat 2020 <https://www.istat.it/storage/rapporto-annuale/2020/Rapportoannuale2020.pdf>. Ma si veda anche CALIANDRO, A., GARAVAGLIA, E., STURIALE, V., DI LEVA, A., *Older people and smartphone practices in everyday life: an inquire on digital sociality of italian older users*, in *The Communication Review*, 2021; SALA, E., GAIA, A., CERATI, G., *The grey digital divide in Social*

Networking Site use in Europe. Results from a quantitative study, in *Social Science Computer Review*, 2020; Il tema non è ovviamente solo italiano. Si veda ad esempio: SNYDER, JOSEPH, *Strategies for Banks to Protect Elderly Clients from Themselves and Others*, *Generations: Journal of the American Society on Aging* 36, no. 2 (2012): 98–100. <https://www.jstor.org/stable/26555918>; o anche *Elder abuse age-friendly banking: best practices in fighting financial exploitation, caregiver support and accessibility*, in *The Gerontologist*, Volume 55, Issue Suppl_2, November 2015, Page 496, <https://doi.org/10.1093/geront/gnv215.01>.

³² Rapporto sulle scelte di investimento delle famiglie italiane; Consob, 2022, in <https://www.consob.it/documents/11973/287812/rf2022.pdf/cf-6f38e9-dbcc-6057-8fff-f56643facdba?t=1674683068756>.

³³ In realtà, va detto che non è propriamente vero che l'utente è libero di navigare ed accedere al proprio conto perché, così come per chiunque navighi nel Web utilizza delle APP per navigare ed accedere a servizi e contenuti, anche nel mondo dell'Open Banking l'utente non naviga direttamente sui servizi online della propria banca (gestore del dato), ma c'è un'applicazione terza (del Third Party Provider, TPP, gestore del servizio) che filtra, aggrega dati e offre servizi all'utente secondo le sue richieste e secondo proprie logiche commerciali. Così, *The Global Open Banking Report*, CBI, 2021, rinvenibile all'indirizzo internet: <https://www.cbi-org.eu/Home/The-Global-Open-Banking-Report-1>

³⁴ Cfr. [https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX-22016A1019\(01\)](https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX-22016A1019(01)).

³⁵ Cfr. <https://www.unric.org/it/agenda-2030>; va detto però che tra tutti i diciassette *Sustainable Development Goal* la parola “Finanza” viene declinata solo al 17^{mo} “Partnership for the Goals”, ossia *Rafforzare gli strumenti di attuazione e rinnovare il partenariato mondiale per lo sviluppo sostenibile*, ma anche qui viene declinata solo come necessità di sviluppare gli aiuti internazionali ai paesi in via di sviluppo (nelle varie forme, ossia dall'aumentarne la capacità fiscale interna e la riscossione delle entrate, al mobilitare ulteriori risorse economiche per i paesi in via di sviluppo da più fonti, sia infine per adottare e applicare regimi di promozione degli investimenti per i paesi meno sviluppati). Prima di allora ricordiamo il “*Summit sulla terra*” svoltosi a Rio de Janeiro nel 1992 <https://www.un.org/en/conferences/environment/rio1992>.

³⁶ Questo il *leitmotiv* di tutti i testi normativi che si sono succeduti nel tempo; vedi per tutti il Considerando n. 3, Regolamento (UE)2019/2088.

³⁷ Così testualmente il Considerando n. 11, Regolamento (UE)2020/852.

³⁸ Sulla stessa scia e, a dire il vero, sulla scia della Direttiva 2014/95/UE in materia di informazioni non finanziarie relativa alle grandi società, si pone la

Proposta di Direttiva del Parlamento europeo e del Consiglio, relativa al *Dovere di diligenza delle imprese ai fini della sostenibilità*, e che modifica la Direttiva (UE) 2019/1937. Molto critico sul tema M. STELLA RICHTER, *Corporate Sustainability Due Diligence, noterelle semiserie su problemi serissimi*, in *Riv. Soc.*, 714, 2022, dove sono presenti ampi riferimenti; l'Autore critica in particolare modo la vaghezza e genericità delle regole dettate dalla Proposta che rischiano di affidare agli amministratori delle grandi società le "massime scelte politiche".

³⁹ Il termine fu coniato dall'ecologista statunitense Jay Westerveld nel 1986, cfr. *The Guardian*, *The troubling evolution of corporate greenwashing*, 20 agosto 2016 (p.71). Parla espressamente di tale aspetto anche la Risoluzione del 28 marzo 2019, così descrivendo il fenomeno: "*Greenwashing refers to the practice of gaining an unfair competitive advantage by marketing a financial product as environmental-friendly, when in fact it does not meet basic environmental standards*", puntando quindi sugli aspetti lesivi della concorrenza.

⁴⁰ Regolamento (UE)2020/852, Considerando n. 11.

⁴¹ L'*High Level Expert Group on Sustainable Finance* fu composto da 20 esperti ad alto livello della società civile, del settore finanziario, del mondo accademico e da osservatori delle istituzioni europee e internazionali. Per una rapida sintesi su come invece il Protocollo di Kyoto del 1997 ed il suo meccanismo dei *carbon offsets*, ossia la possibilità di commercializzare le emissioni inquinanti, abbia di fatto contribuito alla crisi ecologica, L. GALLINO, *Il denaro, il debito e la doppia crisi*, Torino, 2015, in part. p. 43.

⁴² il "*Final report 2018: Financing a sustainable European economy*", a cura dello *EU-High level expert group on sustainable finance*, reperibile all'indirizzo: https://finance.ec.europa.eu/system/files/2018-01/180131-sustainable-finance-final-report_en.pdf.

⁴³ http://europa.eu/rapid/press-release_IP-18-1404_en.htm.

⁴⁴ In gergo anche noto come "Regolamento SFDR" dall'acronimo inglese del titolo: *Sustainable Finance Disclosure Regulation*.

⁴⁵ Considerando 14, Regolamento (UE)2019/2088.

⁴⁶ Di fatto vengono individuati due tipi di prodotti finanziari:

1. ex articolo 8, par.1, un prodotto finanziario che *promuove* tra le altre caratteristiche ambientali o sociali o una combinazione di tali caratteristiche, a condizione che le imprese in cui gli investimenti sono effettuati rispettino prassi di buona governance;
2. ex articolo 9, un prodotto finanziario che ha come *obiettivo* investimenti sostenibili ed è stato designato un indice di riferimento (fermo restando

che se un indice non è stato individuato andrà spiegato in che modo l'obiettivo è raggiunto).

⁴⁷ Ai sensi dell'art. 3, un'attività economica è considerata "ecosostenibile" se:

- a) contribuisce in modo sostanziale al raggiungimento di uno degli obiettivi ambientali di cui allo stesso regolamento (mitigazione dei cambiamenti climatici, adattamento ai cambiamenti climatici, uso sostenibile e protezione delle acque e delle risorse marine, transizione verso un'economia circolare, prevenzione e riduzione dell'inquinamento e protezione e ripristino della biodiversità e degli ecosistemi);
- b) non arreca un danno significativo a nessuno degli obiettivi ambientali suddetti;
- c) è svolta nel rispetto delle garanzie minime di salvaguardia;
- d) è conforme ad alcuni criteri di vaglio tecnici stabiliti dalla commissione.

⁴⁸ Si veda da ultimo anche il Regolamento (UE) 2023/363 della Commissione del 31 ottobre 2022 che modifica e rettifica le norme tecniche di regolamentazione stabilite nel regolamento delegato (UE) 2022/1288 per quanto riguarda il contenuto e la presentazione delle informazioni relative all'informativa nei documenti precontrattuali e nelle relazioni periodiche per i prodotti finanziari che investono in attività economiche ecosostenibili.

⁴⁹ Sempre sui temi della trasparenza, non possiamo non ricordare che è stata pubblicata sulla Gazzetta ufficiale dell'Unione europea, il 16 dicembre 2022, la nuova Direttiva (UE) 2022/2464 del 14 dicembre 2022 sulla rendicontazione societaria di sostenibilità (*Corporate Sustainability Reporting Directive – CSRD*). A partire dal 1° gennaio 2024 verranno estesi gli obblighi di rendicontazione di sostenibilità a tutte le imprese di grandi dimensioni, nonché a tutte le imprese con valori mobiliari ammessi alla negoziazione in mercati regolamentati.

⁵⁰ L'EBA è stata creata nel 2011 e fa parte di una terna che comprende anche l'ESMA (*European Securities and Market Authority*) e la EIOPA (*European Insurance and Occupational Pensions Authority*). L'EBA si occupa di banche, l'ESMA di mercati finanziari (le Borse) e l'EIOPA di assicurazioni e fondi pensione. L'Autorità Bancaria Europea (ABE) è un'autorità indipendente dell'Unione europea (UE), che opera per assicurare un livello di regolamentazione e di vigilanza prudenziale efficace e uniforme nel settore bancario europeo. Gli obiettivi generali dell'Autorità sono assicurare la stabilità finanziaria nell'UE e garantire l'integrità, l'efficienza e il regolare funzionamento del settore bancario. L'EBA, assieme alle altre due autorità citate, fa parte del Sistema Europeo di Vigilanza Finanziaria (SEVIF), che comprende inoltre il Comitato Europeo per il Rischio Sistemico (CERS), il Comitato Congiunto delle Autorità Europee di Vi-

gilanza e le Autorità di Vigilanza Nazionali. Pur essendo indipendente, l'EBA è responsabile dinanzi al Parlamento Europeo, al Consiglio dell'Unione Europea e alla Commissione Europea.

⁵¹ Per eventuale approfondimento, le *Guidelines on Loan Origination and Monitoring* dell'EBA sono consultabili al link: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/Guidelines%20on%20loan%20origination%20and%20monitoring/884283/EBA%20GL%202020%2006%20Final%20Report%20on%20GL%20on%20loan%20origination%20and%20monitoring.pdf.

⁵² Le autorità competenti di cui all'articolo 4, paragrafo 2, del regolamento (UE) n. 1093/2010 sono tenute a conformarsi a detti orientamenti integrandoli opportunamente nelle rispettive prassi di vigilanza (per esempio modificando il proprio framework giuridico o le proprie procedure di vigilanza), anche quando gli stessi sono diretti principalmente agli enti. Ad agosto 2020 la Banca d'Italia ha dichiarato all'EBA l'intenzione di conformarsi agli Orientamenti dalla stessa, espressi in materia di concessione e monitoraggio dei prestiti (EBA/GL/2020/06) e quindi, con Nota n. 13 del 20 luglio 2021 "Attuazione degli Orientamenti dell'Autorità bancaria europea in materia di concessione e monitoraggio dei prestiti (EBA/GL/2020/06)", la Banca d'Italia ha dato attuazione a detti Orientamenti che dunque assumono valore di orientamenti di vigilanza.

⁵³ Ai sensi del Regolamento (EU) n. 1093 / 2010, per «*istituzione finanziaria*» si intendono gli «*enti creditizi*» quali definiti all'articolo 4, paragrafo 1, della direttiva 2006/48/CE, le «*imprese di investimento*» quali definite all'articolo 3, paragrafo 1, lettera b), della direttiva 2006/49/CE e i «*conglomerati finanziari*» quali definiti all'articolo 2, paragrafo 14, della direttiva 2002/87/CE, salvo che, in relazione alla direttiva 2005/60/CE, per «*istituti finanziari*» si intendano gli enti creditizi e gli enti finanziari quali definiti all'articolo 3, paragrafi 1 e 2, di detta direttiva.

⁵⁴ Prendendo le mosse dall'articolo 5 del Trattato sull'Unione Europea, il principio di proporzionalità prevede una proporzione tra costi di applicazione e benefici dell'obiettivo regolamentare. Secondo tale articolo: 1. *La delimitazione delle competenze dell'Unione si fonda sul principio di attribuzione. L'esercizio delle competenze dell'Unione si fonda sui principi di sussidiarietà e proporzionalità.* [omissis] 3. *Le istituzioni dell'Unione applicano il principio di sussidiarietà conformemente al protocollo sull'applicazione dei principi di sussidiarietà e di proporzionalità. I parlamenti nazionali vigilano sul rispetto del principio di sussidiarietà secondo la procedura prevista in detto protocollo.* 4. *In virtù del principio di proporzio-*

nalità, il contenuto e la forma dell'azione dell'Unione si limitano a quanto necessario per il conseguimento degli obiettivi dei trattati. Le istituzioni dell'Unione applicano il principio di proporzionalità conformemente al protocollo sull'applicazione dei principi di sussidiarietà e di proporzionalità.

⁵⁵ Le *Guidelines on Loan Origination and Monitoring* sono state in realtà predisposte al fine di: (i) garantire che gli enti dispongano di standard prudenziali per la concessione di nuovi crediti; (ii) impedire che i crediti in bonis di nuova concessione diventino in futuro *Non Performing* e (iii) contribuire alla stabilità finanziaria complessiva del settore bancario.

⁵⁶ Così U. BIGGERI sul sito internet: <https://www.bancaetica.it/blog/lue-punta-sulla-finanza-sostenibile>, il quale ha affermato: “Ma le esperienze di questi anni, laddove molti ottimi propositi normativi si sono spesso tradotti in regole mal scritte a volte con effetti opposti a quelli auspicati, impongono cautela: è d’obbligo porre grande attenzione a come verranno declinate le singole attività relative a ciascun obiettivo”; nello stesso verso ma con un’accentuata critica agli incentivi, cfr. *Finance Watch, A green supporting factor would weaken banks and do little for the environment*, 1° febbraio 2018, reperibile all’indirizzo: <http://finance-watch.org/hot-topics/blog/1506-green-supporting-factor>; ancora A. BARANES e E. TRAMONTO, *Investimenti sostenibili, per Bruxelles sono solo green*, 12 giugno 2018, reperibile sul sito internet: <https://valori.it/investimenti-sostenibili-per-bruxelles-sono-solo-green/>. Si esprime sul rapporto tra la normativa ESG e le banche, P. ANGELINI, *I rischi finanziari posti dai cambiamenti climatici: carenze informative e piani di transizione*, Intervento all’Associazione nazionale per lo studio dei problemi del credito Milano, 15 novembre 2022, reperibile al seguente indirizzo: <https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2022/ANGELINI-15-novembre-2022.pdf>.

⁵⁷ Sul tema, V. MELI, *Il conto corrente di base tra inclusione finanziaria e controllo della circolazione della ricchezza*, in *Banca, Borsa Titoli di Credito*, 2014, 56; l’Autore ricorda come, con riguardo al conto di base, si è assistito ad un lungo processo evolutivo partito dal conto corrente semplice, il quale prevedeva che il canone annuo onnicomprensivo e il tasso di interesse creditore fossero affidati alla libera determinazione del prestatore di servizi di pagamento. Sulla direttiva 2014/92 ed il relativo decreto legislativo attuativo n. 37/2017, S. MEZZACAPO, *La nuova disciplina nazionale dei “conti di pagamento” alla luce dell’armonizzazione attuata con la payment accounts directive*, in *Banca Borsa Titoli di Credito*, 2017, 787.

⁵⁸ Così l’art. 126-*noviesdecies*, TUB.

⁵⁹ Così l’art. 126-*vicies semel*, TUB.

⁶⁰ Gli artt. 4 e 5 del D.M. 70/2018 individuano i parametri economici per definire la “clientela svantaggiata” e i “titolari di trattamenti pensionistici” che hanno diritto al conto di base gratuito, nonché i loro specifici obblighi tra i quali, a titolo esemplificativo, quello di effettuare una comunicazione annuale entro il 31 maggio dell'importo pensionistico ricevuto. È fatta poi salva la possibilità di addebitare le spese per le operazioni aggiuntive o in numero superiore, nel rispetto dei criteri di ragionevolezza e coerenza, con finalità di inclusione finanziaria di cui all'articolo 3 (che richiama a sua volta il canone annuale onnicomprensivo).

⁶¹ Sul rapporto di conto corrente e l'obbligo a contrarre imposto agli istituti finanziari, cfr. F. GIGLIOTTI, *Obbligo a contrarre e limiti a (diritto di) recesso nel “rapporto di conto corrente” bancario. A proposito di una recente proposta normativa*, in *Riv. Dir. Bancario*, 2021, 247. Sui contratti bancari, non si può non citare B. LIBONATI, *Contratto bancario e attività bancaria*, Milano, 1965 che considerava il conto corrente bancario come contratto “di servizio” necessario a regolare i rapporti di debito-credito tra la banca e i clienti.

⁶² Il tema dell'inclusione finanziaria è poi legato a quello, espressamente disciplinato dall'art. 126-*vicies sexies*, dell'*educazione finanziaria*. Il TUB dunque prevede che “*La Banca d'Italia promuove iniziative dirette a fornire ai consumatori, e in particolare a quelli individuati ai sensi dell'articolo 126-*vicies quater*, informazioni chiare e comprensibili sul conto di base, sulle relative condizioni generali di prezzo, sulle procedure per accedervi e sulle possibilità di ricorso a procedure alternative di risoluzione delle controversie*”. Ma ancora più interessante ai nostri fini, ossia in merito alla sostenibilità applicata all'attività bancaria, è il secondo comma laddove si afferma che: “*La Banca d'Italia può promuovere la redazione di codici di condotta per l'offerta indipendente di iniziative di educazione finanziaria da parte degli intermediari, finalizzate a favorire l'orientamento della clientela e l'assistenza per la gestione responsabile delle finanze personali*”.

⁶³ Per un approfondimento sul tema dell'inclusione finanziaria, V. MELI, *Il conto corrente di base*, op. cit., il quale, sul conto di base, conclude affermando che meglio sarebbe stato concepire una qualche forma di incentivo, quanto meno per premiare l'offerta, ma, prima ancora, la diffusione delle informazioni sui conti di base, ovvero intervenire con qualche forma di “buono”, da consegnare ai soggetti individuati come svantaggiati, perché fosse speso per l'acquisizione di un conto di base. Ancora, N. BOCCELLA - I. SALERNO, *Il microcredito. Soggetti non bancabili. Inclusione finanziaria e sociale*, Roma, 2019; G. CORRADO, *L'esclusione finanziaria*, Torino, 2012. E si veda pure il volume *Inclusione finanziaria: le iniziative del G20 e il ruolo della Banca d'Italia*, edito a cura della Banca d'Italia, Roma, 2011; interessante, ma per certi versi paradossale a tal proposito,

l'affermazione secondo la quale i “servizi di pagamento innovativi migliorano l'inclusione finanziaria”. Un esame comparatistico essenziale del tema offre P. RIGHETTI, *Dalla bancarizzazione all'inclusione finanziaria: il paradosso della modernizzazione dei mercati e le iniziative di contrasto all'esclusione*, in *Etica e finanza*, in S. SIGNORI - G. RUSCONI - M. DORIGATTI (a cura di), Milano, 2005, 99 ss. V., inoltre, il volume edito dall'A.B.I., *Banche e inclusione finanziaria*, Roma, 2009.

⁶⁴ Cfr. S. MEZZACAPO, *La nuova disciplina nazionale dei “conti di pagamento”*, op. cit., il quale espressamente nota che, se è vero che la direttiva mirava all'armonizzazione delle condizioni di mercato e quindi a sviluppare la concorrenza, va altresì rimarcato che, oltre a tali profili strettamente pro-concorrenziali e di efficiente funzionamento del “mercato interno”, la direttiva PAD sottolinea l'importanza di obiettivi *lato sensu* “sociali”, rafforzata dall'indicazione secondo cui gli Stati Membri dovrebbero “promuovere misure a sostegno dell'educazione [finanziaria] dei consumatori più vulnerabili” e la “fornitura congiuntamente ai conti di base di servizi indipendenti di educazione finanziaria” (considerando n. 49 PAD). Sul rapporto tra sistemi di pagamento e concorrenza, M. LIBERTINI, *Regolazione e concorrenza nei servizi di pagamento*, in *Dir. banc. merc. fin.*, 2012, 611-638.

⁶⁵ Ci porterebbe assai fuori tema un'analisi di dettaglio, ma non possiamo non notare come, alle stesse conclusioni sopra descritte, si arriva anche seguendo l'approccio alle discipline privatistiche portato avanti dagli studi dell'economia comportamentale, ossia la “Behavioural Law and Economics”: cfr. A. ZOPPINI, *Contratto ed economia comportamentale*, (voce) Enc. Dir. Sul tema inoltre: *Oltre il soggetto razionale. Fallimenti cognitivi e razionalità limitata nel diritto privato* a cura di G. Rojas Elgueta e N. Vardi, Roma, Roma-Tre Press, 2014, e *I fondamenti cognitivi del diritto. Percezioni, rappresentazioni, comportamenti* a cura di R. Caterina, Milano, Mondadori, 2008; nella letteratura gius-economica si veda *Behavioral Law and Economics* a cura di C. R. SUNSTEIN, Cambridge, Cambridge University Press, 2000, e *The Law and Economics of Irrational Behavior* a cura di F. Parisi e V. L. Smith, Stanford, Stanford University Press, 2005). Se infatti si assume che il nuovo paradigma da utilizzare non è più l'*homo oeconomicus*, anche detto *econs* perfettamente razionale (J. S. MILL, *Principles of Political Economy*, 1848), ma l'*homo sapiens*, quello reale, con i suoi limiti, ancor più delle norme che abbiamo analizzato sul conto di base, bisogna tener conto del soggetto che si ha di fronte, dei suoi limiti e quindi della necessità di adattare quei prodotti ed anche che l'offerta da presentare sia parametrata alle esigenze e alla capacità di tali soggetti. Per completezza, con riferimento all'economia comportamentale, si ricorda che i fondatori del c.d. “*behavioral law and economics movement*” sono considerati C. R. SUNSTEIN (Harvard Law School), R. H. THALER (Chicago) and C. JOLLS (Yale), i quali, nel loro *A behavioral Approach to Law and*

Economics, apparso nel 1998 e reperibile al seguente indirizzo: http://www.law.harvard.edu/programs/olin_center/papers/pdf/236.pdf, diedero avvio a tale approccio agli studi di economia. Per una lettura divulgativa di tale approccio, cfr. R. H. THALER e C. R. SUSTEIN, *Nudge. Improving Decision About Health, Wealth, And Happiness*, Yale University Press, 2008, ora anche nella versione italiana, *La spinta gentile. La nuova strategia per migliorare le nostre decisioni sul denaro, salute e felicità*, Milano, 2014; sempre sul tema R. H. THALER, *Misbehaving. The making of Behavioral Economics*, 2015.

⁶⁶ Affrontano, ad esempio, da ultimo, il tema da un punto di vista delle tecnologie utilizzabili, S. PONTESILLI e M. R. VECCHIATO Vecchiato, *Biometrica Vocale - Servizi bancari online, come garantire un accesso “anti-digital divide”: le tecnologie utili*, rinvenibile su <https://www.agendadigitale.eu/cultura-digitale/servizi-bancari-online-come-garantire-un-accesso-anti-digital-divide-le-tecnologie-utili/>, 18 gennaio 2022.

Gli *smart contracts* nel mercato delle assicurazioni: limiti e opportunità

ETTORE BATTELLI

SOMMARIO. 1. Gli *smart contracts* quali contratti *self-executing*. - 2. La questione della predeterminazione delle clausole contrattuali traducibili in linguaggio algoritmico. - 3. Lo *smart contract* come contratto asimmetrico: profili di tutela del consumatore e della concorrenza. - 4. Il ruolo dei *big data* nei servizi assicurativi. - 5. *Insurtech*: la gestione automatizzata dei servizi assicurativi. - 6. Limiti e opportunità degli *smart contracts* nelle assicurazioni.

1. Gli *smart contracts* quali contratti *self-executing*

Il presente studio mira ad analizzare alcuni aspetti degli *smart contracts* prestando specifica attenzione al loro impatto nella vita dei cittadini e in particolare, in maniera assai significativa, nel delicato settore delle assicurazioni segnato dall'innovazione tecnologica.

Gli *smart contracts* sebbene non siano oramai una novità, tanto da essere regolati tanto nel diritto italiano quanto in quello di altri Paesi¹, si sono diffusi nel mercato globale in modo parallelo e subordinato all'evolversi della tecnologia *blockchain*²; infatti, pur potendo operare a prescindere da tale tecnologia, è pur sempre da essa che traggono quell'elevato grado di certezza e verificabilità che ne costituisce un valore aggiunto acquisito nell'analisi giuridica e soprattutto nella prassi applicativa, mirando ad evitare l'insorgere di controversie e, non da ultimo, sottrarre la contrattazione all'intervento giudiziale³.

In Italia la norma di riferimento è rappresentata dall'art. 8-ter del d.l. n. 135 del 2018, convertito con modificazioni dalla

l. n. 12 dell'11 febbraio 2019 che, al comma 2, al fine di predisporre un primo quadro definitorio⁴ al passo con gli sviluppi dell'economia digitale, "ha tentato"⁵ di offrire una prima definizione di *smart contract*, sancendo che «si definisce "*smart contract*" un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse»⁶.

Gli *smart contracts* soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo rispondente ai requisiti fissati dall'Agenzia per l'Italia digitale⁷. Ben tenendo presente di come essi si muovano nel solco di quella "spersonalizzazione"⁸ progressiva del contratto, funzionale tanto agli interessi dell'impresa quanto a quelli dei consumatori⁹, di essi si avvale l'economia e la circolazione della ricchezza.

Senonché, secondo la definizione prospettata, gli *smart contracts* non sono semplicemente *software* posti in collegamento con un sistema DLT¹⁰ che ricorre alla logica condizionale¹¹. Al contrario, pur "spersonalizzati" per intervento di intelligenze capaci di autogestire i rapporti, al punto da rendere superfluo o comunque ridotto l'intervenuto umano¹², essi pur sempre configurano accordi fra due o più parti volti a costituire un rapporto giuridico patrimoniale e sono, dunque, contratti *ex art.* 1321 c.c.

Non deve però sottacersi la distinzione tra l'attività di "negoziante algoritmica" automatizzata¹³, affidata ad un *software* o ad un sistema di intelligenza artificiale, e l'esecuzione e la gestione del rapporto negoziale quali compiti propri dello *smart* in quanto protocollo autonomamente capace di incorporare regole, a prescindere che sussista o meno un substrato legale¹⁴; anzi, a volte seguendo modelli non riconducibili alle leggi dei singoli stati ma coerenti con la dimensione a-territoriale del contesto digitale (c.d. contratti *lawless*)¹⁵.

Con l'espressione *smart contracts* (ma sarebbe più corretto discorrere di *smart legal contracts*) devono, quindi, intendersi quei contratti "intelligenti"¹⁶ (secondo l'espressione in parola) e "autosufficienti", nel senso di *self-executing*, che rifuggono da interventi esterni, giovandosi di regole proprie funzionalmente destinate al complesso delle attività negoziali¹⁷. Risulta così preferibile utilizzare tale denominazione per riferirsi ai veri e propri contratti completamente automatizzati¹⁸, o in cui è l'automazione a costituirne il nucleo essenziale¹⁹, ben oltre la fase della negoziazione.

Sono definibili, pertanto, *smart contracts* quei contratti che assolvono alla funzione di eseguire specifiche azioni volute dalle parti al verificarsi di predeterminate condizioni che vengono inserite all'interno del codice algoritmico, seguendo la semplice regola logico-algoritmica del «*if...then*»²⁰, che di per se stessa ha tutte le potenzialità per esprimere, in tutto o in parte, un programma contrattuale²¹.

Le principali caratteristiche tecnologiche degli *smart contracts* "conclusi" ed "eseguiti" sulle DLT²² si possono sintetizzare in tre nuclei principali: innanzitutto, immodificabilità e sicurezza dei dati inseriti²³; poi, trasparenza determinata dall'accessibilità alle informazioni contenute nel registro; infine, facile tracciabilità delle operazioni effettuate.

Si può, dunque, affermare come lo *smart contract* si differenzi da fenomeni tecnologici ad esso affini, come i c.d. *algorithmic contract*²⁴, la cui peculiarità risiede, invece, nel fatto che alcune condizioni contrattuali vengono determinate automaticamente dall'algoritmo, rappresentando un semplice modello a sé stante di negoziazione²⁵.

Infatti, è solo attraverso l'automatizzazione del contratto, insieme con il ricorso alla tecnologia *blockchain*, che si realizza una completa tracciabilità delle informazioni e dei dati delle varie operazioni economiche e si assicura la certezza dello scambio, oltre che l'adempimento delle prestazioni. In molti casi, poi, lo *smart contract* assolve a più generali esigenze di certezza tramite

effetti di tipo accertativo, se non addirittura di certificazione o asseverazione di fatti e circostanze, proprio sfruttando la creazione o l'inserimento nel registro distribuito di certi documenti o attestazioni (tramite l'attività dell'"oracolo") di quanto verificatosi "all'esterno" del contratto; cionondimeno va rilevato come, in questi casi, sarebbe più corretto parlare di meri protocolli o programmi per elaboratore di natura non contrattuale²⁶.

Gli *smart contracts* propriamente intesi si caratterizzano per il fatto che, avendo le parti determinato le condizioni contrattuali, non risulta esservi alcun margine di manovra per eventuali interventi successivi. Lo spazio riservato all'autonomia privata sembrerebbe, pertanto, ridursi alla sola fase delle trattative, data la forza *self-executing* di tali protocolli informatici. In questi termini, l'esecuzione del codice algoritmico andrebbe a coincidere con il momento di conclusione del contratto, nel rispetto dei requisiti imposti dall'art. 1326 c.c.²⁷.

Su un piano giuridico, si potrebbe altresì ipotizzare la conclusione del contratto mediante esecuzione della controparte negoziale, secondo il modello dell'art. 1327 c.c.²⁸. Da un punto di vista pratico, una volta che un utente abbia immesso nella catena di blocchi la propria offerta contrattuale, alla parte interessata a concludere quel determinato contratto spetta semplicemente aderire, dandone immediata esecuzione²⁹, eliminando di fatto i rischi connessi tramite una tecnologia che, in definitiva, assicura una accentuata oggettivazione delle scelte dei contraenti³⁰.

I codici algoritmici predeterminati dalle parti, dunque, impongono l'adempimento, senza la possibilità di intervenire successivamente in via modificativa. Data la decentralizzazione dei sistemi *blockchain* sarebbe necessario il consenso di (quasi) tutti i singoli blocchi al fine di poter apporre anche una singola modifica alla catena. Ogni nodo, infatti, detiene al proprio interno una copia del registro in cui è inserito rendendo tale tecnologia fortemente impermeabile a frodi esterne. Questo determina, di-

fatti, una presunzione di immodificabilità e sicurezza del sistema utilizzato e dei dati (informazioni) trattati³¹.

Ne deriva l'esclusione dell'ipotesi stessa di eventuali sopravvenienze contrattuali in quanto tali, poiché se dovessero essere previste in sede di conclusione del contratto, non potrebbero qualificarsi come sopravvenienze, ma piuttosto come mere condizioni prevedibili dalle parti stesse. Anzi, proprio con riferimento alla fase rimediale, è stato evidenziato come gli *smart contracts* possano essere programmati dalle parti contraenti proprio includendo elementi esterni rispetto a quelli già previsti nell'accordo, favorendo così una gestione di eventuali sopravvenienze senza rischi per la stabilità dei termini contrattuali³².

L'ipotesi inversa, invece, risulta essere difficilmente inglobabile all'interno del protocollo informatico data la sua rigidità e la (quasi) assoluta immodificabilità *ex post*³³.

Per comprendere appieno la portata applicativa e apprezzare le potenzialità degli *smart contracts* basta evidenziare come essi abbiano la peculiarità di essere *self-enforceable* proprio perché una volta che il protocollo informatico è concluso, non c'è possibilità di non adempiere alla propria prestazione³⁴. Infatti nello *smart contract* l'esecuzione delle azioni non dipende dall'adempimento delle prestazioni da parte dei singoli contraenti, ma dal mero processo automatizzato previsto dal codice algoritmico³⁵.

Una volta raggiunto l'accordo tra le parti attraverso un processo di identificazione tramite autonome chiavi crittografiche, il contratto si reputa concluso e, da quel momento, immodificabile³⁶, rendendone certa l'esecuzione delle prestazioni previste³⁷.

2. La questione della predeterminazione delle clausole contrattuali traducibili in linguaggio algoritmico e il ruolo dell'oracolo

Esaurita, dunque, la panoramica generale del fenomeno, un aspetto sul quale è necessario soffermarsi è quello della prede-

terminazione delle clausole contrattuali e della sottesa rigidità dei codici algoritmici che compongono uno *smart contract*.

Le condizioni contrattuali devono essere tradotte in un linguaggio algoritmico³⁸, che possa operare nel protocollo³⁹, ragion per cui non sono ammesse formule ampie, oscure o ambigue⁴⁰.

L'esigenza di predeterminare un orizzonte semantico chiaro e ben definito impone un maggior grado di certezza sulle future prestazioni da compiersi⁴¹, portando con sé un evidente difetto di flessibilità⁴², con un inevitabile stato di approssimazione negoziale, a favore, però, di un effetto deflattivo del potenziale (tradizionale ben noto) contenzioso.

L'intrinseca finalità di rendere obiettivo il significato delle determinazioni negoziali, che condurrebbe⁴³ persino a ritenere residuale l'applicazione delle norme sull'interpretazione dei contratti di cui agli artt. 1362 c.c. e seguenti, incontra, difatti, un limite nello stesso linguaggio binario alla base dei codici algoritmici. Si pensi ad una polizza che stabilisca tramite *smart contract* rimborsi in caso di pioggia durante un viaggio o un evento all'aperto. Ebbene cosa accadrà se anziché piovere invece dovesse grandinare? Il soggetto assicurato riceverà il rimborso? Chi decide se l'evento grandine sia un fenomeno assimilabile alla pioggia e ne dovrà conseguire lo stesso effetto auto-esecutivo? E se sono state previste, ad esempio, altre "circostanze eccezionali"⁴⁴ chi le stabilirà ove esse non siano meglio dettagliate nel codice algoritmico in cui il contratto è stato tradotto? Come tradurre principi come quello di giusta causa, ragionevolezza, buon costume, ordine pubblico, solidarietà, equità, ecc...? L'inadeguatezza dell'algoritmo a ragionamenti c.d. "per valore"⁴⁵ e con esso la questione dei limiti "strutturali" del linguaggio del diritto appare in tutta la sua evidenza⁴⁶.

Si pone oltretutto un problema di comprensibilità degli *smart contracts*, poiché il linguaggio umano viene sostituito da un codice informatico⁴⁷, la cui intelligibilità è oscura ai soggetti

non esperti della materia, per certo inintelligibile al giurista più raffinato⁴⁸.

Centrale nel funzionamento dello *smart contract* risulta allora il ruolo di tramite tra il mondo reale e quello algoritmico dei protocolli informatici, svolto dal c.d. “oracolo”, ovvero una sorta di “sensore” esterno (sia esso un *software* o programma informatico o persino una persona fisica) a cui è attribuito il compito di certificare l’avverarsi delle condizioni poste alla base del regolamento contrattuale, andando a costituire l’*input* di attivazione delle prestazioni automatizzate previste nel contratto⁴⁹.

Alla luce di queste considerazioni, è lecito interrogarsi sulle conseguenze derivanti da un errore di valutazione compiuto dall’oracolo⁵⁰ che abbia, quindi, determinato l’esecuzione di alcune prestazioni secondo il codice algoritmico. Al riguardo andrebbe presa in seria considerazione la possibilità di una divergenza tra quanto registrato dall’oracolo in una valutazione del mondo reale “errata” (allorché, ad esempio, in caso di malfunzionamento manchi di rendere prontamente le informazioni necessarie) o “distorta” (come quando trasferisca informazioni fallaci, siano esse dovute al sistema informatico o a manipolazioni ad opera di terzi) e gli automatismi delle *blockchain* caratterizzate dall’auto-esecutività e dalla non modificabilità⁵¹.

La questione andrebbe allora posta in modo diverso, dovendosi riguardare non alla fase di esecuzione del contratto ma a quella della sua formazione, con specifica attenzione alla fase della necessaria scelta, costruzione e programmazione dell’algoritmo utilizzato, tanto più quando l’uso della tecnologia è affidata ad una sola delle parti contranti. Ed è rispetto a questa fase che occorre ragionare in merito all’accertamento dei più tradizionali vizi della volontà⁵².

Si tratterebbe in ogni caso di una prospettiva invalidatoria che appare di difficile configurazione, avendo acquisito come elemento caratterizzante la fattispecie degli *smart contracts* l’im-

possibilità per un contratto “generato” (ma anche “governato”) dall’algoritmo di poter essere affetto da errore, dolo, e men che mai violenza o contrarietà alla correttezza e buona fede⁵³.

Lo *smart contract* «mette fuori gioco»⁵⁴, innanzitutto, le auto-difese contrattuali, in quanto l’effetto esecutivo si produce automaticamente (alla trasmissione di un determinato impulso) secondo la regola già richiamata dell’*if-then* che paralizza tutte le possibili eccezioni dell’onerato⁵⁵, tanto da potersi dire che nella stipula sia insita un’implicita rinuncia alle eccezioni sospensive⁵⁶.

In effetti, proprio la simultaneità tra gli adempimenti e l’impossibilità di accedere agli strumenti di autotutela riducono il rischio di condotte dilatorie ed escludono che l’acquisizione della prestazione sia frustrata da eccezioni, talora strumentali, sollevate dal debitore. Parimenti alle eccezioni invalidatorie, risultano precluse all’onerato l’eccezione di avvenuto pagamento, di novazione, di remissione, di compensazione, di confusione, di impossibilità sopravvenuta o di transazione, proprio per l’insensibilità dell’esecuzione automatizzata all’«esigenza di effettività dell’autotutela mediante eccezioni» che rappresenta il fondamento della fattispecie in esame⁵⁷.

Tuttavia, se si accetta l’ipotesi di un malfunzionamento dell’oracolo che trasmetta in modo erroneo allo *smart contract* eventi nella realtà non verificatisi è indubbio che ciò produca in via automatica anche un “indebito” adempimento «della prestazione collegata senza che il debitore possa eccepire alcunché»⁵⁸.

Poiché le operazioni registrate nella *blockchain* formano un “blocco” della catena che, una volta validato, non può essere cancellato né modificato (se non tramite un processo tecnicamente ed economicamente difficilmente sostenibile, attraverso il principio del 50%+1 dei blocchi costituenti la catena), ne deriva l’impraticabilità di rimedi non solo correttivi (come quelli di rettifica di un errore di calcolo *ex art.* 1430 c.c.) ma anche solo

manutentivi di conservazione dell'assetto contrattuale; si pensi, in tal senso, alla riduzione della controprestazione in caso di impossibilità parziale (art. 1464 c.c.)⁵⁹.

Potrebbe sostenersi, allora, l'applicabilità dell'azione generale di arricchimento *ex art.* 2041 c.c., con l'inserimento di correttivi *ex post* o di forme rimediali successive capaci di intervenire al di fuori delle DLT e degli *smart contracts*⁶⁰ e “non dentro”, come pure lascerebbe intendere la Risoluzione del Parlamento europeo sugli *smart contracts* del 2020⁶¹.

Non a caso tale Risoluzione, laddove riprende testualmente in più parti l'espressione “contratti intelligenti”, evidenzia come essi siano utilizzati in diversi settori economici «senza un adeguato quadro giuridico». Partendo dal presupposto che «esistono incertezze in merito alla legittimità di tali contratti e la loro applicabilità in situazioni transfrontaliere» tramite la Risoluzione il Parlamento «invita la Commissione a valutare lo sviluppo e l'utilizzo delle tecnologie di registro distribuito, comprese le *blockchain* e, in particolare, i contratti intelligenti, a fornire orientamenti atti a garantire la certezza del diritto per le imprese e i consumatori, segnatamente per le questioni riguardanti la legittimità, l'esecuzione dei contratti intelligenti (...) e a presentare proposte per l'appropriato quadro giuridico».

3. Lo *smart contract* come contratto asimmetrico: profili di tutela del consumatore e della concorrenza

Risulta evidente quanto gli *smart contracts* possano rappresentare strumenti utili a ridurre i tempi ed i costi legati alle singole operazioni economiche⁶². Tuttavia, delicati problemi si appalesano nei rapporti contrattuali che vedono coinvolto come controparte un soggetto consumatore. Si imporrebbe, difatti, in capo a quest'ultimo, un onere non sostenibile di conoscere e saper maneggiare il linguaggio tecnico-computazionale⁶³.

Per tali ragioni, in realtà, la stessa definizione dettata dall'ordinamento italiano consente anche una diversa interpretazione in base alla quale il protocollo informatico si affianca al regolamento contrattuale, fungendo da sua "diramazione automatizzata"⁶⁴. E questo modello, in effetti, ad oggi, risulta molto presente nella prassi degli *smart contracts*⁶⁵.

Alla luce di queste argomentazioni, la tutela del consumatore riemerge in una nuova prospettiva⁶⁶, specialmente nel settore delle assicurazioni. Difatti, nel contesto di un mercato tradizionalmente asimmetrico per entrambe le parti contraenti coinvolte, quale è quello assicurativo, si inserisce l'ulteriore e complessa questione della comprensibilità degli algoritmi e dei processi automatizzati⁶⁷. Si è parlato al riguardo di "asimmetria informatica" intendendosi con tale espressione una carenza cognitiva consistente nella non adeguata conoscenza del linguaggio informatico di uno *smart contract* da parte di uno dei contraenti e segnatamente il consumatore-assicurato, che non sarebbe quindi "capace" di esprimere un consenso consapevole idoneo al perfezionamento di un rapporto negoziale di tale natura⁶⁸. Non pare possibile che la mera traduzione in protocolli informatici di clausole abusive sia idonea a superare i vincoli di protezione della disciplina vigente in materia di tutela del contraente in generale e del consumatore in particolare⁶⁹. Dovrebbe semmai parlarsi, da parte del contraente, di consapevole adesione solamente nell'ipotesi in cui il programma negoziale espresso nel linguaggio algoritmico sia stato elaborato congiuntamente o condiviso da entrambe le parti, ad esempio tramite proprio tecnici programmatori informatici⁷⁰.

Si tratta, come evidente, di una ricostruzione del fenomeno che porta ad escludere il consumatore da questo tipo di contrattazione. Risulta semmai fattispecie tutto sommato analoga a quanto già avviene in diversi campi dei rapporti negoziali B2B, laddove le imprese si affidano ad esperti o specialisti nella redazione di taluni contratti ad alto contenuto c.d. tecnico.

Si pensi, poi, che il mercato assicurativo è tradizionalmente caratterizzato da una situazione di asimmetria informativa anche in capo alle compagnie stesse le quali, per offrire le loro polizze, necessitano di alcune informazioni sull'assicurato per determinarne le caratteristiche di rischiosità⁷¹.

Ciò detto, al fianco dei timori legati alla tutela della *privacy*⁷² del consumatore e alle eventuali nuove forme di discriminazione, non possono negarsi gli evidenti vantaggi in termini di semplificazione, ad esempio nella gestione delle polizze assicurative, grazie al binomio algoritmi predittivi e *smart contracts*⁷³.

La nuova tecnologia ha «un ruolo procompetitivo nella misura in cui la stessa possa essere adottata dalle piccole e medie imprese per raggiungere i consumatori e sia idonea a eliminare la necessità di intermediari, così come a ridurre i costi e a rendere più efficiente il mercato»⁷⁴.

Sotto il profilo del diritto della concorrenza la Risoluzione del Parlamento europeo del 20 ottobre 2020 chiede «alla Commissione di esaminare le modalità per garantire un adeguato equilibrio e parità tra le parti dei contratti intelligenti, tenendo conto delle preoccupazioni private della parte più debole o delle preoccupazioni pubbliche, come quelle relative agli accordi di cartello»⁷⁵. Infatti, «la nuova tecnologia potrebbe creare alcuni problemi nella misura in cui, essendo totalmente trasparente, potrebbe consentire agli agenti di un mercato oligopolistico di coordinarsi tacitamente»⁷⁶.

E in effetti, il trattamento algoritmico dei dati, nell'ottica di un soggetto regolatore o di una autorità di vigilanza, potrebbe rappresentare uno strumento assai efficace per monitorare, ad esempio, l'andamento dei prezzi sul mercato, specialmente nei casi in cui soggetti diversi attuino comportamenti, per così dire, «convergenti»; potrebbero essere anche gli stessi operatori ad avvalersi di tali informazioni, rese accessibili tramite un canale «aperto» di condivisione, senza più necessità di accordi aventi ad

oggetto lo scambio di informazioni riservate, al fine di rilevare i prezzi dei concorrenti, adeguando i propri, operando in sostanza meccanismi di restrizione della concorrenza, paragonabile a forme di collusione tacita sul mercato a danno dei consumatori⁷⁷. Si tratta di «Problemi che potrebbero essere più accentuati in una *blockchain* o in una *DLT permissioned*. Si potrebbero, poi, registrare abusi di posizione dominante nella misura in cui le *blockchain permissioned* rifiutassero di far accedere alcuni soggetti e in tal modo precludessero agli esclusi di competere su quel mercato. Oppure nella misura in cui la *blockchain* imponesse una *transaction fee* eccessiva. Si potrebbe poi pensare a un abuso (...) nell'ipotesi in cui la *blockchain* utilizzasse uno specifico standard non accessibile a tutte le imprese»⁷⁸.

4. Il ruolo dei *big data* nei servizi assicurativi

Quel che è certo è che i sistemi tecnologici basati sull'intelligenza artificiale⁷⁹, unitamente alla maggiore capacità di *storage* ed analisi di enormi quantità di dati⁸⁰, stanno sempre più incidendo sulla vita individuale delle persone, ponendo interrogativi nuovi e determinando profonde ripercussioni in ogni aspetto della collettività⁸¹.

Da questa rivoluzione digitale⁸² non è rimasto estraneo il settore assicurativo, tra i primi ad aver colto le opportunità che le nuove tecnologie, ed in particolare il ricorso ad algoritmi predittivi⁸³ e i codici automatizzati di contrattazione, potessero apportare in termini di efficienza, speditezza delle operazioni, riduzione dei costi e adattabilità⁸⁴.

Va, però, notato che la velocità di evoluzione e trasformazione del mondo digitale ha messo in evidenza l'incapacità del diritto di poter anticipare i cambiamenti, dovendo ricorrere spesso ad interventi regolatori *ex post*⁸⁵, talvolta privi di una sottesa progettualità uniforme.

Le trasformazioni dettate dalle nuove tecnologie e dalla digitalizzazione di ampi settori economici non sono, tuttavia, prive di rischi: questi, per un verso, vanno correttamente coniugati alle esigenze di tutela e, per altro verso, equilibrati con gli interessi e diritti che fanno capo ai soggetti coinvolti, sia sul lato dei consumatori sia sul lato delle imprese⁸⁶.

Risulta oggi, oramai, evidente come i dati personali rappresentino il motore di questi nuovi paradigmi economici, i quali fanno discorrere gli studiosi di *data-driven economy*, concetto che sintetizza le nuove sfide poste dai *big data* e dall'uso di criteri algoritmici di predizione e personalizzazione. Dati visti come materiale grezzo⁸⁷ da analizzare al fine di indirizzare al meglio gli investimenti e le innovative soluzioni del mercato unico digitale, nonché quali veicolo di nuovi equilibri economico-giuridici che pongono al centro del rapporto il consumatore/cliente⁸⁸.

Questo approccio offre soluzioni molto efficaci in termini di accuratezza di analisi della clientela e di capacità di flessibilità al caso concreto in relazione alle specifiche esigenze, consentendo di sviluppare una capacità previsionale tale che le imprese assicurative sono in grado di offrire ai clienti (anche potenziali) servizi con proposte commerciali che, con elevata probabilità, essi accetteranno. L'impiego dei *big data* insieme con i modelli algoritmici "intelligenti" ha permesso agli assicuratori una suddivisione dei potenziali clienti in base alla fascia di rischio di appartenenza, con una precisione prima d'ora inimmaginabile, cosicché la conseguente tariffazione personalizzata ha permesso alle compagnie assicurative di scegliere i clienti migliori, a discapito di quelli con rischiosità superiore⁸⁹, riducendo (e pressoché eliminando) dal lato dell'impresa l'asimmetria informativa nel mercato in esame⁹⁰.

Da qui l'esigenza di nuove forme di tutela degli utenti⁹¹.

Effetto diretto della digitalizzazione di queste attività e servizi è la presenza sul mercato di operatori che detengono grosse

quantità di dati e che dispongono di una ampia capacità di analisi e previsione.

È singolare notare che, anche se il loro avvento è relativamente recente, immediata è stata la loro abilità nell'impor⁹², scalando le gerarchie in mercati, in cui il ruolo dei *big data* ha assunto connotati sempre più rilevanti, divenendo un vero e proprio fattore di trasformazione del mercato coinvolgendo non solo la contrattazione ma anche le stesse strategie imprenditoriali⁹³. Basti pensare nel settore assicurativo alle c.d. polizze personalizzate o all'apertura del mercato dei servizi di pagamento a nuove categorie di operatori, i c.d. «*Third party providers*» (TPPs).

Nei paragrafi successivi, tenuto conto anche delle potenzialità derivanti da un utilizzo corretto dei *big data*, ci si concentrerà sull'uso degli *smart contracts* nel settore assicurativo con l'obiettivo di presentare alcune prospettive applicative senza tralasciare i rischi sottesi.

5. *Insurtech*: la gestione automatizzata dei servizi assicurativi

Le nuove tecnologie operano su un duplice piano, i cui estremi paralleli afferiscono a tipologie di servizi assicurativi differenti.

Ad oggi, si assiste, da un lato, ad una effettiva e totale disintermediazione e, dall'altro, ad una parallela nuova intermediazione. Risulta opportuno valutare differientemente le attività tradizionali andate semplificandosi attraverso i servizi digitalizzati (si pensi, a mero titolo esemplificativo, ai pagamenti elettronici), rispetto ad attività del tutto nuove, rese possibili unicamente grazie all'intervento di sistemi di intelligenza artificiale capaci di processare un numero indefinito di dati in tempi assolutamente non alla portata per un essere umano, sulla base di fattispecie standardizzate e preimpostate (a tal proposito, si richiamano le attività di consulenza assicurativa automatizzata)⁹⁴; con il rischio magari di non riuscire a tenere debitamente conto delle specificità del caso concreto.

In questo contesto, decisamente favorevole verso l'innovazione tecnologica, vanno collocate le potenzialità applicative degli *smart contracts*, nella loro capacità di facilitare, velocizzare ed automatizzare la negoziazione e l'esecuzione dei contratti.

Tenendo a mente ciò che si è detto precedentemente in merito alle caratteristiche strutturali degli *smart contracts*, anche con riguardo agli interrogativi circa la loro natura giuridica, si deve notare quanto aspetti intrinseci del settore assicurativo si presentano come fortemente compatibili con le caratteristiche di automatizzazione tipica degli *smart contracts*.

Ed è proprio in ambito assicurativo (ma non solo)⁹⁵ che si possono percepire maggiormente gli effetti benefici derivanti dall'applicazione degli *smart contracts* unitamente alla *blockchain* quale loro tecnologia di supporto⁹⁶.

Come noto, l'innovazione tecnologica legata al mondo assicurativo in termini sia di nuove modalità di offerta di servizi e prodotti sia di rinnovamento dei soggetti coinvolti, prende il nome di «*Insurtech*»⁹⁷. Con tale termine si intende il fenomeno giuridico-economico che coinvolge l'insieme di quelle imprese che investono in nuove tecnologie al fine di acquisire ulteriori e più efficaci possibilità di penetrazione del mercato, proponendo nuovi prodotti assicurativi o riformulando le prassi operative di distribuzione e, quindi, in definitiva, la stessa offerta dei servizi assicurativi più tradizionali⁹⁸. Le peculiarità si rinvencono, difatti, non solo nella digitalizzazione, ma anche nella già evocata disintermediazione e nella personalizzazione dei rapporti negoziali⁹⁹.

Se, poi, si considera anche il sopra citato ruolo svolto dai *big data* e dei connessi strumenti di profilazione molto dettagliata degli utenti, potendo conoscerne le preferenze, le scelte e gli stili di vita, si comprende quanto essi siano strategici nel settore assicurativo¹⁰⁰.

È certamente vero che l'assicuratore non può controllare il comportamento dell'assicurato, il quale potrà decidere di

compiere azioni che rendono lo scambio contrattuale più favorevole per sé stesso anche semplicemente riducendo il proprio livello di prudenza per via di una sopravvenuta carenza di interesse riguardo all'incolumità, ad esempio, dell'oggetto assicurato, data dalla consapevolezza di aver trasferito il rischio in capo all'assicuratore¹⁰¹. Tuttavia, lo scopo dell'uso da parte delle compagnie assicurative, nell'ambito della loro attività di impresa, di nuove tecnologie e sistemi di intelligenza artificiale, anche tramite algoritmi c.d. predittivi, è proprio quello di ridurre la possibilità che si verifichi l'evento¹⁰² cui è subordinata l'esigibilità della prestazione in favore dell'assicurato, incidendo sul rischio¹⁰³.

La tracciabilità delle informazioni e dei dati delle varie operazioni economiche connessa alla trasparenza e decentralizzazione¹⁰⁴ delle singole transazioni potrebbe pure facilitare gli scambi, attraverso processi di semplificazione delle trattative contrattuali offrendo sistemi tecnologici vicini alle esigenze dei singoli consumatori¹⁰⁵, specialmente di quei soggetti profondamente coinvolti dalle dinamiche del Web 3.0¹⁰⁶, in cui l'utente assume un ruolo maggiormente proattivo.

A mutare sono non solo le dinamiche del mercato assicurativo, ma anche le gerarchie dei soggetti coinvolti¹⁰⁷. Infatti, ai tradizionali operatori assicurativi si affiancano soggetti "nuovi" che fanno dei dati il loro motore trainante, affermandosi con forza in un mercato che sta mutando i tratti essenziali ed in cui le assicurazioni sono costrette ad adattarvisi per evitare di essere superate in termini di rapidità di risposta ed efficienza dei nuovi modelli di *business*¹⁰⁸.

Nel caso di contratti di assicurazione, le parti, al momento della conclusione dell'accordo, potrebbero inserire all'interno del codice algoritmico le condizioni e gli altri elementi rilevanti del contratto. Le parti, dunque, dovrebbero predeterminare compiutamente le condizioni che l'oracolo dovrebbe poi verifi-

care nel mondo reale al fine di attivare quanto definito nel codice algoritmico¹⁰⁹.

Gli effetti delle prospettive applicative appena delineate sono evidenti: semplificazione e disintermediazione delle procedure, riduzione dei rischi e dei costi operativi connessi alle transazioni, diminuzione dei tempi richiesti ed una maggiore fiducia nella tecnologia utilizzata.

Da questo punto di vista, l'utilizzo degli *smart contracts* potrebbe velocizzare la conclusione delle operazioni assicurative (ma non solo): «mantenendo standard di tutela almeno pari a quelli offerti dalla forma scritta»¹¹⁰. Ciò, sia ben chiaro, nella consapevolezza che al fianco di questi indubbi vantaggi, permangono una serie di rischi per i consumatori, specialmente in tema di sicurezza informatica e di protezione dei dati personali¹¹¹.

Si comprende così quanto necessario sia approfondire la rivoluzione in atto nel settore sul lato dell'offerta dei servizi assicurativi: coperture assicurative flessibili, personalizzabili ed aderenti alle esigenze del singolo assicurato, la c.d. «*Usage-based insurance*» (UBI).

Sempre sul piano della disciplina consumeristica, non devono poi sfuggire i problemi che portano con sé ipotesi in cui un consumatore si vincoli per un certo periodo di tempo tramite contratti, come quelli qui in esame, la cui attuazione è, per l'appunto, irrevocabile e automatizzata e potrebbe contenere modifiche unilaterali a favore del professionista, rispetto a quanto originariamente pattuito¹¹².

Tuttavia, le novità riguardano anche il lato della domanda, proprio perché, parimenti, ad essere mutate sono anche le esigenze degli assicurati, in considerazione di nuovi rischi quali quelli informatici¹¹³.

Basti pensare alla richiesta di polizze assicurative contro i furti di identità digitale, contro gli attacchi hacker nei confronti

di dati di impresa o contro le varie forme di estorsione telematica (ad esempio, le ipotesi di «*phishing*»).

6. Limiti e opportunità degli *smart contracts* nelle assicurazioni

Si assiste, così, ad una ristrutturazione dell'impianto del contratto assicurativo che si trasforma in "sistema" «*user centric*»¹¹⁴.

È proprio il consumatore-assicurato a divenire l'elemento condizionante le stesse dinamiche contrattuali, attraverso forme di definizione dei premi assicurativi fortemente personalizzabili e modificabili nel tempo. Anche queste considerazioni portano ad alcune preoccupazioni e, in particolare, a timori concernenti forme di discriminazione, causate proprio dalla perfetta conoscibilità del soggetto contraente, delle sue capacità di spesa e delle sue esigenze di vita¹¹⁵.

L'operatività di tali protocolli informatici rappresenterebbe una modalità nuova di gestione, in via automatizzata, delle polizze assicurative grazie al rapporto tra il mondo reale, fatto di persone e delle loro scelte, e il mondo crittografico degli algoritmi predittivi, attivato dalle "segnalazioni" dell'oracolo¹¹⁶. Anche in questa sede applicativa la funzione dell'oracolo, infatti, sarebbe centrale in quanto veicolo di trasmissione delle condizioni contrattuali previste dalle parti¹¹⁷.

Si pensi, a titolo esemplificativo, all'utilizzo di uno *smart contract* posto alla base di una determinata copertura assicurativa contro i danni causati dalla circolazione del proprio veicolo che si attiverebbe automaticamente al realizzarsi del sinistro stradale attraverso i sensori inseriti sull'autoveicolo¹¹⁸.

Altra ipotesi applicativa molto interessante, che sfugge anche dal rischio qualificatorio degli *smart contracts*¹¹⁹, è quella adoperata da alcune compagnie assicurative in relazione a contratti assicurativi che coprono il costo dei biglietti aerei a causa di ritardi o cancellazione del volo¹²⁰. In queste ipotesi, una

volta verificatosi l'evento (ritardo o cancellazione del volo), attingendo in via diretta alle informazioni sullo stato del volo fornite dagli oracoli, in automatico si procede al rimborso previsto in sede contrattuale connettendo il conto corrente del consumatore-assicurato con quello dell'impresa.

Si segnala, peraltro, il prodotto assicurativo della *startup* britannica Neos¹²¹, consistente in un'assicurazione domestica continua (attiva 24/24h) realizzata attraverso sensori intelligenti che, al verificarsi di determinati eventi, inviano una comunicazione agli assicurati tramite un'App per *Smartphone*. Si tratta di una particolare applicazione di uno *smart contract* connesso al c.d. *Internet of Thing* (IoT)¹²², che permette di trasmettere informazioni in tempo reale agli utilizzatori.

Lo stesso sistema *blockchain* può rivelarsi utile, poi, «per una più immediata distribuzione dei prodotti assicurativi, per una più celere liquidazione degli indennizzi e per la lotta alle frodi»¹²³.

Messi in luce i possibili sviluppi e le potenzialità degli *smart contracts*, occorre illustrarne i limiti¹²⁴, poiché bisogna considerare, ad esempio, come eventuali errori o vizi¹²⁵ nei dati che vengono analizzati dalle imprese assicurative possano generare distorsione in termini di premi non corrispondenti alle concrete esigenze del consumatore o eccessivi in relazione agli effettivi profili di rischio. O ancora, se un algoritmo dovesse considerare troppo rischioso assicurare una determinata persona o ente, l'impresa assicurativa potrebbe persino decidere di non offrire copertura assicurativa.

Ebbene, ciò comporterebbe l'erosione di elementi caratterizzanti la stessa natura del contratto assicurativo. Infatti, vi sarebbe una implicita eliminazione dell'alea contrattuale tipica delle assicurazioni nonché una profonda riduzione del principio di mutualità che è alla base di tali contratti (*ex art. 1895 c.c.*). I rischi ora delineati si accentuerebbero negativamente nel caso di assicurazioni obbligatorie, ponendo improprie barriere

all'accesso di polizze assicurative richieste dalla legge e necessarie anche al fine di esercitare specifiche attività lavorative.

I rischi attengono alla possibilità di generare criteri di valutazione e profilazione discriminatori che genererebbero *output* non corretti, creando distorsioni legate ad una non corretta raccolta dei dati da parte di sistemi algoritmici.

L'aspetto più controverso risulta, poi, quello legato al possibile impiego fraudolento degli algoritmi negli *smart contracts*¹²⁶. È evidente la difficoltà di controllo degli interessi perseguiti dalle parti (anche con riferimento talora alla loro identificazione) e al rischio che tali tecnologie si trasformino in strumenti di perseguimento di scopi illeciti.

Il rischio è che contratti illeciti o, come si è in precedenza evidenziato sotto il profilo rimediabile, comunque contrari a norme inderogabili (ad es. usurari o elusivi), o contratti rescindibili per l'emergere delle "condizioni inique" di cui all'art. 1447 c.c. o della lesione *ultra dimidium ex art. 1448 c.c.*, risultino intangibili¹²⁷, con sottrazione di fatto anche alla regola dell'art. 2740 c.c. ed all'azione esecutiva dei creditori¹²⁸.

Proprio la difficoltà di individuare meccanismi rimediabili, in ragione delle peculiari caratteristiche dei contratti che girano su DLT, rappresentano il riflesso giuridico di quell'autosufficienza rispetto alla sfera del diritto "positivo" icasticamente rappresentata dalla formula del "*code is law*", con la quale negli U.S.A. si è voluto esaltare l'attitudine delle contrattazioni *smart* a non lasciare spazio d'interferenza al diritto statale¹²⁹.

In proposito, al *Considerando H*, la Risoluzione del Parlamento europeo 20 ottobre 2020, invita a riflettere sul fatto: «che attualmente gli strumenti automatizzati non sono in grado di differenziare in modo affidabile i contenuti illegali da quelli leciti in un determinato contesto e che pertanto i meccanismi per l'individuazione e la rimozione automatiche dei contenuti possono dar luogo a legittime preoccupazioni giuridiche». Si pro-

spetta come necessario intervenire su un sistema negoziale in cui l'algoritmo esegue senza riuscire a distinguere i contenuti illegali da quelli leciti¹³⁰.

Questi non sono ragionamenti meramente futuribili, ma al contrario questioni che sollevano già oggi un serio e concreto dibattito.

Con riferimento alle assicurazioni automobilistiche non vi è dubbio che i sistemi e i dati GPS e degli altri dispositivi di geo-localizzazione, monitoraggio della velocità e simili (c.d. scatole nere)¹³¹, già presenti sul mercato, sono utilizzati proprio per calcolare i premi assicurativi in relazione non solo al numero di chilometri percorsi ma in base agli "stili" e alle abitudini di guida del cliente.

Da un lato l'obiettivo è quello di contrastare meglio frodi e indebiti arricchimenti di clienti *non compliance*, dall'altro l'assicurato medio vedrebbe abbassarsi il costo della sua polizza, derivante dalla riduzione (o comunque più precisa valutazione) del rischio sopportato dall'assicuratore.

Si pensi, nel caso di "RC auto", all'installazione sulle automobili di dispositivi di *on-board diagnostics* quali le «dash-cams», che siano capaci di registrare lo stile di guida dell'utente, o le nuove auto *smart*¹³², che possono analizzare dati ancora più specifici quali la pressione degli pneumatici, il numero di frenate compiute, il superamento dei limiti di velocità o la posizione alla guida¹³³. Tali sistemi sono utilizzati nei contratti cd. *pay-as-you-drive*, in cui l'assicurato, sostanzialmente, acconsentendo al montaggio a bordo del suo veicolo di un dispositivo deputato a controllare modalità e abitudini di guida, permette ad esso di determinare il mutamento delle condizioni applicate, compreso il valore del premio assicurativo¹³⁴. Per non dire di tutti i dispositivi interconnessi, che si hanno oggi in casa, che potrebbero fornire dati e segnalazione collegati ai diversi contratti assicurativi stipulati dagli utenti (si pensi ai citati casi di assicurazioni domestiche e sanitarie)¹³⁵.

Di automatica regolazione del premio si discorre, persino, con riguardo ad alcuni contratti di assicurazione dentale: i c.d. *smart toothbrush*, il cui premio assicurativo è calcolato in modo automatico sulla base delle abitudini e dell'igiene dentale dell'assicurato¹³⁶.

E sempre lo stesso meccanismo è quello che sta alla base del sistema operativo del *car sharing*, in cui lo *smart contract* regola l'utilizzo dei veicoli, ne sblocca l'allarme consentendone l'avviamento e controlla la regolarità del pagamento¹³⁷.

Sempre in ambito assicurativo, si prospetta l'impiego di *smart contracts* nei contratti di "assicurazione sulla vita"¹³⁸ in cui, ricevuto l'*input* (notizia della morte del titolare della polizza), risulterebbe automatico il pagamento ai beneficiari¹³⁹.

È chiaro, quindi, che il settore assicurativo va innovandosi sia sul piano dei prodotti, sia su quello dei modelli negoziali, in grado di rispondere, con le dovute accortezze, ai nuovi bisogni ma anche idonei a garantire servizi su misura degli utenti (si pensi al settore della tutela della salute)¹⁴⁰, anche in virtù della possibilità di determinare più dettagliatamente i profili dei singoli assicurati e, di conseguenza, i profili di rischio nonché l'entità del premio assicurativo da dover pagare¹⁴¹.

Un tale scenario induce a una rimeditazione dello stesso contratto di assicurazione, tenendo conto degli effetti derivanti dall'utilizzo degli *smart contracts* in questo settore. Tanto più laddove si tiene conto che a tutt'oggi l'art. 1898 c.c. stabilisce che grava sull'assicurato l'onere di dare immediato avviso all'assicuratore di tutti i mutamenti suscettibili di aggravare il rischio. Una norma che, per quanto sin qui esposto, risulterebbe quantomeno desueta e di incerta applicazione laddove l'impresa assicuratrice ragionevolmente ritenga, sotto il profilo di valutazione del rischio, di avere elementi di sua conoscenza più affidabili e tempestivamente aggiornati, potendosi persino affermare che l'impresa assicurativa, che sappia avvalersi delle

potenzialità di adozione degli *smart contracts*, di uso dei *big data* elaborati tramite algoritmi predittivi, nonché di dispositivi *IoT*, giunga a conoscere il cliente meglio di quanto quest'ultimo conosca se stesso¹⁴².

L'automatizzazione della gestione delle polizze assicurative (dalla sua fase di conclusione alla fase successive di esecuzione o di rimodulazione) trova così nell'utilizzo delle nuove tecnologie e, in particolare, degli *smart contracts* uno strumento concretamente percorribile e che risponde con facilità alle esigenze del nuovo mercato assicurativo.

Non può, peraltro, disconoscersi, anche oltre gli stessi confini del mercato delle assicurazioni, il peso che in un'economia globalizzata assumono meccanismi di rafforzamento del vincolo contrattuale e certezza dell'adempimento, di velocità ed efficienza delle negoziazioni, da ritenersi tutti alla stregua di veri e propri fattori concorrenziali¹⁴³, che consentono ai contraenti «di non doversi preoccupare dell'esecuzione del contratto»¹⁴⁴.

Negli *smart contracts*, al di là delle attuali dispute definitorie, è la stessa tecnica a farsi contratto nel senso di essere programmi-macchine in grado di gestire i rapporti negoziali, dalla contrattazione su misura del cliente, all'esecuzione della prestazione, fino alla gestione delle sopravvenienze¹⁴⁵.

La riflessione deve essere allora procedere nel solco della ricerca di un adattamento, nella prospettiva della “resilienza” del contratto alle negoziazioni algoritmiche e al ricorso alle nuove tecnologie. D'altronde la *lex cryptographica* alla base della contrattazione algoritmica caratterizzanti gli *smart contracts* è espressione proprio di quella capacità del contratto di darsi nuove regole per modellarsi su esigenze inedite¹⁴⁶.

Se può ammettersi che molte delle questioni tecnico-giuridiche derivanti dagli *smart contracts* possono essere in qualche modo superate considerandoli alla stregua di contratti elettronici redatti ricorrendo ad un linguaggio umano che riproduca il

contenuto dei codici informatici in cui essi si sostanziano, è invece certo che le soluzioni alle questioni giuridiche poste vanno ricercate non oltre i confini che regolano il diritto dei contratti¹⁴⁷, ma al proprio interno, nel prisma dei principi del diritto privato dello scambio¹⁴⁸, allo scopo di ricomprendervi le nuove mutate fenomenologie dei moderni modelli negoziali¹⁴⁹.

Note di chiusura

¹ Per una panoramica sui primi interventi legislativi si veda R. DE CARIA, *The Legal Meaning of Smart Contracts*, in *European Review of Private Law*, vol. 6, 2019, spec. p. 737 ss.

² Le *blockchain* rappresentano una modalità particolarmente trasparente e decentralizzata per la registrazione di elenchi di transazioni. Tali “catene di blocchi” si sostanziano in una tecnologia di registri distribuiti in cui i dati delle transazioni vengono memorizzati sui singoli “nodi” costituenti la catena, gli uni connessi con gli altri, attraverso un processo di comunicazione simile alle reti *peer-to-peer*. Tecnicamente per «registro» si intende uno specifico codice che è atto ad identificare una determinata catena di blocchi. «Ogni nuova transazione da registrare è unita ad altre nuove transazioni per formare un “blocco”, che viene aggiunto come ultimo anello di una lunga “catena” di transazioni cronologiche. Tale catena forma il libro mastro *blockchain* detenuto da tutti gli utenti»; così P. BOUCHER, *Come la tecnologia blockchain può cambiare la vita*, Servizio di ricerca del Parlamento Europeo, Febbraio 2017, p. 7. La *blockchain* («*Distributed Ledger Technology*») è, per l'appunto, un sistema distribuito in cui ogni nodo svolge una duplice funzione: di *client* e di *server*. Questo garantisce una notevole resistenza ad attacchi esterni, in quanto per poter modificare una singola parte della catena, sarebbe necessario ottenere il “consenso” di tutti gli altri nodi. Tali caratteristiche strutturali differenziano tali tecnologie dai tradizionali registri centralizzati o decentralizzati.

Per una analisi dello stretto rapporto tra *blockchain* e *smart contract*, v. S. CRISCI, *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro amm.*, 10, p. 1787 ss.; P. CUCCURU, *Beyond bitcoin: an early overview on smart contracts*, in *International Journal of Law and Information Technology*, vol. 25, 2017, pp. 179-195; C. MILLARD, *Blockchain and law: incompatible codes?*, in *Computer Law & Security Review*, n. 34, 2018, pp. 843-846.

³ P. CUCCURU, *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, in *Nuova giur. civ. comm.*, 2017, p. 113, rileva come «la profonda automazione ed il grado di certezza garantito dagli *smart contracts* si tradurrebbe in un minore dispendio di risorse nella fase negoziale e di esecuzione del contratto, una maggiore velocità ed immediatezza delle prestazioni, nonché una significativa riduzione del rischio di insorgenza di controversie tra le parti».

⁴ In ambito internazionale, la norma che può considerarsi più vicina a quella italiana è stata elaborata dallo stato dell'Arizona, che statuisce che «“*smart contract*” means an event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger». (cfr. Arizona, *House of Representatives Title 44 - Trade and Commerce, 44-7061*). Altra previsione simile, è

quella dello stato del Tennessee, che qualifica lo *smart contract* come un «an event-driven program, that runs on a distributed, decentralized, shared, and replicated ledger and that can take custody over and instruct transfer of assets on that ledger» (cfr. Tennessee, *Senate Bill 1662*, 47-10-201).

⁵ Evidenziano tra gli altri la poca chiarezza di tale definizione E. BIVONA, *Smart contracts e “interferenze” con la disciplina sui contratti: il sistema dei rimedi alla prova degli algoritmi*, in *Persona e mercato*, 2021, p. 776 ss.; e T. PELLEGRINI, *Prestazioni auto-esecutive. Smart contract e dintorni*, in *Comparazione e diritto civile*, 2019, p. 843 ss.

⁶ Il primo comma definisce le tecnologie basate su registri distribuiti, come «le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturealmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili». Nei c.d. registri (*ledgers*) digitali i dati vengono inseriti tramite crittografia a chiavi asimmetrica, che di essi garantisce immodificabilità ed inconfutabile riferibilità all'autore.

⁷ La questione circa la riferibilità degli utenti ad una determinata chiave crittografica (specialmente nei sistemi pubblici) presenta interessanti spunti di riflessione anche in virtù delle Linee guida dell'Agid sulle regole tecniche per la sottoscrizione di documenti elettronici attraverso il «sistema pubblico di identità digitale» (c.d. SPID).

⁸ Sul punto in specie C. PERLINGIERI, *L'incidenza dell'utilizzazione della tecnologia robotica nei rapporti civilistici*, in *Rass. dir. civ.*, 2015, p. 1245.

⁹ A. BENEDETTI, *Contratto, algoritmi e diritto civile transnazionale: cinque questioni e due scenari*, in *Riv. dir. civ.*, 2021, p. 412, richiama sul punto l'analisi di G. OPPO, *Disumanizzazione del contratto?*, in *Riv. dir. civ.*, 1998, I, p. 525 ss. e la replica di N. IRTI, è vero ma... (*Replica a Giorgio Oppo*), *ivi*, 1999, I, p. 273.

¹⁰ Cfr.: N. GUGGENBERGER, *The Potential of Blockchain Technology for the Conclusion of Contracts*, in *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps*, Aa. Vv., Nomos/Hart, Oxford, 2017, p. 85 ss.; P. BOUCHER, *op. cit.*, p. 4.

¹¹ Sulla natura non contrattuale degli *smart contracts* si vedano convintamente: S.A. CERRATO, *Appunti su Smart Contract e diritto dei contratti*, in *Banca borsa tit. cred.*, 2020, I, p. 378 ss.; F. RAMPONE, *Smart contract: né smart, né contract*, in *Riv. dir. priv.*, 2019, p. 1 ss.; P. CUCCURU, *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, *cit.*, p. 107 ss., secondo cui gli *smart contracts* sono semplicemente strumenti per la negoziazione, conclusione e/o automatica applicazione di rapporti contrattuali o relazioni para-contrattuali. Nello stesso senso anche E. LABELLA, *Gli smart contract: riflessioni sulle presta-*

zioni “autoesecutive” nel sistema di blockchain, in *MediaLaws*, 2020, 3, p. 32 ss., per il quale gli *smart contracts* sarebbero «solo una modalità di esecuzione del contratto molto particolare, ma nulla di più. Una modalità di esecuzione che però prescinde da qualsivoglia attività umana, sia delle parti sia dei terzi». Assai critici A. BENEDETTI, *Contratto, algoritmi e diritto civile transnazionale*, cit., p. 415, e F. DI CIOMMO, *Smart contract e (non-) diritto. Il caso dei mercati finanziari*, in *Nuovo dir.*, 2019, p. 257 ss.

¹² G. LEMME, *Gli smart contracts e le tre leggi della robotica*, in *Analisi Giuridica dell'Economia*, 2019, p. 129 ss., spec. p. 147.

¹³ Il riferimento testuale è all'art. 1, comma 6-*quinquies*, TUF: «Per “negoziazione algoritmica” si intende la negoziazione di strumenti finanziari in cui un algoritmo informatizzato determina automaticamente i parametri individuali degli ordini, come ad esempio l'avvio dell'ordine, la relativa tempistica, il prezzo, la quantità o le modalità di gestione dell'ordine dopo l'invio, con intervento umano minimo o assente, ad esclusione dei sistemi utilizzati unicamente per trasmettere ordini a una o più sedi di negoziazione, per trattare ordini che non comportano la determinazione di parametri di negoziazione, per confermare ordini o per eseguire il regolamento delle operazioni» (aggiunto dall'art. 1 del D.lgs. n. 129/2017). Con la considerazione che laddove queste tecniche di negoziazione algoritmica siano utilizzate per concludere contratti, la loro utilizzazione richiede un accordo a monte di natura normativa, anche se come spesso accade, per fatti concludenti (cfr. A. BENEDETTI, *Contratto, algoritmi e diritto civile transnazionale*, cit., p. 420).

¹⁴ Sull'opportunità di questa distinzione A. BENEDETTI, *Contratto, algoritmi e diritto civile transnazionale*, cit., p. 415, per il quale lo «*smart contract* non è tanto un contratto (...) indica piuttosto un *procedimento di gestione* di tutte o alcune del fasi di un contratto», richiamando la più sfumata la posizione di G. CASTELLANI, *Smart Contracts e profili di diritto civile*, in *comparazionecivile.it*, laddove afferma che: «A dispetto del nome, dunque, gli *smart contracts* non sono necessariamente contratti in senso tecnico, rappresentando piuttosto uno strumento volto alla negoziazione e all'esecuzione automatica dei termini di un contratto». Nello stesso senso si pongono F. DI CIOMMO, *Smart contract e (non-) diritto. Il caso dei mercati finanziari*, cit., p. 259, per il quale l'espressione *smart contract* «non ricomprende esclusivamente contratti, ed anzi per lo più riguarda soltanto una o più fasi esecutive di un precedente contratto», nonché I.A. CAGGIANO, *Il Contratto nel mondo digitale*, in *Nuova giur. civ. comm.*, 2018, p. 1152 ss. per la quale: «Gli *smart contracts*, pur non essendo dei contratti in senso giuridico, possono integrare atti della vicenda contrattuale».

¹⁵ Cfr. G. LEMME, *Gli smart contracts e le tre leggi della robotica*, cit., p. 137, e C. AMATO, *La “computerizzazione” del contratto (smart, data oriented, computable e self-driving contracts. Una panoramica)*, in *Eur. dir. priv.*, 2020, p. 1278.

¹⁶ Utili spunti critici in R. PARDOLESI – A. DAVOLA, «Smart contract»: lusinghe ed equivoci dell'innovazione purchessia, in *Foro it.*, 2019, V, c. 195 ss., per i quali gli *smart contracts* «proprio come i supereroi che si rispettino, fanno tutto da soli».

¹⁷ Cfr. C. AMATO, *La “computerizzazione” del contratto*, cit., p. 1259 ss.

¹⁸ «Gli *Smart Contracts* sono stati già regolamentati in molti Stati degli USA (...) e ormai non si dubita più che gli *Smart Contracts* possano essere considerati (a certe condizioni) contratti»; così M. MAUGERI, *La Risoluzione del Parlamento europeo del 20 ottobre 2020 sugli Smart Contracts nella prospettiva del diritto dei contratti e della concorrenza*, in *Contr. impr. Eur.*, 2021, 1, p. 26, che richiama lo studio di L.A. DI MATTEO – J. JANG, *Blockchain-Based Financial Services and Virtual Currencies: United States*, in *EuCML*, 2019, p. 251.

A sostegno della natura contrattuale degli *smart contracts* si esprimono pur con sfumature diverse: L. PAROLA - P. MERATI - G. GAVOTTI, *Blockchain e smart contract: questioni giuridiche aperte*, in *Contratti*, 2018, p. 683 ss., secondo cui lo *smart contract* è un contratto digitale, autoeseguibile e irrevocabile; e in particolare D. DI SABATO, *Gli smart contracts: robot che gestiscono il rischio contrattuale*, in *Contr. impr.*, 2017, p. 386 ss., la quale evidenzia come «il fenomeno appare, in ogni caso, agevolmente inquadrabile nell'ambito della disciplina generale del contratto».

Critico M. GIACCAGLIA, *Considerazioni su Blockchain e Smart Contratti (oltre le criptovalute)*, in *Contr. impr.*, 2019, p. 941 ss., secondo cui sia le posizioni dottrinali che propendono per la natura contrattuale sia quelle che negano tale natura allo *smart contract* sono parziali e insufficienti. Per un quadro delle differenti posizioni si rinvia a G. SALITO, voce *Smart contract*, in *Dig. disc. priv.*, Sez. civ., Agg., Utet, Torino, 2019, p. 393 ss.

¹⁹ Cfr. F. GHODOOSI, *Contracting in the age of smart contracts*, in *Washington Law Review*, 2021, p. 58: «What is smart about smart contracts? The answer lies in the possibility of automatic execution using algorithmics and codes».

²⁰ Sugli *smart contracts* come protocolli autonomi capaci di incorporare regole, prive di qualsiasi connessione con un substrato legale si veda: L. LESSIG, *Code and Other Laws of Cyberspace*, Basic Books, 1999; e ancor prima, J.R. REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, in *Texas Law Review*, 3, 1998.

²¹ Tale regola del “se→allora”, tipica dei linguaggi di programmazione, tende a coincidere con la regola logico-giuridica del «se A, allora B». Sul punto condivisibilmente argomenta S. ORLANDO, *Profili definitivi degli “smart contracts”*, in R. CLARIZIA (a cura di), *Internet, contratto e persona. Quale futuro?*, Pacini, Pisa, 2021, p. 41 ss., spec. p. 50.

²² Sul punto, occorre precisare che i registri distribuiti DLT sono il più vasto *genus*, di cui la *blockchain* non costituisce che una *species*.

²³ In tal senso A.C. NAZZARO, *Blockchain e assicurazioni*, in A. NAZZARO – S. LANDINI, *Commentario del Codice civile - Dei singoli contratti - Leggi collegate*, vol. III, Utet, Torino, 2020, p. 163, nota 7, la quale sottolinea come il fatto che in ogni blocco sia presente parte della stringa alfanumerica del blocco precedente dia garanzie di immodificabilità. Si consideri che ogni blocco contiene solo una frazione dell'intera operazione negoziale, dalla fase precontrattuale a quella esecutiva, e l'avvio della procedura assicura l'inesorabile continuazione di tutto il processo.

²⁴ L.H. SCHOLZ, *Algorithmic Contracts*, in *Stanford Technology Law Review*, 2018, p. 20 ss.

²⁵ Cfr. per un esame anche delle figure affini M. MAUGERI, *Smart Contracts e disciplina in tema di contratto*, in *Oss. dir. civ. comm.*, 2020, p. 375 ss., la quale esamina diverse possibili tipologie di *smart contract*.

²⁶ Si richiama qui la posizione di G. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. proc. civ.*, 2018, p. 443 ss., che opera una distinzione tra *smart contracts* intesi come meri atti esecutivi di un contratto e *smart legal contracts* aventi natura contrattuale. Concorda nel distinguere le due "tipologie" di *smart contracts* anche S. ORLANDO, *Profili definitivi degli "smart contracts"*, cit., p. 48. Su tale distinzione ritornano G. FINOCCHIARO - C. BOMPRESZI, *A legal analysis of the use of blockchain technology for the formation of smart legal contracts*, in *MediaLaws*, 2020, 2, p. 111 ss., evidenziando che solo gli *smart legal contracts* presentano natura contrattuale, mentre lo *smart contract* inteso in senso informatico deve essere considerato alla stregua di un programma informatico che, al verificarsi di certe condizioni, è capace di essere eseguito in modo automatico. Concorda con tale posizione A. CINQUE, *Gli smart contract nell'ambito del fintech e dell'insurtech*, in *Jus Civile*, 2021, 1, p. 187 ss., la quale sostiene che solo gli *smart legal contracts* sono da intendersi alla stregua di accordi contrattuali, redatti e conclusi, parzialmente o totalmente, in forma digitale.

²⁷ G. GITTI, *Robotic transactional decisions*, in *Oss. dir. civ. comm.*, 2018, p. 662.

²⁸ Di cui già si è detto in E. BATTELLI – E.M. INCUTTI, *Gli smart contracts nel diritto bancario tra esigenze di tutela e innovativi profili di applicazione*, in *Contr. impr.*, 2019, p. 931.

²⁹ *Contra* S. ORLANDO, *Profili definitivi degli "smart contracts"*, cit., p. 53.

³⁰ Doveroso il rinvio al noto saggio di C.M. BIANCA, *Acontrattualità dei contratti di massa?*, in *Vita not.*, 2001, p. 1120.

³¹ I dati vengono, difatti, allocati nei "blocchi" (da cui l'origine del nome *blockchain* appunto "catena di blocchi") ed ognuno di essi è ordinato cronologicamente (*timestamps* che indica l'ora e la data di ciascuna operazione) ed identificato da una stringa alfanumerica non invertibile che prende il nome di

hash. Ogni operazione viene validata, archiviata e superata da altri blocchi che impediscono l'annullamento e l'alterazione di quelli precedenti. Si vedano in materia R. GARAVAGLIA, *Tutto su blockchain. Capire la tecnologia e le nuove opportunità*, Hoepli, Milano, 2018; F. SARZANA DI S. IPPOLITO, M. NICOTRA, *Diritto della blockchain, intelligenza artificiale e IoT*, Ipsoa, Milano, 2018, p. 15.

³² Così A. ZOPPINI, *Considerazioni generali su contratto e nuove tecnologie*, in R. CLARIZIA (a cura di), *Internet, contratto e persona. Quale futuro?*, cit., p. 29 ss., spec. p. 32, il quale richiama a sua volta A. MORACE PINELLI, *Il contratto giusto*, in *Riv. dir. civ.*, 2020, p. 663 ss., e G. GIANNONE CODIGLIONE, *Internet e tutele di diritto civile*, Giappichelli, Torino, 2020, p. 12 ss.

³³ Sul punto, si vedano le notazioni di T. PELLEGRINI, *Prestazioni auto-esecutive*, spec. p. 860 ss.

³⁴ Sull'impossibilità di inadempimento, si veda: V. PASQUINO, *Smart contracts: caratteristiche, vantaggi e problematiche*, in *Diritto e Processo*, Annuale giuridico Università di Perugia, 2017, spec. p. 245 ss.

³⁵ «With a smart contract, complete execution of the agreement, including any transfer of value, occurs without any such opportunity to interrupt»; così K. WERBACH - N. CORNELL, *Contracts ex machina*, in *Duke Law Journal*, vol. 67, 2017, spec. p. 332.

³⁶ Sul tema M. DUROVIC - F. LECH, *The Enforceability of Smart Contracts*, in *Italian Law Journal*, 2, 2019, spec. p. 504 ss.

³⁷ T. PELLEGRINI, *Smart contract*, in E. BATTELLI (a cura di), *Diritto private digitale*, Giappichelli, Torino, 2022.

³⁸ Sulla difficoltà di tradurre il tipico linguaggio contrattuale in codice algoritmico, si veda: E. MIK, *Smart contracts: terminology, technical limitations and real world complexity*, in *Law, Innovation and Technology*, 9, 2017, spec. p. 287 ss.

³⁹ Tale processo prende il nome di «*hashing*», cioè da un elemento appartenente al mondo reale si produce un *output* crittografato leggibile dall'algoritmo e traducibile in specifiche azioni nel mondo virtuale.

⁴⁰ «Ambiguity is anathema to computer language»; così M. RASKIN, *The Law and Legality of Smart Contracts*, in *Georgetown Law Technology Review*, 2017, vol. I, spec. p. 325. La questione non è marginale in relazione al fatto che nei contratti spesso le clausole presentano termini ambigui o che alcune tradizionali forme linguistiche sono naturalmente vaghe (si pensi, ad esempio, al concetto di forza maggiore).

⁴¹ Sul punto A. MORACE PINELLI, *Il contratto giusto*, cit., p. 679, sottolinea come attraverso questa «tecnologia si possa recuperare quella certezza e calcolabilità nella gestione dei rapporti, pretesa dal mercato, che il diritto non riesce più ad assicurare sufficientemente, marginalizzando il ruolo del giudi-

ce: l'adempimento del contratto è certo, l'interpretazione del testo non è più richiesta».

⁴² «Parties to a smart contract must sacrifice flexibility, which is an important source of efficiency in their transactional relationship», così J.M. SKLAROFF, *Smart contracts and the cost of inflexibility*, in *University of Pennsylvania Law Review*, vol. 166, 2017, spec. p. 279.

⁴³ M. MANENTE, *L. 12/2019 - Smart contract e tecnologie basate su registri distribuiti. Prime note*, in *Notariato*, 2016, p. 211; L. PAROLA - P. MERATI - G. GAVOTTI, *Blockchain e smart contract: questioni giuridiche aperte*, cit., p. 686.

⁴⁴ Il richiamo icastico alle “circostanze eccezionali” che esonererebbero, ad esempio, una compagnia aerea dal rimborso al cliente a seguito di cancellazione del volo è di A.U. JANSSEN - F.P. PATTI, *Demistificare gli smart contracts*, in *Oss. dir. civ. e comm.*, 2020, p. 37.

⁴⁵ A. CONDELLO, *Metodo giuridico e algoritmo*, in *Riv. crit. dir. priv.*, 2020, p. 347.

⁴⁶ La questione dell'interpretazione del linguaggio dello *smart contract* è ben affrontata da E. BIVONA, *Smart contracts e “interferenze” con la disciplina sui contratti*, cit., p. 786, il cui efficace ragionamento in questa sede si riprende pressoché testualmente.

⁴⁷ L. PIATTI, *Dal codice civile al codice binario: blockchain e smart contract*, in *Cyberspazio e diritto*, 2016, p. 334.

⁴⁸ P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti. Attività e responsabilità*, Edizioni Scientifiche Italiane, Napoli, 2020, 87, sottolinea come, in assenza di un'adeguata alfabetizzazione delle parti coinvolte, il tecnicismo che connota tali operazioni negoziali mina la consapevolezza del consenso prestato dalla parte che subisce le conseguenze della decisione algoritmica.

⁴⁹ A.U. JANSSEN - F.P. PATTI, *Demistificare gli smart contracts*, cit., p. 41, soffermandosi sul ruolo degli oracoli che «forniscono allo *smart contract* le informazioni esterne necessarie per l'esecuzione (ad esempio, il prezzo delle azioni o il prezzo dell'oro)», evidenziano, dal loro punto di vista, come «l'utilizzazione di oracoli si pone in contrasto con l'assunto secondo cui gli *smart contracts* si eseguono automaticamente».

⁵⁰ Laddove l'oracolo sia una persona fisica, si potrebbero applicare le disposizioni in materia di responsabilità, contrattuale o extracontrattuale, a seconda che si consideri il rapporto che lega le parti contraenti e l'oracolo retto da un vincolo contrattuale o privo di tale vincolo. Maggiore approfondimento meriterebbe l'ipotesi in cui l'oracolo sia rappresentato da un software che raccoglie le informazioni *online*, *offline* o su altre *blockchain*, o si tratti di «oracoli hardware che sono invece sensori di posizione o di peso che sfruttano

l'Internet delle cose (IoT) raccogliendo i dati e rendendoli disponibili allo *smart contract* tramite una condivisione crittografata» (così F. IOANNONI FIORE, *Applicazioni dell'intelligenza artificiale e nuovi strumenti di governo del rischio nei contratti assicurativi*, in *Riv. dir. impr.*, 2022, 1, p. 95 ss., spec. p. 108).

⁵¹ Sull'oracolo quale elemento di vulnerabilità degli *smart contracts*, o meglio quale "breccia" nel carattere *self-executing* degli stessi, si veda P. CUCURU, *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, cit., p. 111.

⁵² Di recente A. ALPINI, *I vizi del consenso fra contratto e trattamento dei dati: la riconoscibilità dell'errore*, in *Persona e mercato*, 2022, 2, p. 205 ss.

⁵³ Così A. BENEDETTI, *Contratto, algoritmi e diritto civile transnazionale*, cit., p. 423.

⁵⁴ E. BIVONA, *Smart contracts e "interferenze" con la disciplina sui contratti*, cit., p. 790.

⁵⁵ Sull'impiego "puramente strumentale" delle eccezioni dilatorie, cfr. F. ADDIS, *Le eccezioni dilatorie, in Inattuazione e risoluzione: i rimedi*, in *Tratt. contratto*, a cura di V. Roppo, V, *Rimedi - 2*, Milano, 2006, p. 413 ss., spec. p. 489. In proposito, N. SZABO, *Smart Contracts*, 1994 (disponibile su <http://szabo.best.vwh.net/smart.contracts.html>) esplicitamente individuava tale peculiarità dello *smart contract* come «protocollo di transazione computerizzato che esegue i termini di un contratto» teso a ridurre o eliminare la possibilità di inadempimento.

⁵⁶ D. DI SABATO, *Gli smart contracts*, cit., p. 401, osserva che adottandolo i contraenti «accettano convenzionalmente questa modalità di esecuzione, con ciò rinunciando agli strumenti di autotutela che l'ordinamento mette generalmente a loro disposizione». Sul tema, in generale, L. BIGLIAZZI GERI, *Eccezione di inadempimento*, in *Dig. disc. priv. sez. civ.*, VII, Utet, Torino, 1991, p. 331 ss.

⁵⁷ E. BIVONA, *Smart contracts e "interferenze" con la disciplina sui contratti*, cit., p. 791.

⁵⁸ Si veda F. DI CIOMMO, *Blockchain, smart contract, intelligenza artificiale (AI) e trading algoritmico: ovvero, del regno del non diritto*, in *Riv. infortuni e malattie prof.*, 2019, p. 7; e in particolare M. GIULIANO, *La blockchain e gli smart contracts nell'innovazione del diritto nel terzo millennio*, cit., p. 1029, che evidenzia la necessità di una fonte affidabile di dati, adeguatamente protetta da attacchi *hacker*, e cita efficacemente il caso della c.d. "notizia non veritiera" (si pensi in concreto ad un ritardo di un volo non verificatosi, al quale sia collegato il pagamento immediato ed irreversibile di un corrispettivo a titolo di risarcimento, senza che la compagnia possa impedirlo).

⁵⁹ Per tutti F. DI GIOVANNI, *Attività contrattuale e intelligenza artificiale*, in *Giur. it.*, 2019, 1680, che parla di "impermeabilità" ai rimedi giurisdizionali.

⁶⁰ Sull'opportunità di inserire rimedi *ex post* di «private enforcement», si veda S. KATYAL, *Private Accountability in the Age of Artificial Intelligence*, in *UCLA Law Review*, vol. 66, 2019, p. 54 ss. Sulla possibilità, invece, di inserire clausole che prevedano forme di risoluzione delle controversie insorte tra le parti per questioni non prevedibili in fase di formazione dell'accordo, si rinvia a M. DUROVIC, *How to Resolve Smart Contract Disputes: Smart Arbitration as a Solution*, in N. AGGARWAL, H. EIDENMÜLLER, L. ENRIQUES (eds.), *Autonomous Systems and the Law*, C.H. Beck, München, 2019, spec. p. 25 ss. Per un approccio critico verso l'inserimento di forme rimediali successive che siano sempre riconducibili a sistemi di intelligenza artificiale, cfr. J. M. SKLAROFF, *op. cit.*, p. 300 ss.

⁶¹ Alla Risoluzione del Parlamento europeo del 20 ottobre 2020 “recante raccomandazioni alla Commissione sulla legge sui servizi digitali: adeguare le norme di diritto commerciale e civile per i soggetti commerciali che operano online”, è dedicata la riflessione di M. MAUGERI, *La Risoluzione del Parlamento europeo del 20 ottobre 2020 sugli Smart Contracts*, cit., p. 39.

⁶² Cfr. R. DE CARIA, *op. cit.*, p. 740 ss. Per una riflessione critica circa i costi connessi allo sviluppo degli *smart contracts* e, in particolare, in relazione ai costi di investimento nelle operazioni di *coding*, si veda J. M. SKLAROFF, *op. cit.*, spec., p. 297 ss.

⁶³ A favore di tale ricostruzione, M. DUROVIC - F. LECH, *op. cit.*, spec. p. 509 ss. Cfr. H. SURDEN, *Computable Contracts*, in *46 UC Davis Law Review*, n. 629, 2012, p. 683 ss.

⁶⁴ Questa interpretazione è la linea seguita dalla Jurisdictional Taskforce del Regno Unito (UKJT), che nel suo *statement* del 18 novembre 2019, ha assunto che nella categoria degli *smart contracts* possano rientrare sia i contratti eseguiti attraverso programmi informatici il cui accordo è contenuto altrove in forme contrattuali “tradizionali”, sia i contratti le cui prestazioni ed obbligazioni siano interamente rappresentate dal codice algoritmico. (cfr. UK JURISDICTION TASKFORCE, *Legal statement on cryptoassets and smart contracts*, 18 novembre 2019).

⁶⁵ Nei paragrafi successivi, si elencheranno prospettive applicative che si legano a tale modello interpretativo. Si rimanda in particolare, ai contratti assicurativi di gestione automatizzata dei sinistri.

⁶⁶ Sui rapporti tra la tecnologia degli *smart contracts* con la disciplina consumeristica, si veda A.U. JANSSEN - F.P. PATTI, *Demistificare gli smart contracts*, cit., p. 44 ss.

⁶⁷ Sia consentito rinviare a E. BATTELLI, *Giustizia predittiva decisione robotica e ruolo del giudice*, in *Giust. civ.*, 2020, p. 281 ss. Sul punto, si veda A. MORETTI, *Algoritmi e diritti fondamentali della persona. Il contributo del regolamento (UE) 2016/697*, in *Dir. inf.*, 4-5, 2018, p. 804 ss.

⁶⁸ Sul superamento del “mito del consenso” si veda già S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1971, p. 50 s. (rist. a cura di G. Alpa, Jovene, Napoli, 2018) che, ragionando di problemi posti all'epoca in cui scriveva, già cinquanta anni fa, definiva il consenso un «comodo alibi per un potere pubblico desideroso di eludere i difficili problemi determinati dal trattamento delle informazioni personali a mezzo degli elaboratori elettronici».

⁶⁹ E. BIVONA, *Smart contracts e “interferenze” con la disciplina sui contratti*, cit., p. 788.

⁷⁰ Così S. ORLANDO, *Profili definitivi degli “smart contracts”*, cit., p. 52.

⁷¹ Così G. D'IPPOLITO - E.M. INCUTTI, *I processi decisionali interamente automatizzati nel settore assicurativo*, in *Riv. dir. impr.*, 2019, spec. p. 745.

⁷² Sull'impatto dei *big data* e sui correlativi rischi per la *privacy* nel settore assicurativo, nonché sui possibili rimedi applicabili anche al di fuori della normativa in tema di *data protection*, si veda B. MCGURK, *Data Profiling and Insurance Law*, Hart, Oxford, 2019.

⁷³ Per un'analisi critica si vedano le riflessioni di A.U. JANSSEN - F.P. PATTI, *Demistificare gli smart contracts*, cit., p. 31 ss.

⁷⁴ M. MAUGERI, *La Risoluzione del Parlamento europeo del 20 ottobre 2020 sugli Smart Contracts*, cit., p. 37. Cfr. OECD, *Blockchain Technology and Competition Policy - Issues paper by the Secretariat*, in [https://one.oecd.org/document/DAF/COMP/WD\(2018\)47/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf), del 26 aprile 2018 e consultato il 24 febbraio 2021.

⁷⁵ M. MAUGERI, *La Risoluzione del Parlamento europeo del 20 ottobre 2020 sugli Smart Contracts*, cit., 29.

⁷⁶ Così M. MAUGERI, *op. cit.*, p. 37.

⁷⁷ A. ZOPPINI, *Considerazioni generali su contratto e nuove tecnologie*, cit., p. 38 s.

⁷⁸ Ancora M. MAUGERI, *op. cit.*, p. 37. Preoccupazioni non dissimili esprime P. CUCCURU, *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, cit., p. 107 ss.

⁷⁹ Come ha sottolineato la Commissione Europea per l'Efficienza della Giustizia (CEPEJ), nella «Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziari e in ambiti connessi», adottata il 3 dicembre 2018, l'impatto dei sistemi di intelligenza artificiale sulla vita dei cittadini, intesi nella loro individualità e nelle loro relazioni interpersonali, lavorative ed istituzionali, deve essere improntato a principi di rispetto delle libertà fondamentali, di non discriminazione, di trasparenza, di imparzialità e di equità.

⁸⁰ Ci si riferisce al fenomeno comunemente ricompreso nell'ampio concetto di “*big data*”, ed in particolare di “*big data analytics*”, cioè l'analisi di dati “personali e non” al fine di utilizzarli all'interno di nuove modalità di *business*,

profondamente orientate alla personalizzazione ed alla dinamicità dei servizi e strumenti offerti. La letteratura scientifica sul punto è ampia. Per una disamina generale del fenomeno, sia consentito rimandare ad alcuni recenti contributi: M. DELMASTRO - A. NICITA, *Big data. Come stanno cambiando il nostro mondo*, il Mulino, Bologna, 2019; M. MAGGIOLINO, *I big data e il diritto antitrust*, Egea, Milano, 2018; V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *MediaLaws - Rivista di diritto dei media*, 2, 2018, p. 7 ss.; G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. dir.*, 2019, pp. 199-236; M. OREFICE, *I big data e gli effetti su privacy, trasparenza e iniziativa economica*, Aracne, Roma, 2018; R.H. WEBER, *Data portability and big data analytics. New competition policy challenges*, in *Concorrenza e mercato*, vol. 23, 2016, pp. 59-72; V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *Ten legal perspectives on "the big data revolution"*, in *Concorrenza e mercato*, vol. 23, 2016, pp. 29-58.

⁸¹ Per un approfondimento su come la tecnologia *blockchain* stia determinando cambiamenti radicali nella società, vedi P. BOUCHER, *op. cit.*, *passim*.

⁸² In economia, in relazione alla rivoluzione digitale determinata dall'utilizzo di strumenti innovativi e sistemi di intelligenza artificiale, si parla di «*disruptive technologies/innovations*», cioè tecnologie a tal punto innovative da generare un nuovo mercato, maggiormente efficiente rispetto al precedente e capace di sostituirlo del tutto, proponendo soluzioni alternative e più facilmente accessibili. Questo concetto è stato ideato per la prima volta da un gruppo di professori e studiosi di Harvard (cfr. J.L. BOWER-C.M. CHRISTENSEN, *Disruptive Technologies: Catching the Wave*, in *Harvard Business Review*, vol. Gennaio-Febbraio, 1995; C.M. CHRISTENSEN-M.E. RAYNOR-R. McDONALD, *What Is Disruptive Innovation?*, in *Harvard Business Review*, vol. Dicembre, 2015).

⁸³ Per un inquadramento generale relativo all'utilizzo di algoritmi predittivi nel settore assicurativo, si rinvia a E. BATTELLI, *Big data e algoritmi predittivi nel settore assicurativo: vantaggi e nuovi rischi*, in *Corr. giur.*, 2019, pp. 1517-1526.

⁸⁴ Sui vantaggi che l'utilizzo degli *smart contracts* potrebbero apportare al settore assicurativo (ma anche a quello bancario e finanziario) in termini di trasparenza ed efficienza degli scambi, cfr. A. CINQUE, *Gli smart contract nell'ambito del fintech e dell'insurtech*, cit., p. 196.

⁸⁵ Sul punto, afferma G. ALPA, *Fintech: un laboratorio per giuristi*, in *Contr. impr.*, 2, 2019, spec. p. 377: «il diritto ha dovuto rincorrere le scoperte scientifiche e le applicazioni tecniche ai rapporti economici per poter compiere le scelte più opportune che non potevano essere affidate ai tecnici e agli scienziati».

⁸⁶ V. FALCE - G. FINOCCHIARO, *La digital revolution nel settore finanziario. Una nota di metodo*, in *Analisi Giuridica dell'Economia*, 2019, p. 316.

⁸⁷ «If data is one of the main raw materials of contemporary economics, inevitably there is a “data market”»; così V. ZENO-ZENCOVICH - G. GIANNONE CONDIGLIONE, *op. cit.*, spec. p. 47.

⁸⁸ In tal senso, si parla di «consumer-empowered economy», cioè un impianto economico-strategico calibrato sulle esigenze del singolo consumatore, in cui le sue preferenze, inclinazioni e ricerche costituiscono le linee condizionanti le scelte operate dalle imprese nell’offerta dei loro beni e servizi.

⁸⁹ Si veda in tema A.C. NAZZARO, *L'utilizzo dei big data e i problemi di tutela della persona*, in *Rass. dir. civ.*, 2018, p. 1239 ss.

⁹⁰ La personalizzazione delle polizze richiede che siano predisposte adeguate procedure per evitare il prodursi di inique distorsioni (*unfair bias*). Si veda V. FERRARI - L. PALOPOLI, *Rapporti civilistici e intelligenze artificiali: attività assicurativa*, in P. PERLINGIERI - S. GIOVA - I. PRISCO (a cura di), *Rapporti civilistici e intelligenze artificiali: attività e responsabilità. Atti del quindicesimo convegno Nazionale Sisdic*, Edizioni Scientifiche Italiane, Napoli, 2020, p. 207.

⁹¹ A. BENEDETTI, *Contratto, algoritmi e diritto civile transnazionale*, cit., p. 413.

⁹² S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell’umanità nell’era dei nuovi poteri*, Luiss University Press, Roma, 2019.

⁹³ Per tutti N. ABRIANI - G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale. Dalla fintech alla corptech*, Il Mulino, Bologna, 2021, p. 65, i quali sostengono che gli ampi *dataset* sono stati forieri di nuovi mezzi di produzione e che, in tale prospettiva, l’I.A. debba considerarsi strumento di ottimizzazione dei processi produttivi oltre che strumento decisionale per le imprese.

⁹⁴ Con riguardo, in particolare, all’intermediazione automatizzata in ambito finanziario si veda D. ROSSANO, *Il robo-advice alla luce della normativa vigente*, in F. CAPRIGLIONE (a cura di), *Liber Amicorum Guido Alpa*, Cedam, Padova, 2019, p. 365 ss.; U. MORERA, *Consulenza finanziaria e robo-advisor*, in F. FIMMANÒ - G. FALCONE (a cura di), *FinTech*, Edizioni Scientifiche Italiane, Napoli, 2019, p. 303 ss.; C. RINALDI, *Le analisi finanziarie robotizzate: consulenze, ratings, classificazioni*, in M. CIAN - C. SANDEI (a cura di), *Diritto del Fintech*, Cedam, Padova, 2020, p. 353 ss.; F. SARTORI, *La consulenza finanziaria automatizzata: problematiche e prospettive*, in *Riv. trim. dir. econ.*, 2018, p. 258 ss.

⁹⁵ Per le potenzialità della *blockchain* e degli *smart contracts* nel settore dell’energia ecosostenibile si veda V. CAPPELLI, *Blockchain e fornitura di energia: riflessioni in materia di responsabilità tra decentralizzazione e tutela dei consumatori*, in *Oss. dir. civ. e comm.*, 2019, p. 335 ss.; V. MOSCON, *Tecnologie blockchain e gestione digitale del diritto d’autore e connessi*, in *Dir. ind.*, 2020, p. 137 ss., illustra invece come la tecnologia *blockchain* potrebbe essere utilizzata al fine di fornire supporto alla costruzione di un registro pubblico per i diritti d’autore.

⁹⁶ Si ricorda, infatti, che, essendo la *blockchain* un sistema assimilabile a quelli *peer-to-peer*, risulta superata l'esigenza della presenza di un soggetto terzo che funga da intermediario al fine di poter operare in una specifica transazione. La disintermediazione, come si è già analizzato *supra*, è uno dei tratti essenziali di questa nuova tecnologia. Cfr. G.P. SALA, *Intermediazione, disintermediazione, nuova intermediazione: problemi regolatori*, in M. CIAN – C. SANDEI (a cura di), *Diritto del Fintech*, cit., p. 8 ss.

⁹⁷ Sul tema si vedano: A. LUBERTI – C. TABARRINI, *Insurtech. Una ricognizione empirica e giuridica*, in CONSUMERS' FORUM (in collaborazione con Università degli Studi Roma Tre), *Consumerism 2018. Il cittadino nell'era dell'algoritmo*, Roma, 2018, p. 93 ss.; 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*, Giuffrè, Milano, 2018, p. 319 ss.; V. RICCIARDI, *InsurTech Definition as Its Own Manifesto*, in S.L.B. VANDERLINDEN – S.M. MILLIE – N. ANDERSON – S. CHISHTI, *The Insurtech Book*, Wiley, Chichester (UK), 2018, p. 6 ss.

⁹⁸ V. CHATZARA, *FinTech, InsurTech, and the Regulators*, in P. MARANO – K. NOUSSIA (eds.), *InsurTech: A Legal and Regulatory View*, Springer, Heidelberg, 2020, p. 3 ss.; A. BORSELLI, *Smart Contracts in Insurance: A Law and Futurology Perspective*, ivi, p. 101 ss.; P. TERESZKIEWICZ, *Digitalisation of Insurance Contract Law: Preliminary Thoughts with Special Regard to Insurer's Duty to Advise*, ivi, p. 127 ss.

⁹⁹ Così A. ZOPPINI, *Considerazioni generali su contratto e nuove tecnologie*, cit., p. 33.

¹⁰⁰ G. D'IPPOLITO – E.M. INCUTTI, *I processi decisionali interamente automatizzati nel settore assicurativo*, cit., p. 736, evidenziano che: «uno dei più rilevanti mutamenti che i *big data* apportano al settore assicurativo è la possibilità, tramite l'utilizzo di sofisticati algoritmi predittivi che analizzano dati sempre più ampi sia dal punto di vista quantitativo che qualitativo, di meglio determinare il rischio assicurativo di un particolare individuo».

¹⁰¹ In macroeconomia si distinguono due comportamenti che il soggetto assicurato può porre in essere: *moral hazard* ed *adverse selection*, che si distinguono a seconda del momento dell'operazione negoziale in cui si verificano. Il fenomeno del *moral hazard* attiene ad una fase successiva alla conclusione del contratto ed è definibile come l'incertezza post-contrattuale inerente alle azioni nascoste del soggetto assicurato (sul rapporto tra interesse all'assicurazione e *moral hazard* si veda V. DE LORENZI, *Contratto di assicurazione: disciplina giuridica e analisi economica*, Padova, 2008, p. 192). L'*adverse selection* si riferisce all'incertezza precontrattuale determinata dalla possibile esistenza di un'informazione nascosta dall'assicurato nella fase delle trattative al fine di ottenere un premio più basso. Questi comportamenti potrebbero tradursi in violazioni di buon co-

stume – inteso come insieme di regole ordinate a comportamenti prudenziali – e di ordine pubblico – inteso come insieme di norme ordinate alla pace sociale. Compie questa traduzione in termini giuridici S. LANDINI in A. NAZZARO – S. LANDINI, *Blockchain e assicurazioni*, in *Commentario del Codice civile - Dei singoli contratti - Leggi collegate*, cit., p. 397 la quale sostiene che buon costume ed ordine pubblico siano clausole generali, norme di direttiva che delegano al giudice la formazione della norma di decisione vincolandolo ad una direttiva espressa attraverso il riferimento ad uno standard sociale. Ovviamente tale standard dovrà essere ricavato seguendo i principi dedotti dall'interprete dalle stesse norme di legge (G. FERRI, *Ordine pubblico, buon costume e la teoria del contratto*, Milano, 1970, p. 271); ma per un'opinione secondo la quale si può far riferimento anche a principi metalegali si veda A. TRABUCCHI, voce *Buon costume*, in *Enciclopedia del diritto*, V, 1959, p. 702.

¹⁰² Sul punto si veda S. LANDINI in *Assicurazione e responsabilità*, Milano, 2004, p. 21.

¹⁰³ La compagnia assicurativa tenta di ridurre il rischio effettivo poiché dalla probabilità effettiva del prodursi del danno dipende il totale delle uscite e quindi i margini di guadagno. Per un'analisi matematica dell'equilibrio finanziario dell'impresa assicuratrice si rimanda al più approfondito studio di B. BISES, *Lezioni di scienza delle finanze. (Parte I. L'intervento pubblico nel sistema economico)*, Milano, 2019, p. 134 ss.

¹⁰⁴ La decentralizzazione tipica della *blockchain* non è priva di rischi e di interrogativi aperti. In particolare, è evidente che attraverso questo sistema tecnologico risulti complesso l'identificazione delle parti coinvolte e la loro collocazione spaziale ai fini di una corretta applicazione della legge vigente in quel determinato territorio. Il fenomeno della decentralizzazione rientra nel più ampio flusso del mondo digitale che conduce ad una transnazionalità dei fenomeni e ad un superamento dei confini fisici per approdare ad un unico spazio globale del mondo di Internet.

¹⁰⁵ Sulla sempre maggiore “personalizzazione” dei servizi offerti, al fine di adattarsi al meglio alle esigenze e caratteristiche del singolo consumatore, si veda G. D'IPPOLITO, *Profilazione e pubblicità targettizzata online. Real-Time Bidding e behavioural advertising*, Edizioni Scientifiche Italiane, Napoli, 2021.

¹⁰⁶ Ad oggi, siamo nel pieno dello sviluppo del c.d. Web 3.0, che trae origine dal termine (Web 2.0) coniato da Tim O'Reilly, nel suo lavoro *What is Web 2.0*, per adeguare il Web alle nuove forme di business e ai nuovi modelli emergenti nelle varie piattaforme online. (cfr. O'REILLY, *What is Web 2.0*, O'Reilly Media, 2005).

¹⁰⁷ «L'innovazione tecnologica è dunque il grimaldello attraverso cui imprese che in passato, in un mercato governato da logiche e regole “tradiziona-

li”, non avrebbero avuto possibilità alcuna di affermarsi, assurgono al ruolo di nuovi e aggressivi *players*, scardinando le posizioni dominanti e costringendo gli *incumbents* a investire, a loro volta, nell’innovazione e nel progresso tecnologico e a rinunciare a diritti quesiti, a quote di mercato in precedenza considerate immutabili», così R. MENZELLA, *Il ruolo dei big data e il mobile payment*, in F. MAIMERI - M. MANCINI (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, Quaderni di ricerca giuridica della Banca d’Italia, Roma, 2019, spec. p. 149.

¹⁰⁸ È quanto emerge dalla relazione del già Direttore generale della Banca d’Italia Fabio Panetta durante la riunione annuale dell’Harvard Law School Association of Europe (F. PANETTA, *Fintech and banking: today and tomorrow*, in *Annual Reunion of the Harvard Law School Association of Europe*, 12 maggio 2018, p. 6).

¹⁰⁹ Questo processo di “abbinamento” di eventi del mondo reale computerizzati all’interno dello *smart contract* viene definito in informatica come «*digital twins*», diretto ad indicare la combinazione tra un elemento al di fuori del mondo virtuale (*off-chain*) ed uno corrispondente in formato crittografico. Sul punto, si veda: R. GARAVAGLIA, *Finalità, funzionamento e tipologia di utilizzi delle blockchain*, in F. MAIMERI - M. MANCINI (a cura di), *Quaderni di ricerca giuridica della Banca d’Italia*, Roma, 2019, spec. p. 177 ss.

¹¹⁰ In questi termini S.L. FURNARI, *Validità e caratteristiche degli smart contract e possibili usi nel settore bancario finanziario*, in E. CORAPI - R. LENER (a cura di), *I diversi settori del Fintech*, Cedam, Padova, 2019, spec. p. 106.

¹¹¹ Con specifico riferimento ai rischi per la *privacy* connessi all’utilizzo degli *smart contracts* e della *blockchain*, si vedano: A. GAMBINO - C. BOMPRESZI, *Blockchain e protezione dei dati personali*, in *Dir. inf.*, 2019, p. 619 ss.; M. GIULIANO, *La blockchain e gli smart contracts nell’innovazione del diritto del terzo millennio*, in *Dir. inf.*, 2018, spec. p. 995 ss. e 1014; G. FINOCCHIARO, *Intelligenza artificiale e protezione dei dati personali*, in *Giur. it.*, 2019, p. 1670 ss.

¹¹² Così A. ZOPPINI, *Considerazioni generali su contratto e nuove tecnologie*, cit., p. 33.

¹¹³ Cfr. A. LUBERTI - C. TABARRINI, *op. cit.*, p. 94 ss.

¹¹⁴ Questa sembra essere anche l’impostazione seguita in sede europea dalla Direttiva (UE) 2016/97 del Parlamento europeo e del Consiglio del 20 gennaio 2016 sulla distribuzione assicurativa (cfr. P. CORRIAS, *La direttiva UE 2016/97 sulla distribuzione assicurativa: profili di tutela dell’assicurando*, in *Assicurazioni*, 2017, pp. 9-24).

¹¹⁵ Discriminazione che in economia si suole definire come discriminazione di primo grado. Più nello specifico, si parla di discriminazioni di prezzo in quanto capaci, attraverso sistemi predittivi, di individuare l’esatto prezzo che il consumatore è disposto a pagare (c.d. prezzo di riserva), annullando di fatto il suo *surplus*.

¹¹⁶ Sull'uso di *smart contracts* e della tecnologia *blockchain* nel settore assicurativo, si veda M. ABRAMOWICZ, *Blockchain-Based Insurance*, in P. HACKER - I. LIANOS - G. DIMITROPOULOS - S. EICH (a cura di), *Blockchain and the Constitution of a New Financial Order: Legal and Political Challenges*, Oxford University Press, Oxford, 2019, p. 195 ss.

¹¹⁷ Si tratta di esempi di “*if... then...*” in cui l’“*if*” corrisponde al verificarsi di un evento futuro e incerto, il cd. *trigger event* (ad es. il caso di ritardo aereo o smarrimento del bagaglio), una condizione contrattuale definibile alla stregua di “condizione sospensiva digitale”: così, P. PEACH, *The Governance of Blockchain Financial Networks*, in *80 Modern Law Review*, 2017, p. 1082.

¹¹⁸ In merito all'uso di strumenti automatizzati nella gestione delle polizze assicurative, uno condotto da Deloitte («*The Internet of Things in insurance*») afferma che l'utilizzo di assicurazioni personalizzate attraverso dispositivi di raccolta dati connessi alla guida ridurrebbe i costi connessi al calcolo del rischio assicurativo; diminuirebbe il numero di controversie e imporrebbe comportamenti virtuosi. Lo studio è reperibile in www2.deloitte.com/tr/en/pages/financial-services/articles/innovation-in-insurance-internet-of-things-iot.html.

¹¹⁹ In questi casi lo *smart contract* riproduce in via crittografica un contratto stipulato in via tradizionale tra le parti e serve da processo di automatizzazione delle sue clausole.

¹²⁰ Tra i vari esempi si richiama lo schema assicurativo previsto da AXA (che ha realizzato i c.d. *smart flight insurance products*), consultabile al seguente link <https://www.axa.com/en/magazine/axa-goes-blockchain-with-fizzy>. Si rileva, però, come la stessa Axa abbia ritirato dal mercato la polizza assicurativa “Fizzy”, una piattaforma *permissioned* che si avvaleva della *blockchain* per erogare rimborsi aerei in modo automatico ai clienti, sostenendo che la decisione fosse determinata dal basso grado di accoglienza di tale prodotto riservata dal mercato.

¹²¹ Per maggiori informazioni in merito al prodotto assicurativo realizzato da Neos è possibile consultare: www.neos.co.uk.

¹²² Il termine si riconduce allo studioso inglese Kevin Ashton ed alle sue ricerche sul tema verso la fine degli anni Novanta. Cfr. K. ASHTON, *That ‘Internet of Things’ Thing*, in *RFID Journal*, 2009; G. NOTO LA DIEGA – I. WALDEN, *Contracting for the ‘Internet of Things’: Looking into the Nest*, in *Queen Mary School of Law Legal Studies Research*, Paper No. 219, 2016.

¹²³ Così F. IOANNONI FIORE, *Applicazioni dell’intelligenza artificiale e nuovi strumenti di governo del rischio nei contratti assicurativi*, cit., p. 98, il quale evidenzia che: «Per quel che concerne la distribuzione, essa avviene prevalentemente tramite internet, e la *blockchain* facilita la registrazione, anche a fini probatori, di quel set informativo imposto dalla direttiva 2016/97 dell’UE, nota come IDD. L’adempimento degli obblighi di informazione, documentazione, regi-

strazione e comunicazione può essere guidato da *blockchain*, la quale fungerà da “notaio”, essendo terzo attore negli scambi dei prodotti assicurativi».

¹²⁴ Si segnalano le letture critiche di: F. RAMPONE, *Smart contract: né smart, né contract*, cit., p. 1 ss., il quale afferma che: «*smart contract* è una locuzione che assume vari livelli di significato, nessuno dei quali è riconducibile alla nozione di contratto dell’art. 1321»; F. DELFINI, *Blockchain, Smart Contracts e innovazione tecnologica: l’informatica e il diritto dei contratti*, in *Riv. dir. priv.*, 2019, 2, p. 176 ss.; R. PARDOLESI - A. DAVOLA, «*Smart contract*»: *lusinghe ed equivoci dell’innovazione purchessia*, cit., p. 195 ss.

¹²⁵ Si parla, in tal senso, di *bias* dei dati utilizzati. Più generalmente il *bias* indica un giudizio (o meglio un pregiudizio) frutto di una non corretta interpretazione delle informazioni analizzate, tramite ragionamenti logici non coerenti, che conducono a risultati argomentativi viziati e privi di oggettività.

¹²⁶ E. BATTELLI - E. M. INCUTTI, *Gli smart contracts nel diritto bancario tra esigenze di tutela e innovativi profili di applicazione*, cit., p. 933 s.

¹²⁷ Sul punto T. PELLEGRINI, *op. cit.*, p. 857, il quale invita a riflettere proprio sulla caratteristica degli *smart contracts* e della stessa *blockchain*: «le mani dello Stato non possono arrivare a toccare ciò che gira su un registro distribuito».

¹²⁸ Si veda Trib. Brescia, 18 luglio 2018, n. 7556, in *Giur. it.*, 2019, p. 118, con nota di R. RAZZANTE, *Verso un nuovo diritto dei contratti?*, in cui la condotta di un notaio, il quale si era rifiutato di eseguire un conferimento in natura avente ad oggetto una cripto-valuta, è stata avallata dal giudice proprio sulla scorta (diversamente agendo) di una sostanziale elusione dell’art. 2740 c.c. attesa l’impignorabilità ad opera dei creditori sociali di “beni”, i cui dispositivi di sicurezza ad alto contenuto tecnologico «potrebbero, di fatto, renderne impossibile l’appropriazione senza il consenso e la collaborazione spontanea del debitore».

¹²⁹ L. LESSIG, *Code and other laws of cyberspace*, Basic books, New York, 1999. Una tesi poi ripresa da A. SAVELYEV, *Contract law 2.0: ‘Smart’ contracts as the beginning of the end of classic contract law*, in *Information & Communications Technology Law*, vol. 26, 2017, p. 116 ss.

¹³⁰ M. MANENTE, *L. 12/2019 - Smart contract e tecnologie basate su registri distribuiti. Prime note*, cit., p. 7, rileva come la questione potrebbe essere risolta tramite la “tipizzazione” degli *smart contracts*, ossia un’«imposizione di modelli standardizzati prefissati, la cui causa sia quindi predeterminata».

¹³¹ La cui obbligatorietà (per i nuovi modelli) è disciplinata a livello sovranazionale dal Regolamento europeo 2019/2144 il quale, tra l’altro, rende obbligatori anche la c.d. frenata automatica, denominata ISA (*Intelligent Speed Assistance*), che nell’ottica di ridurre il numero dei sinistri avvisa i conducenti in caso di violazione del limite di velocità e l’inibizione all’avviamento del motore per chi si mette al volante in stato di ebbrezza.

¹³² Il fenomeno delle c.d. *smart cars* è in costante evoluzione; per tutti: G. CALABRESI - E. AL MUREDEN, *Driverless Cars. Artificial Intelligence and the Future of Mobility*, Il Mulino, Bologna, 2021. Per una disamina delle questioni attinenti alla tutela della *privacy* ed alla attribuzione della titolarità dei dati generati dagli autoveicoli connessi a tali dispositivi, si veda S. ZHANG, *Who owns the data generated by your smart car?*, in *Harvard Journal of Law & Technology*, 32, 1, 2018.

¹³³ Si parla di polizze assicurative «*pay as you drive*» per indicare la personalizzazione a cui il mercato assicurativo nel settore automobilistico sta andando incontro (cfr. A. LUBERTI - C. TABARRINI, *op. cit.*, p. 94; si veda anche D. PORRINI, *op. cit.*, p. 329).

¹³⁴ E. BATTELLI, *Big data e algoritmi predittivi nel settore assicurativo*, cit., p. 1517 ss.

¹³⁵ Tali dispositivi di segnalazione e sicurezza rientrano nel concetto di «*Internet of Things*», vale a dire di *devices* connessi alla rete e capaci di interagire a distanza con l'utente od operare in automatico sulla base della valutazione di determinati dati secondo le impostazioni predefinite. *Amplius* in E. BATTELLI, *Insurtech ed evoluzione dell'offerta di polizze sanitarie: tra innovazione tecnologica e nuovi servizi assicurativi in campo medico*, in *Contr. impr.*, 2022, 1, pp. 52-91, spec. p. 57 e 62 ss.

¹³⁶ A. CINQUE, *Gli smart contract nell'ambito del fintech e dell'insurtech*, cit., p. 199.

¹³⁷ G. LEMME, *Blockchain, smart contracts, privacy, o del nuovo manifestarsi della volontà contrattuale*, cit., p. 315.

¹³⁸ Per tutti in tema l'approfondita ricostruzione di P. CORRIAS, *La genesi dell'assicurazione sulla vita nell'ordinamento italiano*, in *Banca borsa e tit. cred.*, 2019, p. 611 ss.

¹³⁹ E. BIVONA, *Smart contracts e "interferenze" con la disciplina sui contratti*, cit., p. 783.

¹⁴⁰ P. CORRIAS, *Diritto alla salute e contratto di assicurazione: premessa ad un'indagine*, in *Responsabilità civile e previdenza*, 2019, p. 753 ss.

¹⁴¹ Svolge un'analisi approfondita della questione: A. BORSELLI, *Smart Contracts in Insurance: A Law and Futurology Perspective*, cit., p. 101 ss.

¹⁴² A. CINQUE, *Gli smart contract nell'ambito del fintech e dell'insurtech*, cit., p. 200.

¹⁴³ G. LEMME, *Blockchain, smart contracts, privacy, o del nuovo manifestarsi della volontà contrattuale*, cit., p. 310.

¹⁴⁴ A.U. JANSSEN - F.P. PATTI, *Demistificare gli smart contracts*, cit., p. 46

¹⁴⁵ Il richiamo è d'obbligo a H. SURDEN, *Computable Contracts*, cit., p. 658 ss.

¹⁴⁶ E. BIVONA, *Smart contracts e "interferenze" con la disciplina sui contratti*, cit., p. 792.

¹⁴⁷ Sul superamento dei tradizionali principi del diritto dei contratti, v. A. SAVELYEV *Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law*, cit., p. 116 ss.

¹⁴⁸ In tal senso D. DI SABATO, *Gli smart contracts*, cit., p. 386.

¹⁴⁹ A favore di tale tesi G. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. proc. civ.*, 2018, p. 441 ss. Significativamente A. BENEDETTI, *Contratto, algoritmi e diritto civile transnazionale*, cit., p. 411, evidenzia come il diritto civile, quasi sempre, sia riuscito «a “dominare” il nuovo, assimilandolo e non facendolo assimilare (...), mai rassegnati a una supina accettazione del dato economico», rappresentando l'evoluzione della tecnica «un fattore di crescita e di modernizzazione del diritto civile»; come scrive P. FEMIA (*Introduzione*, in G. TEUBNER, *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, Edizioni Scientifiche Italiane, Napoli, 2019, p. 9) essa rappresenta «un rivoluzionario banco di prova per la funzione del diritto civile».

L'algo-governance nelle imprese di assicurazione e l'integrazione dei fattori ESG

GIOVANNI BERTI DE MARINIS

SOMMARIO: 1. La *governance* nelle imprese di assicurazione. - 2. L'utilizzo delle nuove tecnologie nel governo societario delle imprese di assicurazione. - 3. *Governance* delle imprese di assicurazione e fattori ESG. - 4. Conclusioni.

1. La *governance* nelle imprese di assicurazione

L'attenzione dell'ordinamento verso la corretta individuazione delle modalità con cui le imprese – e, fra queste, soprattutto quelle maggiormente strutturate – devono organizzarsi internamente, è sicuramente cresciuta nel tempo¹ sulla scorta della convinzione che tale organizzazione incida positivamente non solo in termini di assunzione di decisioni ponderate e corrette, ma anche in relazione alla consapevole individuazione e gestione dei rischi attuali o potenziali ai quali l'impresa è esposta². Tali aspetti diventano ancor più complessi in tutte quelle circostanze nelle quali alle imprese è richiesto anche di affiancare al perseguimento di un profitto societario anche la realizzazione degli interessi delle proprie controparti³. In questi casi, infatti, la corretta articolazione dei processi decisionali all'interno della società è anche strumentale a bilanciare la naturale pulsione del soggetto economico a generare un utile, con le non sempre coincidenti esigenze di conservazione prudenziale del proprio patrimonio strumentale a garantire l'adempimento delle proprie prestazioni nei confronti dei clienti⁴.

Sulla scorta del maggior impatto delle crisi finanziarie⁵ tale esigenza, che si era manifestata prima ed in maniera più intensa

nel comparto bancario⁶, emerge anche nel comparto assicurativo che è stato interessato da un importante flusso di regole volto a razionalizzare e rendere maggiormente efficiente la struttura interna delle imprese del settore⁷.

La dir. 2009/138/CE (d'ora in avanti, *Solvency II*), infatti, valorizza molto i profili organizzativi dell'impresa di assicurazione quali strumenti che, se correttamente orientati alla previsione e gestione del rischio, sono senza dubbio in grado di assicurare la solvibilità dell'impresa di assicurazione⁸ anche in maniera maggiormente performante rispetto all'imposizione – pur prevista – di requisiti patrimoniali «statici»⁹.

L'esigenza che traspare dal nuovo assetto regolatorio è quella di creare le condizioni in funzione delle quali le imprese di assicurazione siano sempre in grado di individuare i rischi ai quali risultano esposte e, quindi, di eliminarne o mitigarne gli effetti negativi agendo in funzione di scelte che siano ponderate e consapevolmente orientate in quel senso. Non si tratta, quindi, di eliminare i rischi che sono tipici di attività economiche tanto complesse ma, piuttosto, di gestirli correttamente tramite una organizzazione interna che risulti adeguata rispetto al livello di complessità dell'attività economica che l'impresa porta avanti¹⁰.

Tale obiettivo, al fine di evitare che impostazioni eccessivamente rigide vadano a penalizzare le imprese dimensionalmente meno rilevanti, viene perseguito tramite un approccio normativo fortemente condizionato dal principio di proporzionalità¹¹ che dovrebbe permettere di non appesantire con eccessivi – ed inutili – oneri di natura organizzativa tutti quei soggetti vigilati la cui sana e prudente gestione possa essere garantita tramite vincoli maggiormente snelli.

Spetterà dunque all'impresa di assicurazione di “autovalutarsi” al fine di modulare la complessità delle proprie strutture interne (c.d.a., quantità e composizione dei comitati endo-con-

siliari, articolazione delle funzioni fondamentali di governo societario ecc.) seguendo, però, le direttrici segnate dalle disposizioni di dettaglio rinvenibili, sul versante domestico, negli artt. 29 ss. c. ass., nel Regolamento IVASS 3 luglio 2018, n. 38 e, in particolare, nella connessa Lettera al mercato del 5 luglio 2018.

2. L'utilizzo delle nuove tecnologie nel governo societario delle imprese di assicurazione

Prescindendo dai tecnicismi collegati ai diversi modelli di governo societario che, in applicazione del principio di proporzionalità, l'impresa di assicurazione dovrà adottare, l'evoluzione della *corporate governance* incontra un ulteriore punto critico nell'impatto che le nuove tecnologie hanno sul mondo economico. La pervasività delle nuove tecnologie nei mercati¹² si è estesa fino a riguardare anche le modalità con cui, all'interno delle imprese di assicurazione, si sviluppano i processi decisionali. Tale fenomeno viene riassunto con il termine di *Algo-governance* o *CorpTech*¹³ che, da tenere distinto rispetto al c.d. *RegTech* che integra invece l'utilizzo delle nuove tecnologie da parte dei Regolatori, impone una seria riflessione in relazione alla non sempre facile convivenza delle disposizioni disciplinanti il governo societario con l'utilizzo di tali nuovi strumenti.

Il tema si presenta di particolare interesse poiché, mentre l'impatto delle nuove tecnologie sui sistemi di produzione e distribuzione che caratterizzano le industrie finanziarie sembra abbia attirato maggiormente l'attenzione degli interpreti¹⁴, non altrettanto può dirsi in relazione alle ricadute che le stesse hanno sull'articolazione dei processi decisionali all'interno delle imprese¹⁵ che, dato il progresso tecnologico, non vengono più solo rese più agevoli dall'utilizzo di sistemi informatici ma, in maniera più o meno intensa, vengono addirittura proposte e raccomandate dalla macchina¹⁶.

Il problema connesso all'utilizzo di nuove tecnologie, dunque, non è tanto dato dalle ipotesi in cui questi nuovi strumenti vengano utilizzati per facilitare l'assunzione di decisioni che sono prese esclusivamente dai soggetti deputati a farlo -come nel caso, ad esempio, dell'utilizzo di piattaforme al fine di svolgere le assemblee sociali o finanche i c.d.a. a distanza¹⁷ e che, pur ponendo il problema dell'accessibilità di tali tecnologie a tutti i soggetti potenzialmente foriero di effetti discriminatori, ha però tendenzialmente semplificato la partecipazione dei soggetti interessati alla vita dell'impresa ed il contestuale esercizio delle loro prerogative¹⁸ - quanto, piuttosto dai casi in cui si utilizzino sistemi complessi di intelligenza artificiale¹⁹ che, capaci di "apprendere" grazie alla loro capacità di processare quantità massicce di dati, dialogano sulla scorta di complessi algoritmi con la realtà che li circonda modificando, di conseguenza, le proprie "scelte" e suggerendole, quindi, a coloro che assumono poi la responsabilità delle stesse²⁰.

Una volta impostato il programma sulla scorta degli obiettivi strategici da perseguire, tali sistemi sono in grado di coadiuvare le persone fisiche nel prendere una certa decisione; proporre o raccomandare l'assunzione di una determinata scelta o, addirittura, sostituirsi all'uomo prendendo una decisione in sua vece²¹.

I vincoli normativi imposti dall'art. 2380-bis, co. 1 c.c., uniti alla complessità anche solo teorica di attribuire soggettività giuridica ad un sistema di IA²² ed alla difficoltà di declinare i requisiti soggettivi (c.d. *fit and proper*) richiesti per le cariche aziendali tarandoli su un algoritmo²³, rende evidente la problematicità di configurare gli stessi quali autonomi centri decisionali²⁴ ma non fanno venir meno la possibilità di utilizzarli quali strumenti di supporto per assumere decisioni strategiche da parte degli amministratori. Il risultato offerto dal sistema di IA - fornitura di dati aggregati o suggerimento/raccomandazione di decisioni - viene quindi fatto oggetto di controllo e verifica

da parte dell'uomo che ovviamente assumerà la responsabilità di scelte che, pur se formate anche grazie all'apporto macchinico, rimangono decisioni imputabili al soggetto giuridico deputato ad assumerle²⁵.

Se non possono avanzarsi dubbi circa il positivo apporto che tali strumenti possono dare nell'assunzione da parte dell'uomo delle decisioni più complesse data la loro capacità di processare in tempi rapidissimi moli estremamente consistenti di dati e di ordinarli ed elaborarli con risultati assolutamente non raggiungibili autonomamente dall'essere umano²⁶, non possono però tacersi le difficoltà ricostruttive che tale utilizzo necessariamente implica.

Tale potenziale attrito risulta tanto più evidente ove lo si analizzi in relazione a tutte quelle imprese - e fra queste quelle assicurative - che, operando in mercati estremamente complessi ed esposti a repentini cambi di scenario economico, sentono maggiormente il bisogno di appoggiare le proprie decisioni su analisi complete e dettagliate dei dati offerti dalla realtà economica²⁷ ma che, dall'altro, si vedono assoggettate a regole che non sempre si conciliano con il loro utilizzo.

Il primo punto di ingaggio è rintracciabile nell'obbligo di agire informati che si concretizza nel richiamare gli organi preposti a prendere decisioni che siano aderenti - sia formalmente che sostanzialmente - alle politiche proprie dell'impresa e che si fondino su un percorso logico trasparente, motivato e verificabile. In questo si concretizza la c.d. *Business judgement rule* che esonera da responsabilità gli amministratori che abbiano effettuato scelte che, seppur foriere di conseguenze negative, appaiano però contraddistinte da ragionevolezza²⁸.

Tale regola, e la conseguente responsabilità derivanti dalla sua violazione, rende difficilmente utilizzabili tutti quei sistemi di IA che non permettano al soggetto che deve prendere la decisione in funzione dei dati elaborati dal sistema di verificarne

origine e genuinità (c.d. *black box*)²⁹. In questi casi, il soggetto rischia di fondare le proprie decisioni sulla scorta di risultati forniti dal sistema di IA – gli *output*– non avendo però la possibilità di conoscere né quali siano i dati utilizzati dal sistema di IA – fra quelli allo stesso forniti (*input*) – per l'elaborazione dei risultati né, tantomeno, il percorso che ha portato il medesimo sistema ad utilizzarli in quel modo³⁰.

Ma il problema, anche se in maniera più sfumata, si pone anche nel caso di utilizzo di sistemi di IA “trasparenti” che, pur offrendo dati intelligibili, impongono comunque al soggetto che se ne avvalga il possesso di specifiche competenze³¹ che gli permettano di assumere consapevolmente la responsabilità delle scelte e di spiegarne l'iter logico agli organi collegiali che conservano comunque un ruolo di controllo critico sulle decisioni dei singoli³².

Sicuramente non meno rilevanti sono poi le conseguenze che l'impiego di tali nuove tecnologie può avere sull'operato delle funzioni fondamentali nelle quali si articola il governo societario delle imprese di assicurazione che, ciascuna per le proprie competenze, hanno il ruolo di individuare e gestire i rischi ai quali l'impresa è esposta e, incardinando un flusso informativo con il board, collaborare alla gestione e mitigazione degli stessi. Anche tali funzioni risultano interessate dall'apporto tecnologico di tali sistemi non solo perché utilizzeranno gli stessi al fine di operare al meglio, ma anche perché l'utilizzo delle nuove tecnologie è esso stesso un rischio che, nelle imprese particolarmente strutturate, va dominato e correttamente gestito³³.

Se dunque tali nuovi strumenti rappresentano affascinanti sfide per aumentare l'efficienza dei processi decisionali nelle imprese assicurative³⁴, impongono però una approccio normativo critico e consapevole anche dei rischi che una apertura tecnologica di tal genere può determinare³⁵. Sullo sfondo si percepisce la seria difficoltà nella quale si trovano i regolatori di

fronte a tale tematica³⁶ combattuti fra l'esigenza di dettare regole precise per l'utilizzo delle nuove tecnologie in tale ambito e quella di evitare che disposizioni troppo rigide che ne frenino l'evoluzione e lo sviluppo³⁷. Tali preoccupazioni sembrano dunque lasciar propendere per approcci regolatori che privilegino strumenti di *soft law* con la precipua finalità di accompagnare gradualmente le imprese interessate verso una integrazione di tali tecnologie che risulti consapevole sia delle opportunità che dei rischi di cui le stesse sono portatrici³⁸.

3. *Governance* delle imprese di assicurazione e fattori ESG

La “virata” verso l'utilizzo di nuove tecnologie in ambito societario che brevemente è stata descritta va letta, come sopra accennato, alla luce dell'approccio *risk based* che dovrebbe caratterizzare l'attività assicurativa in conformità con le indicazioni provenienti dal sistema *Solvency II* che, a sua volta, porta a guardare con occhi diversi i potenziali rischi ai quali l'impresa è esposta e l'impatto che gli stessi possono avere in termini di stabilità dell'impresa. Non vi è dubbio che tale generale tendenza abbia ultimamente visto una crescita di interesse verso tutti quei fattori di natura ambientale e sociale che compongono la galassia dei c.dd. fattori ESG (*Environmental, social and governance factors*) e che concretizzano altrettanti inediti rischi ai quali l'impresa risulta esposta.

Nonostante si tratti di fattori “non patrimoniali” connessi prevalentemente a profili di sostenibilità ambientale e sociale dell'attività economica portata avanti dall'impresa, risultano sempre più evidenti le ricadute economiche positive che possono derivare da un corretto approccio da parte del soggetto economico a tali problematiche³⁹. Va infatti segnalato che la consistenza quantitativa e qualitativa del patrimonio di una impresa può risultare influenzato da elementi quali i cambiamenti cli-

matici in atto, la necessità sempre più insistente di adattare i sistemi di produzione in modo da ridurre l'impatto ambientale degli stessi, l'influenza che la transizione ecologica può avere sugli investimenti che l'impresa ha effettuato e sui relativi rendimenti nonché le non trascurabili ricadute reputazionali che potrebbero generarsi ove l'impresa si dimostri insensibile alle tematiche sopra menzionate⁴⁰.

È stato quindi evidenziato come l'empatia che l'impresa dimostri verso i fattori ESG integrandoli nelle proprie policy aziendali, permetta alla stessa – con particolare riferimento a quelle maggiormente strutturate – di sviluppare una maggiore capacità di prevenire e mitigare i rischi connessi a tali fattori⁴¹ stimolando l'adozione di politiche di “lungo termine” che, orientando l'agire economico dell'impresa verso orizzonti temporali più ampi, liberano la stessa dalla “schiavitù” della ricerca dell'utile immediato⁴².

Tali brevi premesse giustificano la crescente attenzione che lo stesso legislatore europeo e, quindi, nazionale è andato riservando alla regolamentazione di tali aspetti. Nonostante non fossero mancati già in passato elementi che, pur se in maniera velata, lasciassero emergere la rilevanza dei fattori non patrimoniali per l'impresa di assicurazione⁴³, è a partire dalla dir. 2014/95/UE⁴⁴ recepita in Italia con d.lgs. 30 dicembre 2016, n. 254 che si è iniziato ad introdurre regole comuni per gli “enti di interesse pubblico”⁴⁵ in relazione alla c.d. «comunicazione di informazioni di carattere non finanziario». Fra i soggetti interessati da tali disposizioni rientrano, insieme alle altre imprese operanti nei mercati finanziari, anche le imprese di assicurazione e di riassicurazione dimensionalmente rilevanti⁴⁶. Ai sensi di tali disposizioni, si introduce l'obbligo di effettuare una dichiarazione individuale⁴⁷ o consolidata⁴⁸ – di carattere non finanziario da depositare presso il registro delle imprese⁴⁹ – nonché da diffondere al pubblico e da trasmettere a Consob quale autorità

incaricata della vigilanza sul punto⁵⁰ - che contenga le informazioni attinenti le politiche adottate sui temi ambientali, sociali, relative al personale, al rispetto dei diritti umani, alla lotta contro la corruzione attiva e passiva⁵¹ con l'obiettivo di far emergere l'impatto (positivo o negativo) che l'impresa ha su quei fattori ambientali e sociali⁵². La dichiarazione menzionata deve infatti indicare proprio in relazione ai fattori sociali ed ambientali come l'impresa si sia organizzata per gestire tali elementi, le politiche adottate sul punto ed i principali rischi che l'impresa subisce da tali fattori o ai quali espone gli stessi⁵³.

Calando però il discorso nelle specificità del mercato assicurativo⁵⁴ va segnalato che EIOPA aveva pubblicato già in data 30 aprile 2019 un *Opinion on Sustainability within Solvency II* proprio al fine di verificare come le disposizioni della direttiva europea sopra menzionata permettano una corretta valutazione nel calcolo dei requisiti prudenziali –sia sotto il profilo della valutazione degli *assets*⁵⁵ che delle *liabilities*⁵⁶ nonché, di conseguenza, della valutazione delle politiche di investimento⁵⁷, di sottoscrizione⁵⁸ e dei requisiti patrimoniali⁵⁹– dei rischi di sostenibilità che, tuttavia, vengono per il momento delineati esclusivamente quali rischi climatici⁶⁰.

Si tratta di un documento di estremo interesse in quanto mette in evidenza la difficoltà di far dialogare il “sistema” descritto dalla dir. *Solvency II*, tarato su una stabilità economica dell'impresa dipendente pressoché esclusivamente da dati di natura patrimoniale, con l'emersione di tale nuova sensibilità verso l'impatto economico che i rischi ambientali e sociali possono generare. Nonostante la direttiva menzionata stimoli le imprese ad una valutazione prospettica della propria solvibilità, la stessa appare comunque tarata su orizzonti temporale troppo brevi per permettere all'impresa di assicurazione di integrare in tale valutazione anche i rischi ambientali e sociali che risultano apprezzabili solo ponendosi in una prospettiva di lungo termine⁶¹. Pur evidenziando questa difficoltà di fondo, in tale

Opinion si stimolano i soggetti vigilati ad integrare in maniera graduale tali rischi nelle proprie politiche aziendali tramite analisi di scenario e stress test che permettano all'impresa di familiarizzare con l'impatto che l'avverarsi di tali rischi potrebbe avere sulla solvibilità dell'impresa⁶².

A tale generale richiamo che l'autorità europea di settore rivolge al mercato assicurativo, si affianca una presa di posizione maggiormente netta espressa all'interno del *Technical advice* EIO-PA «on the integration of sustainability risks and factors in the delegated acts under Solvency II and IDD» pubblicato anch'esso in data 30 aprile 2019 che, nell'intento di facilitare la creazione di un sistema normativo che spinga le imprese di assicurazione ad individuare e gestire correttamente i rischi di sostenibilità e ad adottare una visione di lungo termine⁶³, per quello che in questa sede interessa, proponeva significative modifiche Regolamento delegato UE 2015/35 che integrava la dir. *Solvency II*

Tali considerazioni hanno trovato terreno fertile nella Commissione UE che, proprio al fine di fare mergere i “rischi di sostenibilità” nel mercato assicurativo, emana il Regolamento delegato UE 2021/1256 che modifica il Regolamento delegato UE 2015/35. Queste novità impongono una riarticolazione della funzione di *risk management* che dovrebbe essere chiamata ad identificare e valutare anche i rischi di sostenibilità⁶⁴ e ad includerli nel sistema di gestione dei rischi tenendo in debita considerazione i fattori ESG nelle relative politiche⁶⁵ e nella valutazione del fabbisogno di solvibilità globale⁶⁶. Una valutazione dei rischi di sostenibilità che appare strumentale a permettere alle imprese di assicurazione anche di integrare gli stessi nella valutazione della sicurezza, qualità, liquidità e redditività del portafoglio nonché di valutare l'impatto a lungo termine che tali fattori possono avere sulle proprie strategie di investimento⁶⁷.

Le modifiche apportate impongono, quindi, una ricalibratura dello stesso governo societario al quale, nei vari livelli nei

quali si articola, viene richiesto di sviluppare una crescente sensibilità verso la “sostenibilità” – per il momento declinata pressoché esclusivamente in termini ambientali ed ecologici -, di accrescere le proprie competenze sui profili evidenziati in modo da poterli correttamente valutare e di contribuire ad orientare le scelte economico/imprenditoriali dei soggetti vigilati verso opzioni sostenibili e di lungo termine⁶⁸.

Se questi sono gli sviluppi emersi al livello europeo, va segnalato come anche sul versante nazionale si registra una certa sensibilità da parte dell'IVASS sul punto che, in attesa di un quadro di regole comuni definite e stabili, ha però già nel Regolamento IVASS n. 38 del 2018 preso atto del potenziale impatto che i rischi connessi a fattori ESG possono avere sul sistema di governo societario. L'art. 4, comma 2 del citato Regolamento, infatti, richiama l'attenzione della governance delle imprese di assicurazione verso la necessità di valutare anche i rischi “di natura ambientale e sociale, generati o subiti, anche secondo una visione prospettica ed in considerazione del fabbisogno complessivo di solvibilità dell'impresa”⁶⁹. Si tratta, evidentemente, di una “porta” che il regolatore nazionale ha lasciato aperta all'integrazione dei fattori ESG nel governo societario delle imprese vigilate e che, alla luce di un'auspicabile e rapida definizione di regole di dettaglio al livello europeo, comporterà sicuramente l'individuazione di disposizioni domestiche maggiormente specifiche e puntuali.

4. Conclusioni

La nuova sfida di creare ambienti economici sostenibili, quindi, si gioca anche sulla corretta articolazione delle strutture societarie all'interno delle quali si formano le decisioni economiche proprio di quei soggetti che, per dimensione e per ruolo svolto all'interno delle moderne economie, sono in grado di impattare

in maniera più consistente sui mercati. Il governo societario, soprattutto nelle suddette imprese capaci di muovere ingenti capitali e di finanziare tramite la loro consistente attività di investimento altre realtà economiche, può infatti contribuire ad orientare i capitali verso impieghi “ecosostenibili” privilegiando scelte che vengano dettate non solo dai pur rilevanti interessi di guadagno immediato, ma che si lascino condizionare anche dal perseguimento di obiettivi non patrimoniali che solo apparentemente appaiono contrastare con i primi. Stesso discorso potrebbe essere fatto, ancora, per le modalità con cui tali imprese selezionano i propri fornitori di servizi (la c.d. *supply chain*) privilegiando coloro che si dimostrino in linea con tali nuove sensibilità.

Valutare razionalmente i rischi ambientali ai quali l'impresa è esposta, contribuisce a dare maggiore stabilità economica alla stessa che, per tempo, è in grado di prevenirne o mitigarne gli effetti adattandosi progressivamente agli stessi. Anche gli investimenti che l'impresa intenda effettuare in attività sottostanti che si dimostrino sensibili alle problematiche della sostenibilità, si dimostrano nel lungo periodo maggiormente proficui generando, così, un doppio effetto positivo: da un lato, l'impresa investe in attività economiche che generano un utile e, dall'altro, orientano i capitali verso imprese che limitano l'impatto della loro attività economica sull'ambiente e sulla società contribuendo, quindi, a creare economie sostenibili.

Perché ciò avvenga, però, è necessario che il “germe” della sostenibilità venga innestato proprio dove nascono le decisioni economico/organizzative delle imprese di assicurazione e, dunque, proprio nelle dinamiche che caratterizzano la *governance* delle stesse. È proprio a questo punto che la sostenibilità incrocia lo sviluppo tecnologico nella misura in cui l'utilizzo di processi algoritmici possa aiutare le funzioni di governo societario e, in ultima istanza, il board ad organizzare ed analizzare i dati

connessi alla sostenibilità in modo da permettere a questi di influire sulle relative decisioni di impresa. Il profilo è tutt'altro che sconosciuto in ambito assicurativo sottolineandosi come la sostenibilità sociale ed ambientale debba essere considerata uno degli obiettivi che necessariamente qualunque sistema di IA deve perseguire⁷⁰.

Non è casuale, in quest'ottica, che già siano stati lanciati i primi sistemi algoritmici che misurano il posizionamento dell'impresa in termini di sostenibilità ed individuano in che maniera la stessa stia perseguendo i propri obiettivi di sostenibilità. Si tratta di sistemi che, in funzione dei dati immessi, vanno a monitorare l'attività di impresa non solo, come accaduto fino ad ora, in relazione a fattori di natura patrimoniale, ma valorizzando quelli di natura non patrimoniale. Si tratta di sistemi complessi che, utilizzati dalle imprese, restituiscono alle stesse una "fotografia" di come le stesse stiano operando sul versante della sostenibilità che dovrebbe permettere al soggetto economico di verificare le scelte fatte ed eventualmente correggerle nella misura in cui si siano rilevante poco efficaci o abbiano generato *performance* inferiori alle aspettative. Oltre a tale già importante funzione, tali sistemi dovrebbero anche riuscire a fornire una visione prospettica dei potenziali rischi ESG ai quali l'impresa risulta potenzialmente esposta in futuro così potendo supportare scelte volte a mitigarne gli effetti⁷¹.

Appare allora evidente l'importanza di poter fare affidamento su sistemi di processamento di dati e di elaborazione di soluzioni che, integrati nelle c.dd. stanze dei bottoni, agevolino la gestione di quella imponente massa di dati che devono essere conosciuti dall'impresa per autovalutare la propria sostenibilità e per migliorare le proprie performance sul punto, nella convinzione che tale attività non rappresenti un mero costo per l'impresa ma che sia, al contrario, una opportunità da cogliere in un mondo economico e sociale sempre più attento a come gli

operatori economici si muovano sul terreno della sostenibilità delle proprie scelte imprenditoriali.

All'interno di economie in cui il successo di una iniziativa economica viene valutato e condizionato anche dall'empatia che la stessa dimostra verso la sostenibilità, l'impresa – qualunque essa sia – deve progressivamente cambiare il proprio DNA per poter sopravvivere in un mercato che, già da ora, sta dando chiari segnali di un profondo cambiamento in questo senso. È altrettanto evidente, però, che anche sulla scorta delle risultanze emergenti da un quadro normativo europeo ancora in corso di formazione⁷², lo sviluppo di tali tecnologie non può scalfire la visione antropocentrica dei nostri sistemi ordinamentali che, pur consapevoli delle positive ricadute derivanti dall'utilizzo di sistemi di tal genere, richiamano comunque l'esigenza di considerarli strumenti di supporto delle attività umane ma mai sostitutivi delle stesse. Tale principio generale, sembra dunque ampiamente riscontrabile anche nell'utilizzo di sistemi di IA all'interno del governo societario delle imprese di assicurazione – ed in generale delle imprese operanti nei mercati regolamentati –, nel quale forse la vera sfida non consiste tanto nell'implementazione di sistemi di IA efficienti – come detto già esistenti e funzionanti – quanto, piuttosto nel creare una classe dirigente fatta di donne ed uomini capaci di maneggiare consapevolmente tali potenti strumenti senza affidarsi ciecamente ed acriticamente agli stessi.

Note di chiusura

¹ Sul punto, diffusamente, R. LENER, *Il ruolo della corporate governance nell'economia globale*, in *Banca impr. soc.*, 2017, p. 3 ss.; P. SINGER e C.A. SIRIANI, *La corporate governance. Elementi, teoria e profili operativi*, Torino, 2015, p. 23 ss.

² V., in tale ottica, le considerazioni di P. MONTALENTI, *Il diritto delle assicurazioni tra ordinamenti nazionali e globalizzazione*, in *Assicuraz.*, 2014, p. 399, il quale pone l'accento sul fatto che solo attraverso una corretta articolazione del governo societario si possa giungere ad una gestione sana e prudente dell'impresa assicurativa.

³ Cfr., S. BUTERA e F. MONTEMAGGIORI, *La governance delle imprese di assicurazione secondo il principio di proporzionalità. Fondamenti internazionali ed europei e regole nazionali*, in *Assicuraz.*, 2018, p. 44, le quali, dopo aver evidenziato la rilevanza che in generale assume il governo societario quale strumento di mitigazione dei rischi, evidenziano che «quello che vale per la sana gestione di ogni impresa assume un particolare rilievo per le imprese del settore finanziario. In tale ambito, il fine prudenziale dell'efficienza di gestione dei rischi rappresenta, accanto al rispetto delle regole di correttezza e trasparenza, l'obiettivo della regolamentazione e supervisione delle Autorità di settore. Ciò allo scopo di contemperare gli interessi degli azionisti con la tutela pubblica del risparmiatore, sia esso depositante, investitore o assicurato, sancita dall'art. 47 della Costituzione».

⁴ Evidenzia la delicatezza del ruolo svolto dal governo societario all'interno delle imprese finanziarie, M. SIRI, *La centralità del governo societario nel sistema di Solvibilità II*, in *Quaderno IVASS n. 11, La riforma del sistema europeo delle Autorità di controllo. La Governance delle imprese di assicurazione. La gestione delle crisi nel settore bancario e assicurativo*, 2018, p. 68 s. secondo il quale in tale settore «il governo societario deve tener conto degli interessi delle altre parti interessate (depositanti, risparmiatori, titolari di polizze di assicurazione vita, ecc.), nonché della stabilità del sistema finanziario, data la natura sistemica di molte istituzioni ed intermediari. Gli interessi dei creditori degli istituti finanziari (depositanti, titolari di polizze di assicurazione sulla vita, beneficiari di regimi pensionistici e, in una certa misura, dipendenti) sono potenzialmente in contrasto con quelli dei loro azionisti. Questi ultimi traggono beneficio dalla crescita della quotazione di borsa e della massimizzazione degli utili nel breve periodo e sono potenzialmente meno interessati ad un livello di rischio troppo basso».

⁵ Cfr., M. BROGI, *Corporate governance bancaria e sana e prudente gestione*, in *Banca impr. soc.*, 2010, p. 283 ss.; P. SCHWIZER, *Le nuove regole di corporate governance e dei controlli interni: quale impatto sulla gestione delle banche?*, *ivi*, 2015, p.

7 ss.; D. BOUZEMARENE, *L'evoluzione della regolamentazione europea in materia di governance delle banche: dalla CRD IV alle Guidelines EBA*, ivi, 2016, p. 3 ss.; A. MIRONE, *Regole di governo societario e assetti statutari delle banche tra diritto speciale e diritto generale*, ivi, 2017, p. 33 ss.

⁶ Sulle analogie e differenze riscontrabili fra il comparto bancario e quello assicurativo in relazione alla disciplina del governo societario, F. VELLA, *Banche e assicurazioni: le nuove frontiere della corporate governance*, in *Banca impr. soc.*, 2014, 289 ss.

⁷ Cfr., P. MANES, *La nuova normativa Solvency II: corporate governance, approccio al rischio e mercato assicurativo europeo*, in *Contr. impr./europa*, 2018, p. 240 ss.

⁸ V., sul rapporto fra governance e solvibilità, L. SELLERI, *L'impatto di Solvency II sull'organizzazione dell'impresa di assicurazione: verso l'organizzazione per processi?*, in *Dir. ed eco. assicurazione*, 2010, p. 615 s.

⁹ V., il considerando n. 29 della direttiva Solvency II: «Taluni rischi possono essere affrontati correttamente solo tramite requisiti di governance anziché tramite i requisiti quantitativi riflessi nel requisito patrimoniale di solvibilità. Un sistema di governance efficace è pertanto essenziale per la gestione adeguata dell'impresa di assicurazione e per il sistema di regolamentazione».

¹⁰ P. MANES, *La nuova normativa Solvency II: corporate governance, approccio al rischio e mercato assicurativo europeo*, cit., p. 248 ss.

¹¹ Cfr., l'art. 41, par. 2 della direttiva Solvency II. Per qualche prima osservazione sul punto, v. D. MARINO e C. CIMARELLI, *Prima lettura delle novità introdotte dal Regolamento IVASS sul governo societario delle imprese e dei gruppi assicurativi*, in *Dirittobancario.it*, 2018, p. 2 s. Il principio in parola orienta le regole di governo societario all'interno di tutti i mercati finanziari. V., sul punto, P. DE BIASI, «One Size Fits All» vs Principio di proporzionalità in ambito bancario e mobiliare, in *Riv. reg. merc.*, 2018, p. 197 ss.; I. SABBATELLI, *Banche di credito cooperativo: requisiti degli esponenti aziendali e principio di proporzionalità*, in *Riv. trim. dir. econ.*, 2018, p. 191 ss.

¹² La stessa unione europea, pur con le difficoltà che la stessa incontra nell'individuare una politica legislativa da applicare alle nuove tecnologie, dimostra una fortissima attenzione verso l'impatto che le nuove tecnologie possono avere per lo sviluppo dell'economia del mercato unico. Si veda, in primo luogo, la Risoluzione del Parlamento europeo del 3 ottobre 2018, «Tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione». Il percorso europeo verso una sempre più concreta presa di coscienza circa la rilevanza che le nuove tecnologie possono avere per lo sviluppo del mercato finanziario in generale, trova un primo punto di arrivo nella Comuni-

cazione della Commissione europea relativa a una strategia in materia di finanza digitale per l'UE del 24 settembre 2020 [COM(2020) 591 final]. Sui rilievi che, per quanto riguarda il mercato assicurativo, sono state formulate sul punto da EIOPA, v. il documento *European Commission's Digital Finance Strategy consultation – EIOPA draft response* del 22 giugno 2020.

¹³ V. L. ENRIQUES e D. ZETZSCHE, *Corporate Technologies and the Tech Nirvana Fallacy*, in *Hastings Law Journal*, 2020, 72, p. 55 ss., che viene fatta propria da N. ABRIANI e G. SHNEIDER, *Il diritto societario incontra il diritto dell'informazione. IT*, Corporate governance e Corporate Social Responsibility, in *Riv. dir. soc.*, 2020, p. 1326 s.

¹⁴ Cfr., senza pretesa di esaustività, F. SARTORI, *La consulenza finanziaria automatizzata: problematiche e prospettive*, in *Riv. trim. dir. econ.*, 2018, p. 253 ss.; F. CAPRIGLIONE, *Industria finanziaria, innovazione tecnologica, mercato*, *ivi.*, 2019, p. 372 ss.; R. LENER, *Tecnologie e attività finanziaria*, *ibidem*, p. 267 ss. Con specifico riferimento al settore assicurativo, v. A. CAMEDDA, *La rivoluzione tecnologica nel settore assicurativo: l'avvento dei Big data*, in *giustiziacivile.com*, 2017; C. MUGELLI, *I principi etici per l'utilizzo dei "big data analytics tools" nel settore assicurativo: rischi ed opportunità*, in *Dir. merc. ass. fin.*, 2019, p. 473 ss.; G. D'IPPOLITO e E.M. INCUTTI, *I processi decisionali interamente automatizzati nel settore assicurativo*, in *Riv. dir. impresa*, 2019, p. 735 ss.; E. BATTELLI, *Big data e algoritmi predittivi nel settore assicurativo: vantaggi e nuovi rischi*, in *Corriere giur.*, 2019, p. 1517 ss.

¹⁵ Accenna al profilo, A. NUZZO, *Algoritmi e regole*, in *Analisi giur. econ.*, 2019, p. 45.

¹⁶ V., sul punto, le riflessioni di M.T. PARACAMPO, "FinTech" tra algoritmi, trasparenza e "algo-governance", in *Dir. banca*, 2019, p. 213 ss.

¹⁷ Si tratta, peraltro, di una evoluzione che è stata accelerata per effetto delle misure emergenziali poste in essere al fine di contenere il diffondersi del contagio da COVID-19. L'esigenza di limitare gli spostamenti e di mantenere il distanziamento interpersonale ha spinto il legislatore dell'emergenza a imporre che anche i consessi societari si svolgessero da remoto. Sul punto, v. M. PALAZZO, *Cosa resta della disciplina in materia di riunioni assembleari contenuta nella legislazione dell'emergenza?*, in *Nuove leggi civ. comm.*, 2020, 4, p. 909 ss. Si tratta, però, di misure che sicuramente verranno almeno in parte mantenute anche in condizioni di normalità.

¹⁸ La dottrina si era già soffermata su tali profili: C. PICCIAU, *The (Un)Predictable Impact of Technology on Corporate Governance*, in *Hastings Business Law Journal*, 2021, p. 108 s.; L. PAPI, *Il rafforzamento del ruolo degli azionisti attraverso la modernizzazione dei processi di partecipazione informativa e decisionale: l'adunanza "virtuale"*, in *Riv. dir. soc.*, 2017, p. 328.

¹⁹ Evidenzia la problematica, N. ABRIANI, *La corporate governance nell'era dell' algoritmo. Prolegomeni a uno studio sull'impatto dell'intelligenza artificiale sulla corporate governance*, in *Nuovo dir. soc.*, 2020, p. 264 s. La più autorevole e condivisa definizione di sistema di IA è quella elaborata dall'*High-Level Expert Group on Artificial Intelligence* della Commissione Europea che, nel documento "A definition of AI: Main capabilities and scientific disciplines" dell'aprile 2019, afferma: "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal".

²⁰ Sul ruolo svolto dagli algoritmi nell'ecosistema FinTech, v. M.T. PARACAMPO, "FinTech" tra algoritmi, trasparenza e "algo-governance", cit., p. 213 ss.

²¹ Su tali profili, e sulle soluzioni già sperimentate nel mercato di sistemi di IA integrati all'interno dei board, MONTAGNANI, *Flussi informativi e doveri degli amministratori di società per azioni ai tempi dell'intelligenza artificiale*, in *Persona e mercato*, 2020/2, p. 89 ss. e, spec., p. 91.

²² Indugia sul punto, P. TULLIO, *Diritto societario degli algoritmi. E se i robot diventassero imprenditori commerciali?*, in *Analisi giur. econ.*, 2019, p. 237 ss. Sul punto, tuttavia, v. la Risoluzione del Parlamento europeo del 16.2.2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica - 2015/2103(INL) - che sembra aprire al riconoscimento di una personalità artificiale ai sistemi di IA più evoluti.

²³ Sul punto, G.D. MOSCO, RoboBoard. *L'intelligenza artificiale nei consigli di amministrazione*, in *Analisi giur. econ.*, 2019, p. 248.

²⁴ Non può però mancare di rilevare che la prassi societaria ha già testato forme più o meno intense di sostituzione di membri del c.d.a con sistemi di intelligenza artificiale. Gli esempi più famosi sono Vital, Alicia T e Dao Project. Su tali esperienze, G. SCARCHILLO, *Corporate governance e intelligenza artificiale*, in *Nuova giur. civ. comm.*, 2019, p. 881 ss.

²⁵ V., ancora, G.D. MOSCO, RoboBoard. *L'intelligenza artificiale nei consigli di amministrazione*, cit., p. 256 ss. Indugia nell'analisi dei profili connessi alla responsabilità nell'utilizzo dell'IA, M. COSTANZA, *Impresa robotizzata e responsabilità*, in U. RUFFOLO (a cura di), *Intelligenza artificiale e responsabilità*, Milano, 2017, p. 107 ss.; G. COMANDÈ, *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi giur. econ.*, 2019, p. 169 ss.

²⁶ V., sul punto, G. SCARCHILLO, *Corporate governance e intelligenza artificiale*, cit., p. 885, ove evidenzia che “più complesse e rilevanti sono le decisioni da assumere da parte degli organi di amministrazione di una società, maggiore importanza va assumendo la base informativa sulla quale si forma la volontà degli amministratori. L’analisi e l’elaborazione di enormi quantitativi di dati (cc.dd. *big data*) è probabilmente la principale attività per cui le macchine intelligenti sono state concepite e realizzate. Peraltro, in tale attività esse risultano senza dubbio più efficienti degli uomini. In altre parole, le intelligenze artificiali dovrebbero fungere da supporto per ridurre gli sforzi di ricerca dei dati necessari per l’assunzione di una determinata decisione, in modo tale da consentire un risultato qualitativamente migliore e riducendo di molto il gap informativo che c’è tra il mercato e gli amministratori di una determinata società”. Riflessioni in questo senso anche in A. NUZZO, *Contenuti e forme dell’informazione societaria tra passato e futuro. Titoli e operatori atipici nell’era dell’algoritmo*, in *Analisi giur. econ.*, 2019, p. 596 ss.

²⁷ Lo nota M.L. MONTAGNANI, *Flussi informativi e doveri degli amministratori di società per azioni ai tempi dell’intelligenza artificiale*, cit., p. 98 s.

²⁸ C. AMATUCCI, *Adeguatezza degli assetti, responsabilità degli amministratori e business judgement rule*, in *Giur. comm.*, 2016, I, p. 643 ss.; V. CALANDRA BUONAUURA, *Corretta amministrazione e adeguatezza degli assetti organizzativi nella Società per azioni*, *ivi*, 2020, p. 439 ss.

²⁹ Cfr., sul punto, le considerazioni di N. ABRIANI, *La corporate governance nell’era dell’algoritmo. Prolegomeni a uno studio sull’impatto dell’intelligenza artificiale sulla corporate governance*, cit., p. 283.

³⁰ Sul problema della genetica assenza di trasparenza negli algoritmi, v. A. NUZZO, *Contenuti e forme dell’informazione societaria tra passato e futuro. Titoli e operatori atipici nell’era dell’algoritmo*, cit., p. 587 s. e, spec., p. 595 ove evidenzia che “il contributo dell’algoritmo all’analisi e alla formazione delle decisioni non dovrebbe sollevare dubbi di legittimità fintantoché, beninteso, l’avvalersi dell’artefatto tecnologico non si risolve in una «delega in bianco» alla macchina, in particolare ove ciò non consenta di dare chiaramente conto delle ragioni alla base della decisione assunta, la cui ragionevolezza deve emergere (ferma restando la copertura assicurata dalla *business judgement rule*). In definitiva, occorre riuscire a motivare la scelta e a tal fine l’algoritmo deve contribuire a darne spiegazione in forme comprensibili all’uomo. È chiaro, allora, che non dovrebbero porre problemi gli algoritmi di tipo «debole» (in relazione ai quali le tecniche di ingegneria ricorsiva consentano di ricostruire i parametri della decisione); mentre gli algoritmi di deep learning (che si affidano a reti neurali «forti») possono al contrario porre non pochi problemi”.

³¹ Insiste sul punto D. CAPONE, *La Governance dell'Artificial Intelligence nel settore assicurativo, tra principi etici, responsabilità del board e cultura aziendale*, Quaderno IVASS n. 16, 2021, p. 21. Considerazioni in tal senso anche in G.D. MOSCO, RoboBoard. *L'intelligenza artificiale nei consigli di amministrazione*, cit., p. 254.

³² Diffusamente, M.L. MONTAGNANI, *Flussi informativi e doveri degli amministratori di società per azioni ai tempi dell'intelligenza artificiale*, cit., p. 99 ss. e spec., p. 103 s. ove ipotizza l'opportunità di prevedere nelle s.p.a. uno specifico comitato endo-consiliare che si occupi dei profili tecnologici connessi all'attività amministrativa dell'impresa o, ove per ragioni di proporzionalità risulti inopportuno costituire tale comitato, le medesime funzioni dovrebbero essere svolte da parte del comitato sui controlli interni. Medesima soluzione viene proposta da D. CAPONE, *La Governance dell'Artificial Intelligence nel settore assicurativo, tra principi etici, responsabilità del board e cultura aziendale*, cit., p.18. V., pure, la considerazione di N. ABRIANI, *La corporate governance nell'era dell' algoritmo. Prolegomeni a uno studio sull'impatto dell'intelligenza artificiale sulla corporate governance*, cit., p. 273 ove fa notare: "che un domani, non troppo lontano, la presenza di esperti (o di comitati di esperti) di tecnologia all'interno del board assurgerà a standard indefettibile di *good governance*".

³³ Cfr., sul punto, D. CAPONE, *op. cit.*, p. 20, ove evidenzia che "In virtù degli sviluppi normativi, ma anche della ormai acquisita cultura del controllo, tutte le imprese del settore finanziario sono ormai pienamente consapevoli dell'importanza del modello delle tre linee di difesa per la gestione di qualsiasi tipologia di rischio, anche estremamente innovativo come è il caso dell'utilizzo degli strumenti di AI. Le strutture di *risk governance* esistenti potrebbero quindi vedere ampliato il proprio mandato per ricomprendervi le nuove responsabilità, in particolare chiarendo la suddivisione di ruoli e prerogative delle *key functions* (attuariale, *risk management*, *compliance* e *audit*) rispetto all'AI".

³⁴ È stato notato dalla dottrina come i membri dei board siano oggi sempre più impegnati nel reperimento di dati e nell'analisi degli stessi. L'adozione di algoritmi in tali casi permetterebbe agli amministratori di concentrare la propria attività nell'individuazione delle decisioni da adottare. Cfr., in questo senso, G.D. MOSCO, RoboBoard. *L'intelligenza artificiale nei consigli di amministrazione*, cit., p. 252 ss.

³⁵ F. MATTASOGLIO, *Algoritmi e regolazione. Circa i limiti del principio di neutralità tecnologica*, in *Riv. reg. merc.*, 2018, p. 226 ss.

³⁶ Evidenzia le difficoltà connesse alla normazione di un fenomeno tanto peculiare e di dimensioni mondiali, A. CELOTTO, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *An. giur. econ.*, 2019, p. 56 ss.

³⁷ Riferimenti in questo senso in M.T. PARACAMPO, “FinTech” *tra algoritmi, trasparenza e “algo-governance”*, cit., p. 239 ss.

³⁸ Indugia sul punto, D. CAPONE, *La Governance dell’Artificial Intelligence nel settore assicurativo, tra principi etici, responsabilità del board e cultura aziendale*, cit., p. 14 e, spec., p. 17, la quale evidenzia che “la velocità nello sviluppo e la rapida estensione dei potenziali ambiti di utilizzo degli strumenti di intelligenza artificiale non consentono, al momento, la definizione di un framework normativo statico che imponga obblighi, codifichi divieti e irroggi sanzioni. Le sperimentazioni sul campo non sono, infatti, sempre compatibili con un sistema fatto di regole rigide ed eteroimposte⁵⁰. Nella fase attuale di sviluppo è importante assicurare flessibilità al quadro regolamentare di riferimento, ferma restando la necessaria, piena tutela dei diritti fondamentali individuali, ad oggi garantita dalla normativa sui dati personali e da quella a tutela del cliente, da tenere costantemente aggiornate e adeguate alle nuove esigenze”.

³⁹ Pongono in evidenza come le politiche assunte da una impresa in relazione al profilo della sostenibilità possano «contribuire ad aumentare il valore dell’investimento stesso», L. ANDRIOLA, M. JORIZZO e P. SABELLI, *Sustainable investors relation: comunicare agli investitori tramite le strategie di sostenibilità ambientale*, in *Ambiente e sviluppo*, 2016, p. 743 ss.

⁴⁰ Sul punto, v. A. ANTONUCCI, *La responsabilità sociale dell’impresa*, in *Nuova giur. civ. comm.*, II, 2007, p. 128; M. LIBERTINI, *Economia sociale di mercato e responsabilità sociale dell’impresa*, in *Orizz. dir. comm.*, 2013, p. 2 il quale evidenzia la capacità di atteggiamenti socialmente responsabili di creare fiducia nel mercato.

⁴¹ Insiste su tale aspetto il Piano d’azione per finanziare la crescita sostenibile [COM(2018)97 final] della Commissione datato 8 marzo 2018, p. 3 ove si evidenziano le destabilizzanti ricadute economiche che si produrrebbero per effetto, in particolare, dei fenomeni meteorologici connessi ai cambiamenti climatici. Non è un caso che nel suddetto Piano d’azione si arrivi ad ipotizzare di tenere in considerazione i fattori ESG nella determinazione dei requisiti prudenziali richiesti ai soggetti vigilati. V., in questo senso, il Piano d’azione per finanziare la crescita sostenibile, cit., pp. 10 s.

⁴² Nella dottrina straniera, viene evidenziata l’opportunità di privilegiare decisioni che, attente ai fattori ESG, si dimostrino positive nel lungo termine, S.N. GARY, *Best interest in the long term: fiduciary duties and ESG integration*, in *Univ. of Colorado Law Rev.*, 2019, p. 731 ss.

⁴³ Va infatti evidenziato come, a prescindere da quanto si dirà, siano riscontrabili velate aperture agli aspetti non patrimoniali nello stesso codice delle assicurazioni private. All’art. 94, comma 1 bis c. ass., infatti, già si preve-

deva di includere nella relazione sulla gestione non solo gli indicatori di risultato finanziari, ma anche «se del caso, quelli non finanziari pertinenti all'attività specifica dell'impresa, comprese le informazioni attinenti all'ambiente e al personale». Cenni sul punto in G. IACOBONE, *Art. 94*, in ALB. CANDIAN e G. CARRIERO (a cura di), *Codice delle assicurazioni private*, Napoli, 2014, p. 401

⁴⁴ La direttiva menzionata modifica la direttiva 2013/34/UE.

⁴⁵ Ai sensi degli artt. 1 e 2 del d.lg. n. 254 del 2016, sono enti di interesse pubblico le società italiane emittenti valori mobiliari ammessi alla negoziazione su mercati regolamentati italiani e dell'Unione europea, le banche, le imprese di assicurazione e di riassicurazione italiane che abbiano avuto, in media, durante l'esercizio finanziario un numero di dipendenti superiore a cinquecento e, alla data di chiusura del bilancio, abbiano superato la somma di 20.000.000 di euro come stato patrimoniale o il cui totale dei ricavi netti superi i 40.000.000 di euro.

⁴⁶ Sul punto, v. E. BELLISARIO, *Rischi di sostenibilità e obblighi di disclosure: il d.lgs. n. 254/16 di attuazione della dir. 2014/95/UE*, in *Nuove leggi civ. comm.*, 2017, p. 19 ss.

⁴⁷ Ai sensi dell'art. 3 del d.lg. 254 del 2016.

⁴⁸ Ai sensi degli artt. 4 e 6 del d.lg. 254 del 2016.

⁴⁹ Cfr., A. QUARANTA, *La comunicazione di informazioni di carattere non finanziario: la nuova disciplina colpisce nel segno*, in *Ambiente e sviluppo*, 2017, pp. 523 s.

⁵⁰ Sul punto, G. MOLLO, *La comunicazione di informazioni di carattere non finanziario quale strumento di attuazione della Responsabilità Sociale dell'Impresa*, in *Riv. dir. ind.*, 2019, p. 328.

⁵¹ La relazione in parola deve essere attestata, secondo quanto afferma l'art. 3, comma 10 del d.lg. 254 del 2016, da parte del soggetto incaricato della revisione legale del bilancio che ne certifichi la conformità rispetto alla normativa vigente. Ciò solleva non poche perplessità circa la capacità dei soggetti designati a fornire certificazioni attendibili su dati che, da un lato, fuoriescono dalle specifiche competenze tipiche dei revisori e, dall'altro, risultano per loro natura sfuggenti. Sul punto, v. E. BELLISARIO, *Rischi di sostenibilità e obblighi di disclosure: il d.lgs. n. 254/16 di attuazione della dir. 2014/95/UE*, cit., p. 43 ss.

⁵² Interessante, sul punto, la lettura dei recenti Orientamenti della Commissione UE del 17 giugno 2019 «sulla comunicazione di informazioni di carattere non finanziario: integrazione concernente la comunicazione di informazioni relative al clima», pp. 7 s. [C(2019) 4490 fin]

⁵³ In questo senso, art. 3, comma 1, del d.lg. 254 del 2016.

⁵⁴ S. DE POLIS, *Il ruolo del settore assicurativo a sostegno della transizione dalla brown alla green economy*, del 30 ottobre 2019, in www.ivass.it.

⁵⁵ *Opinion on Sustainability within Solvency II*, cit. nel testo, pp. 11 e 21 ss.

⁵⁶ *Opinion on Sustainability within Solvency II*, cit., pp. 11 s. e 23 ss.

⁵⁷ *Opinion on Sustainability within Solvency II*, cit., pp. 12 s. e 25 ss.

⁵⁸ *Opinion on Sustainability within Solvency II*, cit., pp. 13 s. e 29 ss.

⁵⁹ *Opinion on Sustainability within Solvency II*, cit., pp. 14 ss. e 33 ss.

⁶⁰ L'*Opinion* menzionata distingue i rischi climatici in *transition risks*; *physical risks* e *liability risks*. Mentre il primo dei rischi menzionati tende ad impattare prevalentemente sugli *assets* dell'impresa di assicurazione, gli ultimi due incidono principalmente sugli aspetti patrimoniali connessi alla *liability*. L'*Opinion* afferma infatti che i «Transition risks can arise from the process of adjustment towards a low carbon economy. A range of factors influence this adjustment, including: climate changerelated developments in policy and regulation, the emergence of disruptive technology or business models, shifting sentiment and societal preferences, or evolving evidence, frameworks and legal interpretations». Quando invece si riferisce ai *Physical risks* fa riferimento a rischi che «arise from a number of factors, and relate to specific weather events (such as heatwaves, floods, wildfires and storms) and longerterm shifts in the climate (such as changes in precipitation, extreme weather variability, sea level rise, and rising mean temperatures). Some examples of physical risks crystallising include: increased frequency, severity or volatility of extreme weather events impacting property and casualty insurance; and increased frequency and severity of flooding leading to physical damage to the value of financial assets or collateral held by banks, such as household and commercial property». Da ultimo, i «Liability risks come from people or businesses seeking compensation for losses they may have suffered from the physical or transition risks from climate change outlined above. Liability risks are of particular relevance to insurance undertakings given these risks can be transferred by means of liability protection, such as Directors & Officers and Professional Indemnity insurance. These are likely to fall under three different categories: failure to mitigate; failure to adapt; failure to disclose». In questo senso, *Opinion on Sustainability within Solvency II*, pp. 5 s.

⁶¹ Diffusamente, sul punto, le considerazioni contenute in *Opinion on Sustainability within Solvency II*, cit., pp. 6

⁶² *Opinion on Sustainability within Solvency II*, cit., pp. 16 s. e pp. 49 ss.

⁶³ Le medesime preoccupazioni sono avvertite all'interno di tutti e tre i settori regolamentati. Da ultimo, in ambito bancario, v. il *Report on undue short-*

term pressure from the financial sector on corporations del 18 dicembre 2019 emesso dall'EBA in attuazione dell'azione n. 10 del Piano d'azione sulla finanza sostenibile con il quale si cerca di stimolare una visione di lungo termine anche valorizzando i riflessi positivi che possono avere i fattori ESG in tal senso. Medesime risultanze emergono nel *Report on undue short-term pressure on corporations* di ESMA del 18 dicembre 2019.

⁶⁴ V. le modifiche all'art. 269 del Regolamento delegato UE 2015/35.

⁶⁵ In questo senso vanno le modifiche introdotte all'art. 260 del Regolamento delegato UE 2015/35.

⁶⁶ V. la modifica introdotta al Regolamento delegato UE 2015/35 per effetto dell'introduzione del par. 1 bis all'art. 269.

⁶⁷ In questo senso vanno lette le modifiche al Regolamento delegato UE 2015/35 effettuate con l'introduzione dell'art. 275 bis. V. sul punto, pur commentando il *Consultation paper* che ha dato vita al *Tecnica advice* che poi ha ispirato il Regolamento delegato, M. CATENACCI e P. SANNA, *I consultation paper di ESMA e EIOPA in materia di investimenti sostenibili*, in *www.dirittobancario.it*, 2019, p. 5. Va inoltre segnalato che i profili sopra descritti vengono messi in diretta relazione anche con la necessità di integrare tali fattori di sostenibilità nelle preferenze dei clienti da valutare ai fini della definizione del mercato *target* ai sensi dell'art. 25 IDD. Sul punto, v. *infra*.

⁶⁸ Rilevante sotto tale ultimo profilo è il passaggio contenuto al punto n. 94 del *Tecnica advice*, cit. nel testo, p. 18 in tema di disciplina delle remunerazioni, ai sensi del quale "Remuneration can also be used as a tool for the integration of sustainability risks in the investment decisions. Solvency II Delegated Regulation currently provides that the remuneration policy and remuneration practices shall be in line with the undertaking's business and risk management strategy, its risk profile, objectives, risk management practices and the long-term interests and performance of the undertaking. Therefore, changes in the undertaking's investment risk management policy to incorporate sustainability risks will have a subsequent impact on the undertaking's remuneration policy. Undertakings are also requested to take into account both financial and non-financial criteria when assessing an individual's performance. The consideration of sustainability factors is a good example of non-financial criteria that could be taken into account when assessing individual performance". Da tali considerazioni, deriva la proposta di modifica dell'art. 275 del Regolamento delegato 2015/35 con l'introduzione di un quarto comma che prevede l'inclusione dei rischi di sostenibilità anche nell'elaborazione della politica sulle remunerazioni. V. *Tecnica advice*, cit., p. 19.

⁶⁹ Si soffermano su tale profilo, S. DELL'ATTI e S. SYLOS LABINI, *Il governo societario nelle imprese di assicurazione. Regolamentazione, proporzionalità e gestione del cambiamento*, Milano, 2019, p. 49 s. e, spec., p. 50 ove notano che «una simile previsione potrebbe apparire secondaria. In realtà si inserisce entro il più ampio dibattito sviluppatosi a livello internazionale in merito al ruolo che la finanza può ricoprire nell'ambito dell'economia sostenibile. (...) A livello nazionale si registra un crescente livello di consapevolezza e di iniziativa tra le istituzioni del mercato assicurativo, ma ancora ampi sono i margini di miglioramento per lo sviluppo di buone pratiche. In tal senso, la previsione contenuta nel Regolamento n. 38/2018 va nella direzione di accrescere l'attenzione e la consapevolezza dei board delle imprese rispetto alle tematiche di sostenibilità e di governo "responsabile"».

⁷⁰ D. CAPONE, *La Governance dell'Artificial Intelligence nel settore assicurativo, tra principi etici, responsabilità del board e cultura aziendale, Quaderno IVASS n. 16, 2021, p. 15*, ove si evidenzia che "Anche le più puntuali raccomandazioni adottate da policymakers, standard setters o associazioni di categoria dei diversi settori di applicazione dell'AI, sia a livello globale (OECD) sia europeo (Commissione Europea) possono essere ricondotte a questi principi di carattere generale. Minimo comune denominatore di queste raccomandazioni è richiedere che le modalità di configurazione e di governo dell'AI siano tali da assicurare: sostenibilità sociale ed ambientale (deve apportare benefici nei confronti della società in generale e delle generazioni a venire); accountability (possibilità di individuare un processo per l'adozione delle tecniche di AI e soggetti che ne rispondano e lo guidino); equità (nel doppio significato di giustizia e non discriminazione); trasparenza (che include un concetto di comprensibilità proporzionata al soggetto nei cui confronti va garantita); sicurezza tecnologica e protezione dei dati personali (inclusa la possibilità di garantire al proprietario di avere accesso ai propri dati)".

⁷¹ Si veda, ad esempio, il software SIRating o le piattaforme sviluppate da Ecomate.

⁷² Proposta di Regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione [COM(2021) 206 final] e, prima ancora, v. gli Orientamenti etici per un'IA affidabile dell'8 aprile 2019.

Sostenibilità e diritto dei privati.

Il caso della capacità tecnologica dei contratti sostenibili nel settore turistico

SARA LANDINI

Sommario: 1. Premessa. - 2. Contrasti sul concetto di sostenibilità. - 3. L'idea di sostenibilità nel diritto privato e nel diritto dei privati. - 4. Contratti *Green* tra privati. Il fenomeno dei contratti sostenibili nel turismo. - 5. Conclusioni.

1. Premessa

L'idea di sostenibilità nel senso di sviluppo sostenibile, ovvero di una produttività che si coniuga con istanze sociali e ambientali rispettose dei bisogni delle generazioni future, trova spazio anche nel diritto privato.

La sostenibilità ha anche una dimensione prescrittiva¹, leggibile primariamente già negli artt. 3 e 21 TUE, 11 TFUE, 37 Carta UE che impongono obblighi agli Stati membri di permettere lo sviluppo del presente senza pregiudicare il futuro, norme che ispirano anche il nostro codice dell'ambiente dlgs 152/2006 (d'ora in poi c.a.)². Il quadro normativo internazionale è stato da ultimo ridisegnato dall'Agenda 2030 per lo sviluppo sostenibile, adottata il 25 settembre 2015 in occasione della 70a Assemblea generale delle Nazioni Unite (Risoluzione NU A/RES/70/1). A livello di diritto unionale ricordiamo la nuova strategia dell'UE sull'adattamento ai cambiamenti climatici (COM/2021/82 final). Questa strategia afferma che, nel 2050, l'UE sarà una società resiliente al clima e pienamente adattata agli impatti inevitabili dei cambiamenti climatici. Non dimentichiamo come a livello di diritto unionale si sia intervenuti, proprio nel senso di

dare concretezza applicativa al concetto di sostenibilità, disegnando la tassonomia degli interventi in chiave di sostenibilità. Ricordiamo sul punto l'art. 17 del regolamento 2020/852/UE (c.d. regolamento tassonomia, attinente all'istituzione di un quadro che favorisca gli investimenti ecosostenibili).

La dottrina giusprivatistica ha da tempo sottolineato come ai sensi dell'art. 3 *quater* del codice dell'ambiente (dlsq 152/06 da ora in poi c.a.) ogni attività umana debba conformarsi al principio dello sviluppo sostenibile "affinché nell'ambito delle dinamiche della produzione e del consumo si inserisca altresì il principio di solidarietà per salvaguardare e per migliorare la qualità dell'ambiente anche per il futuro". Si nota come per tal via si giunga ad una "concezione aperta della solidarietà costituzionale" di cui all'art. 3 Cost. che "consente di riconoscere doveri di solidarietà ambientale a carico di tutti i consociati"³. E del resto giudizi di valore sull'attività economica dei privati orientati a renderla funzionale alla preservazione dell'ambiente già potevano desumersi dalla nostra Carta Costituzionale e in particolare dagli artt. 2, 4, 9, 32, 41 Cost.⁴, nonché dal principio di ragionevolezza di cui all'art. 3 Cost. da leggersi anche come utilizzo razionale delle risorse naturali⁵. Le stesse costruzioni sulla teoria dei beni comuni hanno sullo sfondo tale idea nel momento in cui disegnano lo statuto di tali beni improntandolo a principi di condivisione e di funzione sociale della proprietà⁶.

La sostenibilità è poi penetrata nel diritto dei privati attraverso prassi che possono dirsi ispirate ai suddetti valori in attuazione del principio di sussidiarietà.

Nei contratti di franchising, ad esempio è possibile che sia richiesto all'affiliato di adeguarsi a standard di ecosostenibilità; nei contratti di fornitura tra imprese è possibile che il fornitore si impegni a realizzare i propri prodotti secondo standard di produzione ispirati a criteri di sostenibilità; nelle associazioni di professionisti e di imprese gli associati si impegnano spesso

ad operare nel rispetto di siffatti standard ⁷.

I contratti tra privati divengono così veicolo di istanze sociali e strumento di salvaguardia di interessi generali.

Manca, come avremo modo di vedere nei prossimi paragrafi, un'idea ben definita di cosa debba intendersi per sostenibilità e delle regole di condotta in cui si declina tale concetto. Gli stessi interventi, volti a creare una tassonomia, sono in definitiva orientati primariamente a identificare obbiettivi piuttosto che contenuti.

Si tratta, al riguardo, di riflettere sulle potenzialità ordinanti della indeterminatezza dei principi al fine di stabilire se sia necessario individuare regole di condotta qualificabili come ecosostenibili o se l'indeterminatezza, propria della normazione per principi, non rappresenti un vantaggio aprendo alla possibilità di un bilanciamento in concreto degli interessi in gioco ⁸. È vero che pare possibile coniugare tali differenti tendenze regolatorie (regolamentazione per principi e disciplina dettagliata delle condotte) attraverso l'indicazione di norme che individuano le condotte ammesse e/o quelle vietate lasciando aperture ad un'interpretazione delle stesse conforme ai principi costituzionali.

Altro è il problema di quantificare gli effetti sull'ambiente di determinate pratiche al fine di qualificarle come ecosostenibili perché rispondenti a determinati indici ambientali. Si tratta in questo caso di riempire di contenuti quantitativi il termine sostenibilità al fine di governare anche problemi giuridici come quello della misura dell'adempimento in caso di "clausole di sostenibilità" contenute nei contratti tra privati e quello della correttezza nell'uso degli "*environmental claims*" di cui parleremo nel prosieguo del discorso.

Il presente scritto mira a mettere in luce questi fenomeni e i problemi che possono porsi nel tentativo di dare giuridica rilevanza a "criteri quantitativi". In particolare, si tratta di stabilire

se l'introduzione di tali indicazioni quantitative nelle clausole contrattuali incida sulla applicazione delle regole in tema di contratto. Il raggiungimento o meno degli indici quantitativi, senza lasciare spazi all'interpretazione dei giudicanti, porta infatti in maniera assiomatica agli effetti previsti. La verità è che tali indici contenuti nelle clausole contrattuali verranno pur sempre a legarsi con le clausole generali (buona fede, diligenza del buon padre di famiglia ecc.) contenute nelle norme sul contratto in generale. Vedremo come.

2. Contrasti sul concetto di sostenibilità

In ecologia per sostenibilità si intende la capacità dei sistemi biologici di rimanere produttivi nel tempo. Sostenibilità delle attività umane è un concetto che, pur avendo affinità con tale definizione, presenta una maggiore complessità.

La parola "sostenibilità" in economia implica la c.d. "ecological economics" orientata alla integrazione degli aspetti sociali, culturali e di tutela della salute, con quelli monetari e finanziari.

Il concetto di sviluppo sostenibile viene fatto risalire al report elaborato dalla Commissione Brundtland delle Nazioni Unite il 20 Marzo 1987 in cui si legge che "lo sviluppo sostenibile è quello sviluppo che incontra le necessità delle generazioni presenti senza compromettere la possibilità per le generazioni future di soddisfare i propri bisogni"⁹.

Durante il World Summit sullo sviluppo sociale sono stati enunciati i pilastri della sostenibilità: la libertà, l'uguaglianza, la solidarietà, la tolleranza, il rispetto per i diritti umani, il rispetto per la natura, la responsabilità sociale¹⁰.

Un altro documento importante nella storia della sostenibilità è la Earth Chart contenente le basi per la fondazione di una società sostenibile a livello globale improntata al rispetto per la natura, ai diritti umani fondamentali, alla giustizia economica e

alla cultura della pace. Questa carta è il risultato di una serie di incontri svoltisi tra il 1995 e il 2000 dalla Commissione Earth Chart presieduta da Steve C. Rockefeller ¹¹.

Vi sono stati poi tentativi di tradurre in specifiche regole di condotta il principio di sostenibilità. Così UNEP (United Nations Environment Program) e il UNWTO (United Nations of the World Tourism Organization) hanno elencato alcune regole del turismo sostenibile. In particolare si richiede alle imprese turistiche di fare un uso ottimale delle risorse ambientali mantenendo processi ecologici essenziali; di conservare l'eredità naturale e la biodiversità; di rispettare l'autenticità socio culturale delle comunità in cui si svolge l'attività turistica. L'impresa turistica deve preservarne l'eredità culturale, le tradizioni e contribuire alla comprensione interculturale e alla tolleranza. Deve provvedere al benessere socio-economico di tutti i portatori di interesse anche contribuendo all'arricchimento delle popolazioni ospitanti l'offerta turistica, fornendo loro servizi sociali, riducendo la povertà.

E altre potrebbero essere le iniziative da ricordare intorno al concetto di sostenibilità.

Va detto che l'idea di sviluppo sostenibile ha incontrato anche critiche soprattutto tra gli economisti che hanno evidenziato come il termine rappresenti un ossimoro: lo sviluppo inteso come crescita economica sarebbe improntato a logiche di incremento degli utili e non ragioni di utilità sociale ¹². Si potrebbe rispondere che non vi sono ragioni per escludere la conciliazione tra utilità economica e utilità sociale. Non ci sembra vi siano motivi per affermare che le leggi della crescita economica si muovono secondo paradigmi inconciliabili rispetto ai valori della tutela della persona e della utilità sociale.

La scienza economica ha peraltro da tempo adottato approcci che valorizzano il raggiungimento di obiettivi di equità sociale, solidarietà, giustizia. Intendiamo riferirci alla Welfare Economics ¹³. Si suole dire che l'economia è una scienza pratica che

rifugge da concetti vaghi come appunto l'equità, la giustizia, la libertà¹⁴. In realtà è possibile approntare strumenti di misurazione del raggiungimento di tali obiettivi attraverso l'individuazione di specifici criteri. Si pensi con riferimento all'equità ad una serie di parametri che possono considerarsi indice della riduzione della povertà: il livello di scolarizzazione, il livello di occupazione, la ricchezza pro capite, ecc.

Così alla critica di quanti vedono nella sostenibilità un concetto evanescente vi è chi ha cercato di trovare una risposta in criteri per misurare la sostenibilità attraverso indicatori, benchmarks, standard e sistemi di certificazione¹⁵.

Si tratta di criteri accettati dalle collettività interessate (associazioni dei consumatori, associazioni di operatori economici) che entrano nel quadro ordinamentale anche attraverso l'autonomia dei privati che li recepisce nel testo dei contratti (contratti associativi, contratti di fornitura tra privati, ecc.)¹⁶.

Gli economisti non devono fermarsi a considerare modelli efficienti individuati attraverso il rapporto tra costi ed utilità marginali, ma possono anche valutare costi ed utilità sociali rapportando l'efficienza alla utilità sociale. A tale obiettivo giungono i fautori della teoria del *Second Best*¹⁷. Una volta raggiunto il livello ottimale di efficienza si verifica se lo stesso risultato ottimale anche dal punto di vista del benessere della collettività. In caso contrario dovrà ricercarsi un secondo modello che riesca a soddisfare pure le utilità sociali.

In critica al concetto di sostenibilità altri autori hanno affermato che essa non è un principio, ma un obiettivo tendenziale inglobante una serie di principi e valori¹⁸. Si tratterebbe di un "*unfocused concept*" al pari della libertà e della giustizia che descrive "*a dialogue of values that defies consensual definition*"¹⁹.

A tali obiezioni si è cercato di rispondere assumendo che la sostenibilità è in realtà un concetto integrato di altri valori, principi e dimensioni non solo giuridiche²⁰. Del resto come ab-

biamo visto i pilastri della sostenibilità come definiti dalle Nazioni Unite coincidono con principi fondamentali riconosciuti a livello internazionale tra cui solidarietà, uguaglianza, tutela della salute, ecc.

L'argomentare giuridico conosce la necessità di confrontarsi con una pluralità di principi interessati dalla soluzione del caso concreto. La dottrina tende a risolvere eventuali conflitti attraverso un bilanciamento tra gli stessi ²¹.

Il fatto che si pongano problemi di sostenibilità e che quindi l'interprete debba confrontarsi con una pluralità di principi compresi nel concetto di sostenibilità importerebbe la necessità di operare un bilanciamento tra gli stessi ove si tratti di principi da porre sullo stesso piano.

Laddove il confronto sia tra principi relativi a diritti economici e principi relativi a diritti fondamentali della persona si avrà una prevalenza dei secondi stante il loro diverso peso in una ideale gerarchia di valori.

L'idea di sostenibilità potrebbe però aprire ad altre prospettive. Essa si fonda su un'integrazione di principi e di valori anche in apparente contrasto tra loro. Il concetto di sviluppo sostenibile porterebbe a pensare non in una logica di gerarchia dei valori e dei principi, ma in una logica di complessità di valori e principi che devono trovare un coordinamento secondo il criterio ordinante della proporzionalità. Del resto questa, come avremo modo di vedere, risulta essere la via che vanno percorrendo i giudici amministrativi nell'applicazione del principio di sostenibilità.

Solo laddove le ragioni dello sviluppo vengono a confliggere con situazioni esistenziali senza lasciare spazio a logiche conciliative che consentano *realmente* uno sviluppo sostenibile, non potrà aversi integrazione ma le ragioni del mercato dovranno essere considerate recessive rispetto alle ragioni di tutela della persona²².

Rimane il fatto che in tale coordinamento di valori e di principi il concetto di sostenibilità risulta pur sempre sfumato, senza con-

torni ben definiti. Da qui la possibile rilevanza di indici quantitativi.

Come detto, volendo individuare applicazioni giurisprudenziali del principio, il primo riferimento è individuabile nelle pronunce dei giudici amministrativi.

3. L'idea di sostenibilità nel diritto privato e nel diritto dei privati

Come detto nel diritto privato i riferimenti alla sostenibilità sono individuati primariamente nella Carta Costituzionale e nel Codice dell'ambiente.

È vero che anche nel codice civile sono in più parti rievocate le ragioni della produzione in relazione a interessi individuali per quanto, come vedremo, pare difficile trovare nelle stesse espressioni del principio di sostenibilità per come sin qui descritto.

In particolare, nel diritto privato applicazioni giurisprudenziali del bilanciamento tra interessi individuali, tutela dell'ambiente e ragioni della produzione si sono posti in particolare con riferimento all'art. 844 c.c. in tema di immissioni dettato con l'intenzione di comporre i conflitti tra proprietari di fondi contigui con uno sguardo di favore per il soggetto capace di contribuire maggiormente allo sviluppo economico della nazione.

La norma prevede che il proprietario di un fondo non è tenuto ad escludere le immissioni propagantesi dal suo fondo ma solo a mantenerle entro la soglia della "normale tollerabilità".

Le immissioni sono inoltre ammesse, anche in violazione dei diritti dei proprietari finitimi, laddove l'autorità giudiziaria accerti la loro strumentalità rispetto alla produzione²³.

Si prevede, infatti al primo comma che "il proprietario di un fondo non può impedire le immissioni di fumo o di calore, le esalazioni, i rumori, i scuotimenti e simili propagazioni derivanti dal fondo del vicino, se non superano la normale tollerabilità, ha avuto anche a riguardo la condizioni dei luoghi"

Il secondo comma lascia poi ampi margini di discrezionalità

all'autorità giudiziaria, stabilendo che “nell'applicare questa norma l'autorità giudiziaria deve contemperare le esigenze della produzione con la ragione della proprietà. Può tenere conto della priorità di un determinato uso”²⁴.

La discrezionalità del giudice nella valutazione della “normale tollerabilità” delle immissioni è stata posta al vaglio di legittimità costituzionale.

La Consulta si è pronunciata sulla questione rigettando l'istanza e assumendo che l'art. 844 c.c. è norma “destinata a risolvere il conflitto tra proprietari di fondi vicini per le influenze negative derivanti da attività svolte nei rispettivi fondi; il criterio della normale tollerabilità in esso accolto va riferito esclusivamente al contenuto del diritto di proprietà e non può essere utilizzato per giudicare della illiceità di immissioni che rechino pregiudizio anche alla salute umana o all'integrità dell'ambiente naturale, alla cui tutela è rivolto in via immediata tutto un altro ordine di norme di natura repressiva e preventiva”²⁵.

La Corte di Cassazione ha poi più volte sottolineato come nell'ordinamento vi siano altre norme preposte a tutelare il prioritario diritto alla salute e in specie gli art. 2043 e 2058 c.c. e lo stesso art. 32 della Costituzione²⁶.

Due i noti orientamenti dottrinali sul punto: alcuni ritengono corretto l'utilizzo dell'art. 844 c.c. ai soli fini della difesa della proprietà²⁷; altri, invece, applicano la norma anche al fine di prevenire danni alla salute o all'ambiente²⁸.

Quest'ultimo filone interpretativo ha avuto un seguito nella giurisprudenza che ha individuato nell'art. 844 uno strumento idoneo a prevenire o a contenere la portata dannosa delle immissioni che, laddove intollerabili, verranno inibite dal giudice⁽²⁹⁾.

L'applicazione dell'art. 844 al fine di tutelare l'ambiente e la salute richiede però un'interpretazione della normativa che dia atto dell'evoluzione ordinamentale sul punto. Come abbiamo già osservato la norma contenuta nell'art. 844 mette a fuoco la

priorità d'uso e dell'interesse della produzione, quali fattori rilevanti nella valutazione della condizione di intollerabilità. L'intento del legislatore del '42 pareva essere quello di subordinare la protezione degli interessi individuali proprietari alle ragioni economiche dei fondi. Insomma l'art. 844 era destinato a risolvere conflitti tra interessi patrimoniali.

Le considerazioni sull'applicabilità dell'art. 844 come strumento di tutela di situazioni esistenziali si pongono nel solco del ben noto orientamento che porta a rileggere le disposizioni codicistiche tenuto conto di quel processo di depatrimonializzazione del diritto privato che ha ormai spostato il proprio baricentro nella direzione della clausola di promozione e tutela della persona di cui all'art. 2 Cost.³⁰.

Non riteniamo comunque che nell'art. 844 si trovi un indice di rilevanza della sostenibilità nel diritto privato. Soprattutto alla luce di una interpretazione costituzionalmente orientata non pare che la norma apra a logiche di contemperamento tra interessi patrimoniali sottesi a processi produttivi e situazioni giuridiche esistenziali. Nell'applicare l'art. 844 a tutela di situazioni esistenziali non sembra possibile contemperare le esigenze della produzione, come si potrebbe fare in caso di applicazione della norma nella soluzione di conflitti aventi ad oggetto interessi puramente patrimoniali³¹. Resta il fatto che il giudizio sulla normale tollerabilità nei rapporti di vicinato è frutto del bilanciamento degli interessi contrapposti³².

Riferimenti alla produzione nazionale si hanno pure nell'art. 838 "Espropriazione di beni che interessano la produzione nazionale o di prevalente interesse pubblico" ove si prevede che "quando il proprietario abbandona la conservazione, la coltivazione o l'esercizio di beni che interessano la produzione nazionale, in modo da nuocere gravemente alle esigenze della produzione stessa, può farsi luogo all'espropriazione". Al di fuori della disciplina dei diritti reali e della proprietà ricordiamo

l'art. 722 ove si prevede che le norme sulla indivisibilità dei beni (art. 720) e sulla determinazione delle condizioni di vendita degli immobili (art. 721) si applicano anche per i beni di interesse della produzione nazionale. All'art. 720 poi si prevede che tali beni «devono preferibilmente essere ricompresi per intero... nella porzione di uno dei coeredi... o di più coeredi se questi ne richiedono congiuntamente l'attribuzione».

Queste norme individuano solamente un regime particolare per i beni funzionali alla produzione nazionale ordinato alla garanzia del loro miglior utilizzo nell'interesse della collettività. Non vi è spazio per valutazioni in termini di sostenibilità.

Ancora l'art. 2050 c.c. contiene una norma riconosciuta come una delle più innovative del codice del 1942 e ordinata al fine di trovare una soluzione compromissoria tra gli opposti interessi della produzione e della tutela dei potenziali danneggiati dalle attività produttive pericolose ³³.

La disposizione, però, non contempera le esigenze della produzione con la tutela dei diritti individuali, ma piuttosto riconosce un onere della prova agevolato per la vittima che veda pregiudicati i propri diritti dall'esercizio dell'attività produttiva. In pratica le attività produttive ancorché pericolose sono consentite, purché non lesive di diritti altrui nel qual caso sorgeranno in capo all'esercente obbligazioni risarcitorie salva la prova, a suo carico, di aver adottato tutte le misure necessarie ad evitare il danno.

Riteniamo invece che il concetto di sostenibilità prenda corpo nel diritto privato per il tramite dell'applicazione diretta delle sopraricordate norme costituzionali (artt. 2,4,9,32,41 Cost.) oltre che del codice dell'ambiente ove come detto, risulta affermata la necessaria conformazione di ogni attività umana al principio di sostenibilità.

Va detto che, da un punto di vista applicativo, regole di sostenibilità nei rapporti tra privati sono piuttosto poste nei contratti, ovvero nel diritto dei privati in cui si vanno sviluppando

prassi negoziali di interesse in tal senso.

4. I contratti *Green* tra privati. Il fenomeno dei contratti sostenibili nel turismo

Il riferimento più immediato riguarda il contenuto degli statuti di associazioni di operatori economici che prevedono regole ordinate a imporre ai consociati o aspiranti tali condotte ritenute ecosostenibili pena la impossibilità di acquisire la qualità di socio oppure pena la revoca della qualità di socio acquisita.

In altri casi gli statuti sanciscono sanzioni di tipo premiale legate all'osservanza di condizioni di sostenibilità³⁴, come il riconoscimento di premi a favore dei soci che abbiano raggiunto un livello alto di conformità a standard di sostenibilità ambientale.

La sostenibilità è penetrata anche nei contratti tra imprese³⁵. Si parla ad esempio di *Green Franchising* con riferimento a quelle società affilianti le quali mettono a disposizione dei propri affiliati anche il proprio *know how* in termini di riduzione delle emissioni inquinanti e che prevedono nei propri codici di condotta il rispetto da parte degli affiliati di determinati standard ecologici.

Il tema si lega a quello della *Social Responsibility* delle imprese che orientano la propria attività non solo alla produzione e agli utili economici, ma anche a fini sociali. Da tempo la letteratura giuridica si va interessando ai codici di condotta redatti in funzione di *Social Responsibility* e ai rapporti tra *soft law* e *hard law*. I codici di condotta sarebbero ascrivibili alla *soft law* in quanto la loro osservanza sarebbe rimessa alla libera scelta dei consociati³⁶: è vero che, attraverso l'autonomia privata tali linee guida divengono regole del rapporto e la loro violazione rappresenta un'ipotesi di inadempimento contrattuale.

Nella gestione dell'impresa i codici di condotta rappresentano un sistema di autodisciplina volto a gestire rischi relativi all'impatto che l'attività di impresa può avere sulla persona e sull'ambiente. Si parla al riguardo di codici etici per distinguerli dai codi-

ci di condotta più legati a profili di organizzazione dell'impresa³⁷.

Il *Green Franchising* è un fenomeno che riguarda anche il marketing del prodotto sia nella commercializzazione dei prodotti verso il consumatore sia nella promozione dei contratti di franchising offerti sul mercato a imprese potenziali affiliate.

Sostenibilità è una parola chiave nel turismo. È diventata una priorità coniugare la crescita del settore turistico con la conservazione dei beni culturali: sia i cosiddetti beni culturali (musei, siti archeologici, ecc.), sia i beni ambientali (bellezze naturali, parchi, ecc.).

Il turismo sostenibile è importante perché viaggiare non dovrebbe essere dannoso per l'ambiente generalmente inteso. Dovremmo viaggiare in un modo che possa avvantaggiare le persone e le comunità in cui ci troviamo e che mitighi gli impatti negativi dei viaggi sull'ambiente. Il turismo sostenibile consiste nel dimostrare che ci prendiamo cura del mondo. Grazie al principio della sostenibilità il turismo ha il potenziale per rendere il mondo un posto migliore portando benefici economici alle destinazioni più povere, attraverso lo scambio culturale e la comprensione e attraverso l'auto-crescita.

Il turismo sostenibile e l'ecoturismo sono due modi possibili per affrontare i numerosi problemi ambientali e sociali associati al turismo. L'UNEP (Programma delle Nazioni Unite per l'ambiente) e l'UNWTO elencano 12 principi del turismo sostenibile: redditività economica, prosperità locale, qualità dell'occupazione, equità sociale, soddisfazione dei visitatori, controllo locale, benessere della comunità, ricchezza culturale, integrità fisica, diversità biologica, efficienza delle risorse e purezza ambientale. L'UNEP ha una lunga storia di contributo allo sviluppo e all'attuazione del diritto ambientale. DELC è la divisione all'interno dell'UNEP che sovrintende alle molteplici sfaccettature di questo quadro giuridico globale. Pertanto, il ruolo del DELC nel quadro dell'UNEP è principalmente quello di garantire il progressivo sviluppo del diritto ambientale in diversi settori am-

bientali e livelli di governance.

Il termine sostenibilità è legato ai contratti con i consumatori perché, come è noto, le affermazioni ambientali e di sostenibilità nella pubblicità dei prodotti, compresi i prodotti turistici, hanno un forte impatto. È quindi necessario distinguere le affermazioni ambientali corrette da quelle sleali, considerando l'impatto che possono avere sul comportamento economico del consumatore. Alcuni autori confrontano gli effetti di quattro tipi di annunci (pubblicità): un advertising (d'ora in poi 'adv') verde funzionale che promuove i vantaggi ambientali di un prodotto; un adv green emozionale che utilizza una rappresentazione visiva di uno scenario naturale gradevole, un adv verde di tipo misto implicante strategie funzionali ed emotive. I risultati di uno studio sperimentale, che utilizza un campione rappresentativo di consumatori statunitensi, suggeriscono che sia gli annunci emotivi che quelli di tipo misto possono influenzare significativamente l'atteggiamento del consumatore verso il marchio. Questi effetti non dipendono dal coinvolgimento ecologico dei consumatori. Gli annunci funzionali, al contrario, influiscono sugli atteggiamenti verso il marchio solo quando il coinvolgimento, misurato come comportamento di acquisto ecologico o atteggiamenti di prodotto ecologico, è elevato³⁸.

Alcuni autori si sono soffermati sui possibili interventi sostenibili degli operatori alberghieri tra cui sistemi alimentari sostenibili, soluzioni energetiche alberghiere, impatti della tecnologia, gestione dei rifiuti idrici e alimentari, progettazione di hotel ecologici, sistemi di certificazione ed ecolabel e la natura in evoluzione delle strategie di responsabilità sociale d'impresa³⁹.

L'approccio green può essere applicato sia ai prodotti che ai servizi e si sviluppa in ambiti molto diversi: dall'abbigliamento all'alimentare, dal turismo ai servizi per le aziende. Ognuna delle attività di franchising ecosostenibile si concentra su un compor-

tamento particolare, essenziale per vivere una vita più ecosostenibile ed eco-responsabile, che, come accennato in precedenza, sono: riduzione, riutilizzo e riciclo:

I franchising ecologici dedicati alla 'RIDUZIONE' rispondono alle esigenze delle aziende e dei privati in merito all'efficienza energetica o alla vendita di prodotti che riducano la produzione di rifiuti, come gli alimenti biologici venduti sfusi o i prodotti ecologici ottenuti dal riciclo. In questo caso, il franchisor normalmente garantisce tutta la formazione tecnica necessaria, soprattutto per le energie rinnovabili e i servizi impiantistici. L'affiliato è tenuto al rispetto degli obblighi formativi e delle regole di condotta, che sono normalmente contenute in un codice di condotta, cui il contratto fa riferimento come parte integrante del contenuto contrattuale. Rilevante, in tal modo, anche la previsione dei diritti del franchisor di effettuare controlli periodici e la previsione di termini di conguaglio nel caso in cui i controlli dovessero sfociare in inadempienze e sanzioni per i casi di tardivo conguaglio. Il mancato adattamento prolungato può portare alla risoluzione del contratto. Anche questo può essere espressamente previsto nel contratto.

I franchising ecologici che puntano sul 'REUSE' investono in un settore in crescita, come quello dell'usato, sfruttando tutte le opportunità offerte dall'e-commerce. I comportamenti eco-responsabili, come la rigenerazione delle cartucce o il riutilizzo di capi di abbigliamento e accessori per bambini, sono una tendenza consolidata e consolidata nelle abitudini di acquisto. Qualcosa di simile può essere applicato al settore dell'ospitalità. Gli hotel devono obbligare i propri ospiti a riutilizzare o riciclare gli asciugamani durante il soggiorno. Lavare gli asciugamani ogni giorno consuma troppa acqua, troppi detersivi e troppa energia. L'hotel di solito cerca di convincere i propri ospiti a riciclare o riutilizzare con una semplice carta in camera che richiede agli ospiti di riutilizzare

asciugamani o lenzuola. In questo caso, il franchisor deve fornire all'affiliato il proprio know-how in materia di comunicazione agli ospiti, anche se esistono prassi omogenee nel settore.

Le franchigie ecologiche specializzate nel 'RICICLO' valorizzano il riciclo e monetizzano la raccolta differenziata dei rifiuti, che non solo riduce l'impatto sull'ambiente, ma offre anche strumenti di fidelizzazione e reddito aggiuntivo per chi già possiede un'attività. Alcuni hotel e resort cercano di ridurre al minimo l'impatto diretto dell'attività turistica sull'ambiente attraverso varie iniziative: utilizzo e riciclaggio dell'acqua, riducendo l'impatto sull'ambiente.

Tuttavia, la sostenibilità include anche la sostenibilità sociale. Il franchising sostenibile bilancia le sue esigenze di business con l'impatto sulla salute e gli obiettivi di qualità ed equità del franchising sociale per la salute. L'affiliante e l'affiliato devono affrontare dei compromessi mentre scelgono le strategie di finanziamento: l'aumento del recupero dei costi da parte degli affiliati può influire sulla capacità del programma di servire i poveri; concentrarsi su prodotti ad alto margine piuttosto che sulla fornitura di servizi può ridurre l'impatto sulla salute; e i programmi spesso faticano a trovare un equilibrio tra la definizione delle priorità dei risparmi sui costi e le attività di formazione o assicurazione della qualità⁴⁰.

In questo senso assume importanza il know-how acquisito dal franchisor nella "comunicazione verde" con i consumatori. La formazione specifica e la consegna di segni distintivi, opuscoli, ecc. devono essere forniti dal franchisor. Devono inoltre essere presi provvedimenti per ridurre il rischio di lesione della proprietà intellettuale del franchisor.

Naturalmente, il franchising verde presenta anche sfide per l'affiliato: capacità tecnologica perché alcune attività verdi possono essere facilitate dalla tecnologia; attenta valutazione dell'investimento e dell'impegno necessario.

5. Conclusioni

Tra le conseguenze negative legate alle attività turistiche, vi è una possibile perdita dell'identità sociale e culturale del territorio ospitante, un aumento della produzione di rifiuti, un aumento del consumo di beni e risorse primarie (acqua, energia, ecc.), l'alterazione e distruzione di montagne, laghi, coste, ecosistemi marini, una perdita di biodiversità, impatti estetici e visivi, inquinamento del suolo e delle acque, congestione e inquinamento acustico, la concentrazione dei benefici in poche grandi aziende e/o paesi esteri, un aumento della domanda di mobilità, lavoro illegale e/o minorile e prostituzione.

L'impatto del turismo sull'ambiente può essere definito in termini di "pressione ambientale e sociale": maggiore afflusso di veicoli, maggiore presenza di persone, maggiore produzione di rifiuti e maggiore costruzione di nuove strutture ricettive.

Bisogna considerare non solo l'inquinamento emesso dai viaggi (aereo, auto, ecc.) ma anche fattori fondamentali come la costruzione e la manutenzione di alberghi, alimenti industriali negli alberghi, o souvenir tradizionalmente acquistati dai turisti, che sono invece considerati in studi più recenti.

La soluzione può essere trovata in interventi volti ad attuare divieti e limiti. Abbiamo qui invece voluto sottolineare il ruolo dell'autonomia privata nella regolamentazione di tutte le forme di turismo e nel governo dello sviluppo sostenibile. Si propone un approccio dal basso verso l'alto con una gestione condivisa dei problemi ambientali che derivano, in primo luogo: dal basso, cioè dalle imprese locali che, anche grazie agli input e alle richieste di soggetti esterni (organizzazioni di intermediari come associazioni di categoria e società civili), possono promuovere lo sviluppo di strategie e strumenti per l'attivazione di processi di gestione ambientale che coinvolgano l'intero territorio. In questa prospettiva, la partecipazione dei vari attori crea un processo

che, partendo dal sistema produttivo locale e dall'insieme condiviso delle sue esperienze e conoscenze degli operatori, riesce a coinvolgere le istituzioni territoriali e le società civili.

Parlando di sostenibilità e diritto privato, può dirsi che il principio di sostenibilità ha trovato una particolare applicazione nell'ambito del diritto dei privati ovvero di quelle regole che questi costruiscono nella cornice dell'autonomia loro riconosciuta dall'ordinamento. Il riferimento più immediato è alle clausole di sostenibilità contenute ad esempio nei c.d. *Green Franchising*. A livello applicativo si è posto inoltre il problema di valutare la sostenibilità dei prodotti commercializzati attraverso "dichiarazioni ambientali" nei rapporti con i consumatori.

Si evidenziano, da parte dell'ordinamento e delle stesse parti contraenti, esigenze di dare concretezza al concetto di sostenibilità che è definito solo a livello convenzionale. Gli indici ambientali sono così penetrati nei contratti e nel linguaggio di diritto privato rappresentando uno strumento per conferire oggettività ad un concetto, quello di sostenibilità, che non risulta avere confini delineati e immediatamente verificabili.

L'impiego del concetto di sostenibilità nei contratti e più in generale nei rapporti commerciali tra privati necessita di una determinazione attuata attraverso la sinergia tra i differenti saperi che si sono confrontati con tale termine.

Si tratta di un'operazione necessaria per rispondere a questioni di diritto privato: vi è stato o meno adempimento alla clausola di sostenibilità? La promozione di un prodotto come sostenibile risponde a standard aventi un livello di oggettività che esclude la ingannevolezza del messaggio?

Il punto è che l'adozione di indici quantitativi, indubbiamente utili nel determinare il concetto di sostenibilità, dovrà coniugarsi con le norme e i principi di diritto privato aprendo all'interpretazione dei giudicanti. Dare una misura alla sostenibilità non vuol dire mutare il ruolo dell'interprete nella soluzio-

ne dei problemi giuridici e nella applicazione delle regole ⁴¹. Applicare le norme vuol dire sempre interpretarle con un apporto creativo al loro contenuto.

Così nell'interpretare una clausola introduttiva di un'obbligazione di tenere una data condotta qualificata come eco-sostenibile e contenente indici ecologici per valutare la sua esatta esecuzione, sarà sempre possibile adeguare detta clausola alle circostanze concrete, ai fini del rispetto dell'economia del contratto attraverso, un'interpretazione secondo buona fede.

Parimenti gli indici ecologici potranno servire a "pesare" su basi oggettive la correttezza nell'uso di dichiarazioni ambientali nella commercializzazione dei prodotti, ma questo non esclude che la valutazione debba essere condotta alla luce delle clausole generali di diligenza professionale e di correttezza nei rapporti contrattuali per come elaborate dagli interpreti.

Sostenibilità e diritto dei privati

Note di chiusura

¹ G. PERLINGIERI, «Sostenibilità», *ordinamento giuridico e «retorica dei diritti»*. A margine di un recente libro, in *Foro nap.*, 2020, p. 101 ss.

Il principio dello sviluppo sostenibile ha trovato applicazione nella giurisprudenza amministrativa avuto particolare riguardo alle procedure di VIA (valutazione di impatto ambientale) e VAS (valutazione ambientale strategica) ovvero a quelle procedure, disciplinate a livello nazionale nel codice dell'ambiente, di valutazione in materia ambientale finalizzate alla piena realizzazione di detto principio. “La valutazione ambientale strategica (v.a.s.) è la valutazione delle conseguenze ambientali di piani e programmi al fine ultimo di assicurare lo sviluppo sostenibile del territorio sotto il profilo ambientale: si tratta, dunque, di un passaggio endoprocedimentale della pianificazione, concretantesi nella espressione di un parere che riflette la *verifica di sostenibilità ambientale della pianificazione stessa*. Si tratta, in quanto tale, di una procedura finalizzata precipuamente a mettere in rilievo le possibili cause di un degrado ambientale derivante dall'adozione di piani e programmi interessanti il territorio, introdotta dalla direttiva comunitaria 2001/42/ Ce che prevede, appunto, la sua applicazione a piani e programmi produttivi di effetti significativi sull'ambiente. Stante, poi, l'appartenenza alla competenza esclusiva dello Stato della materia relativa alla “tutela dell'ambiente”, ai sensi dell'art. 117 comma 2 lett. s) cost., il legislatore nazionale ha approntato a proposito della v.a.s. un'organica disciplina con il d.lg. 3 aprile 2006 n. 152 (cd. t.u. ambientale)”: così Corte giustizia UE, in 11 settembre 2012, n. 43, Nomarchiaki Aftodioikisi Aitoloakarnanias e altro, in *Diritto e Giustizia online* 2012, 12 settembre .

² M. PENNASILICO, *Economia circolare e diritto: ripensare la “sostenibilità”*, in *Persona e Mercato*, 2021, p. 714. Si veda anche C. VOIGT, *The principle of sustainable development. Integration and ecological integrity*, in ID. (ed.), *Rule of Law for Nature. New Dimensions and Ideas in Environmental Law*, Cambridge, 2013, p. 146 ss.; I. ALOGNA, *La circolazione del modello di sviluppo sostenibile. Prospettive di diritto comparato per un percorso multidirezionale*, in G. Cerrina Feroni et Al. (a cura di), *Ambiente, energia, alimentazione. Modelli giuridici comparati per lo sviluppo sostenibile*, I, 1, in *Cesfin.it*, 2016, p. 145 ss.; L. FASANARO, *Sviluppo sostenibile e storia internazionale: riflessioni storiografiche, problemi metodologici e visioni politiche*, in M. Merlati e D. Vignati (a cura di), *Una storia, tante storie. Studi di storia internazionale*, Milano, 2019, p. 255 ss.; G. ROSSI, *Dallo sviluppo sostenibile all'ambiente per lo sviluppo*, in *Riv. quadr. dir. amb.*, 1, 2020, p. 4 ss.; G. VETTORI, *Verso una società sostenibile*, in *Pers. merc.*, 2021, p. 463 ss.

³ La espressione tra virgolette è di M. PENNASILICO, in *Manuale di diritto civile dell'ambiente*, Napoli, 2014, p. 13. Dello stesso autore si veda anche *Contratto e uso responsabile delle risorse naturali*, in *Rass. Dir. Civ.*, 2014, p. 754; Si ricordano inoltre i contributi di A. LENER, *Ecologia, persona, solidarietà: un nuovo ruolo del diritto civile*, in N. Lipari (a cura di), *Tecniche giuridiche e sviluppo della persona*, Roma - Bari, 1974, p. 333; S. PATTI, *La tutela civile dell'ambiente*, Padova, 1979; P. PERLINGIERI, *I diritti umani come base dello sviluppo sostenibile. Aspetti giuridici e sociologici*, in *La persona e i suoi diritti. Problemi del diritto civile*, Napoli, 2005, p. 71 ss.

⁴ Cfr. M. PENNASILICO, *Contratto e uso responsabile delle risorse naturali*, cit., p. 754.

⁵ M. PENNASILICO, in *Manuale di diritto civile dell'ambiente*, cit., p. 161 e prima M. LIBERTINI, *La responsabilità d'impresa e l'ambiente*, in *La responsabilità dell'impresa*, Convegno per i trent'anni di Giurisprudenza commerciale, Bologna, 8-9 ottobre 2004, Milano, 2006, p. 199 ss

⁶Le riflessioni sul tema dei beni comuni in Italia sono risalenti. Si veda la nota monografia di P.GROSSI. *Un altro modo di possedere. L'emersione di forme alternative di proprietà alla coscienza giuridica post-unitaria*, Milano, 1977.

I suoi studi sono stati recentemente ripresi dalla nostra dottrina che ha individuato l'esigenza di sottrarre una serie di beni, funzionali al soddisfacimento di interessi fondamentali della persona, alla logica dell'appropriazione esclusiva propria del diritto di proprietà per come definito nel nostro codice civile. In particolare si segnalano: A.LUCARELLI, *Introduzione: verso una teoria giuridica dei beni comuni*, in *Rass. Dir. pubbl. eur.*, 2007, 2, p. 3 ss.; U.MATTEI, *Beni comuni. Un manifesto*, Roma-Bari, 2011; G.CARAPEZZA FIGLIA, *Oggettivazione e godimento delle risorse idriche. Contributo a una teoria dei beni comuni*, Napoli, 2008; ID., *Premesse ricostruttive del concetto dei beni comuni nella civilistica italiana degli anni Settanta*, in *Rass. Dir. civ.*, 2011, p. 1061ss.; M.R.MARELLA, *Per un diritto dei beni comuni*, in M.R.Marella (a cura di) *Oltre il pubblico e il privato. Per un diritto dei beni comuni*, Ed. Ombre Corte, Verona, 2012, p. 9; I. GARACI, *Lo statuto giuridico dei «nuovi beni» immateriali: fra proprietà privata e beni comuni*, in *Rass. Dir. civ.*, 2015, 2, p. 434.

⁷ Avevamo già messo in luce il fenomeno nel nostro *Travel and Tourism Contracts*, in *Book Series The Power of Law directed by G. Alpa*, Anteazza, 2013, p. 151 ss. Il saggio riprende in parte il nostro saggio *Clausole di sostenibilità nei contratti tra privati. Problemi e riflessioni*, in *Dir.pubbl.*, 2015, pp. 611-636

Sul punto v. anche M. PENNASILICO, *Sviluppo sostenibile, legalità costituzionale e analisi "ecologica" del contratto**, in *Studi in onore di Grasso*, in corso di pubblicazione.

⁸ Sul punto M. PENNASILICO, in *Manuale di diritto civile dell'ambiente*, cit., p. 27. È consolidata l'affermazione che i principi a differenza delle norme avrebbero un contenuto indeterminato che lascerebbe spazio all'interpretazione dei giudici R. DWORKING, *The Model of Rules*, I in *Taking the Rights Seriously*, Cambridge, Mass., 1977, p. 14 ss.; R. GUASTINI, *Teoria e dogmatica delle fonti*, in *Tratt. dir.civ. comm. Cicu-Messineo*, continuato da L. Mengoni, Milano, 1998, p. 272 ss.; R. ALEXY, *Concetto e validità del diritto* (1992), Torino, 1997, p. 129 ss.; J. RAZ, *Legal Principles and the Limits of Law*, in *Yale Law Journal*, 1972, p. 823 ss.; A. PINTORE, *Norme e principi, una critica a Dworkin*, Milano, 1982, p. 19 ss.; P. COMANDUCCI, *Principi e indeterminazione del diritto* (1997), in *Id.*, *Assaggi di metaetica a due*, Torino, 1998, p. 81 ss.; G. PINO, *I principi tra teoria della norma e teoria dell'argomentazione giuridica*, in *Diritto e questioni pubbliche*, 2011, p. 75 ss.; U. SCARPELLI, *Dalla legge al codice, dal codice ai principi*, in *Rivista di filosofia*, 1987, pp. 3 ss.; A. FALZEA, *I principi generali del diritto* (1991), in *Id.*, *Ricerche di teoria generale del diritto e di dogmatica giuridica*, vol. I, Milano, 1999, pp. 337-338; G. ZAGREBELSKY, *Il diritto mite. Legge diritto giustizia*, Torino, 1992, p. 47. Afferma GROSSI, *L'odierna "incertezza" del diritto*, in *Giust. Civ.*, 2014, p. 937: "Il principio ha una potenzialità e, pertanto, anche una ricchezza, che è ignota a ogni proposizione legale. Il principio serba in sé una natura efficacemente espansiva."

Altre le osservazioni che si possono compiere sull'indeterminatezza dei concetti fatti propri dal legislatore in norme di diritto amministrativo. Come osservato la indeterminazione, che svolge di norma la preziosa funzione di conferire "elasticità e dinamicità all'ordinamento", apre ad una maggiore discrezionalità nell'esercizio del potere da parte della pubblica amministrazione rappresentando una possibile insidia per i cittadini. Cfr. E. FERRERO, *Concetti giuridici indeterminati e poteri discrezionali delle amministrazioni*, in *Dir. Proc. Amm.*, 2014, p. 761. Peraltro il concetto di sostenibilità è particolarmente "giovane" e non trova determinazione neppure in una consolidata cultura giuridica sul punto. Il tema richiama le osservazioni di P. CARNEVALE, *Diritto, normazione e ambiguità*, in *Dir. Pubbl.*, 2013, p. 353 e in particolare p 360 ove parla di "ambiguità provocata" con riferimento all'introduzione da parte del legislatore di concetti nuovi privi di una tradizione.

⁹ W.M. ADAMS, *The Future of Sustainability: Re-thinking Environment and Development in the Twenty-first Century*, (2006). Report of the IUCN Renowned Thinkers Meeting, 29-31 January 2006.

United Nations General Assembly (1987) *Report of the World Commission on Environment and Development: Our Common Future*. Transmitted to the General Assembly as an Annex to document A/42/427 - Development and International Co-operation: Environment. La commissione riprendendo la sua risoluzione

ne del 19 dicembre 1983, n. 38 su “Preparation Process for Environmental Perspective to the Year 2000” accoglieva la costituzione di una speciale commissione che più tardi è stata chiamata “World Commission on Environment and Development”.

¹⁰ United Nations General Assembly (2005). 2005 World Summit Outcome, Resolution A/60/1, adottata dalla General Assembly il 15 Settembre 2005. Il documento è leggibile sul sito:

<http://www.who.int/hiv/universalaccess2010/worldsummit.pdf>

¹¹ The Earth Charter Initiative (2000). <http://www.earthcharterinaction.org/content/pages/Read-the-Charter.html>

¹² M. REDCLIFT, *Sustainable Development (1987-2005): an Oxymoron Comes of Age*, in *Problems of Sustainable Development*, (2009) 4/1 , pp. 33-50.

¹³ J.R. HICKS, *The foundation of welfare economics*, in *Economic Journal*, 49 (1939), pp. 194-300; H. S. HOUTHAKKER, *Can Speculators Forecast Prices?*, in *Review of Economic Studies*, 1957, 143-151; R. G. LIPSEY – K. LANCASTER, *The General Theory of Second Best*, in *The Review of Economic Studies*, Vol. 24, No. 1. (1956 - 1957), pp. 11-32.

¹⁴ P.J. BOETTKE, P. LESSON, C. Y. COYNE, *The Continuing Relevance of F.A. Hayek's Political Economy*, in *Advances in Austrian Economics*, 2008, pp. 79-98.

¹⁵ Si veda <http://www.worldsustainable.org/>

¹⁶ Il tema del contratto come strumento di sviluppo sostenibile ha trovato da tempo riconoscimento nella dottrina amministrativistica. Si veda in particolare S. NESPOR, *I contratti ambientali: una rassegna critica*, in *Dir. pubbl. comp. eur.*, 2003, p. 962 ss. il quale parla di “contratti ambientali” come accordi tra due o più parti una delle quali almeno pubblica aventi ad oggetto prestazioni di rilevanza ambientale. V. anche E. BELLOMO, *Il Green Public Procurement nell'ambito della Green Economy*, in *Dir. proc. amm.*, 2013, p. 163 ss.; G. FIDONE, *L'integrazione degli interessi ambientali nella disciplina dei contratti pubblici: il Green Public Procurement*, in G.F. Cartei (a cura di), *Cambiamento climatico lo stato dell'arte*, Torino, 2013, p. 123 ss.; C. GUCCIONE E L. PALATUCCI, *Profili ambientali nelle procedure ad evidenza pubblica*, in *Tratt. dir. amb. Dell'Anno e Picozza*, II, *Discipline ambientali di settore*, Padova, 2013, p. 727 ss.

Come osserva M. PENNASILICO, *Contratto e uso responsabile delle risorse naturali*, cit., p. 757 l'appalto pubblico verde indica “l'effetto e la funzione del ricorso a criteri valutativi ecologici nella formazione, interpretazione ed esecuzione di appalti pubblici vale a dire la promozione e integrazione degli interessi ambientali nella materia dei contratti pubblici...” Le stazioni appaltanti inse-

riranno nei bandi di gara tra i criteri di aggiudicazione “clausole ecologiche” in modo da orientare la scelta del contraente in funzione di interessi ambientali. “La funzione dell’appalto verde non è soltanto premiale, ma anche correttiva del mercato e responsabilmente preventiva rispetto a sprechi di energia e risorse naturali, consumi eccessivi e danni ambientali”.

¹⁷ Vedi R.G. LIPSEY - K.LANCASTER, *op. loc. citt.*

¹⁸ J.MARKUS, M.K. MILNE, K. KEARINS, & S. WALTON, *Creating Adventures in Wonderland: The Journey Metaphor and Environmental Sustainability*, in *Organization*, (2006) 13/6, pp. 801-839.

¹⁹ B.D. RATNER, *Sustainability as a Dialogue of Values: Challenges to the Sociology of Development*, in *Sociological Inquiry*, (2004) 74/1, pp. 50-69. See also J.D. MARSHALL, & M.W. TOFFEL, *Framing the Elusive Concept of Sustainability: A Sustainability Hierarchy*, in *Environmental & Scientific Technology*, (2005) 39/3, pp. 673-682 and , J. BLEWITT, *Understanding Sustainable Development*, London, 2008, pp. 21-24.

²⁰ “If sustainability is to mean anything, it must act as an integrating concept. In particular, it is clear that the social dimensions of sustainability must be integrated with the biophysical dimensions... Clearly the very concept of sustainability is predicated on a need to think across temporal scales. And both the social and ecological dimensions of the term bring to the fore the need for spatial integration. The disciplinary division of knowledge in the university system means that many cross-scalar issues get lost in the ‘white spaces’ between disciplines. The concept of sustainability may have a role in helping to bridge some of those gaps”: J. ROBINSON, *Squaring the circle? Some thoughts on the idea of sustainable development*, in *Ecological Economics* 48 (2004) 369-384 e in particolare p. 378.

²¹ Sul punto In tal senso E. NAVARRETTA, *Bilanciamento di interessi costituzionali e regole civilistiche*, in *Riv. crit. dir. priv.*, 1998, p. 637 ss.; ID., *Diritti inviolabili e risarcimento del danno*, Torino, 1996, p. 53 ss.; F.D. BUSNELLI - E. NAVARRETTA, *Abuso del diritto e responsabilità civile*, in *Diritto Privato*, III, 1997, p. 171 ss.

²² Un'impronta personalistica all'idea di sostenibilità è conferita dall'interpretazione che i giudici hanno dato della stessa. Si veda da ultimo Tar. Campania 2 dicembre 2013, in *Foro Amm. TAR*, 2013, 3802 per il quale uno sviluppo sostenibile è quello che vede “garantita la qualità della vita e della salute quale valore umano fondamentale di ogni persona e della società (informazione, partecipazione ed accesso)”.

²³ Cfr. U. MATTEI voce “Immissioni”, in *Dig. disc. priv. sez. civ.*, vol. XI, Torino 1993, p. 311

²⁴ Il giudice, poi, può tenere conto della priorità di un determinato uso. Il c.d. criterio del preuso, tuttavia, “è stato interpretato come un elemento che rientra nel giudizio di contemperamento di cui al 2° comma con una evidente forzatura interpretativa. Ridotto in questo angusto spazio, il criterio del preuso risulta schiacciato dalle ben più forti ragioni della produzione. È viceversa nell’ambito del giudizio sulla tollerabilità (un giudizio in cui le ragioni dell’impresa possono non entrare affatto), che il criterio *first-come first-served* può spiegare i suoi effetti”. Cfr. A. MUSY, *Immissioni sonore nell’isola di Ponza, regole economiche superstiziose e soluzioni giuridiche*, nota a Cass. Sez. Un. 29 luglio 1995 n. 8300, in Giur. It. 1996, 1, I, c. 328 ss.

²⁵ Corte Cost., 23 luglio 1974 n. 247, in *Giust. Cost.*, 1974, p. 2371, e in *Giur. It.* 1975 I, 1, 3, con nota di Salvi, *Legittimità e razionalità dell’art. 844 c.c.* e più recentemente Corte Cost. 18 luglio 1986 n. 184 in *Giust. Cost.*, 1986, 1430.

Quanto poi al giudizio sulla “intollerabilità” i giudici tendono ad interpretare l’art. 844 nel senso che per stabilire se una immissione sia o meno tollerabile, occorra avvalersi di analisi tecniche eseguite non già per verificare l’eventuale superamento di valori standard contenuti in norme pubblicistiche bensì per accertare la condizione di colui che lamenta le altrui immissioni Cass. 1° luglio 1994 n. 6242, in *Foro it.*, 1995, I, 1260 e più recentemente Cass. 1° febbraio 2011 n. 2319, in *Mass. Foro it.*, 2011; Cass. 17 gennaio 2011 n. 939, *ibidem*.

²⁶ Cass., 11 settembre 1989 n. 3920, in *Mass. Foro it.*, 1989; Cass. Sez. Un. 19 luglio 1985 n. 4263, in *Giust. civ.*, 1986, I, 128. Per la giurisprudenza di merito Trib. Verona 13 ottobre 1989, in *Giur. It.* 1990, I, 2, 374, con nota di F. Basile, *Danno alla salute e immissioni intollerabili*; Trib. Milano, 7 giugno 1988, in *Foro It.*, 1989, I, 903; Trib. Napoli, 22 febbraio 1983, in *Dir. Giur.*, 1983, 354, con nota di R. Sgobbo, *La disciplina delle immissioni tra Codice Civile e Leggi Speciali: a proposito di un nuovo caso Italsider*.

In dottrina A. DE CUPIS, *Disciplina delle immissioni e tutela della salute*, in *Riv. Trim. Dir. e Proc. Civ.*, 1983, p. 252; C. SALVI, voce “Immissioni”, in *Enc. Giur. Trecani*, XV, Roma, 1989, p. 8; Id., *Le immissioni industriali*, Milano, 1979, p. 353; G. VISINTINI “Immissioni (Dir. Civ)”, in *Noviss. Dig. It.*, Appendice, III, Torino, 1982, p. 1220; V. SCALISI, *Immissioni di rumore e tutela della salute*, in *Riv. Dir. Civ.* 1982, I, p. 1927; P. PERLINGERI, *Il diritto alla salute quale diritto alla personalità*, in *Rass. Dir. Civ.*, 1982, p. 1030 ss.; A. IANNELLI, *Sulla tutela delle immissioni industriali e sulla non operabilità dell’art. 844 c.c.*, in *Rass. Dir. Civ.*, 1980, 376; A. D’ANGELO, *L’art. 844 c.c. e il diritto alla salute*, in *Tutela della salute e diritto privato*, a cura di Busnelli e Breccia, Milano, 1978, p. 433.

²⁷ V. In particolare A. DE CUPIS, *op. cit.*, p. 252, il quale afferma che “la normale tollerabilità enunciata nell’art. 844 c.c., è un criterio ispirato ad una media valutazione, adeguato ad un equo contemperamento di interessi patrimoniali, ma inapplicabile, a meno di forzarne il significato, alla tutela della salute, in relazione alla quale va tenuto conto dell’influenza lesiva delle immissioni nell’organismo fisico – psichico del singolo individuo”.

²⁸ V. in special modo G. VISINTINI, *op. loc. citt.*

²⁹ “La tutela ex art. 844 c.c. basta a garantire il ristoro del danno alla salute in dipendenza da immissioni intollerabili di fumo provenienti dal fondo altrui, non essendo necessario proporre autonoma domanda ex art. 2043 c.c.”: così Cass. 23 maggio 2013, in *Giust. Civ.*, 2013, p. 2381 ss.

Quanto al rapporto tra le differenti azioni “l’azione inibitoria ex art. 844 c.c. può essere esperita dal soggetto leso per consentire la cessazione delle esalazioni nocive alla salute, salvo il cumulo con l’azione per la responsabilità aquiliana prevista dall’art. 2043 c.c. nonché con la domanda di risarcimento del danno in forma specifica ex art. 2058 c.c.”: così Corte app. Roma 30 gennaio 2013, in *Redazione Giuffrè* 2013. Con riferimento alla complementarietà tra tutela reintegratoria e tutela inibitoria si veda R. PARDOLESI, *Azione reale e azione di danni nell’art. 844. Logica economica e logica giuridica nella composizione del conflitto tra usi incompatibili della proprietà vicine*, in *Foro.it*, 1977, I, 1149.

Infine, in pronunce di merito il comportamento lesivo del diritto alla salute è stato inibito attraverso il ricorso all’art. 700 c.p.c. V. da ultimo Trib. Roma 9 maggio 2011 “Le immissioni acustiche intollerabili provenienti da strutture parrocchiali (prolungato rintocco di campane e schiamazzi) sono suscettibili di essere oggetto di una pronuncia inibitoria all’esito di un procedimento d’urgenza ex art. 700 c.p.c. in quanto costituenti fenomeno idoneo a cagionare un danno alla salute, dovendo escludersi l’applicazione del criterio della priorità di un determinato uso, parametro avente carattere meramente facoltativo e residuale.” Si veda inoltre *ex plurimis* Trib. Salerno, 3 novembre 2004, *Redazione Giuffrè* 2005; Pret. Torino 27 dicembre 1990 in *Dir. Fam.*, 1991, 1060.

Tale giurisprudenza si pone nel solco di quella letteratura che rinviene nell’art. 700 c.p.c. un rimedio inibitorio esperibile contro qualsiasi tipo di illecito. Si veda A. FRIGNANI, *L’injunction nella common law e l’inibitoria nel diritto italiano*, Milano, 1974, p. 441.

³⁰ Cfr. P. PERLINGIERI, *La personalità umana nell’ordinamento giuridico*, Napoli, 1972 passim e in specie p. 139; Id., *Depatrimonializzazione e diritto civile*, in *Rass. dir. civ.*, 1983, p. 4; C. DONISI, *Verso la «depatrimonializzazione» del diritto privato*, in *Rass. dir. civ.*, 1980, 644 ss.; A. DE CUPIS, *Sulla “depatrimonializzazione” del diritto privato*, in *Riv. dir. civ.*, 1982, II, 482 ss.

³¹ Cass., 12 luglio 2016, n. 14180, in pluris-cedam.utetgiuridica.it.

³² Si veda V. CORRIERO, *Sviluppo ecologico e strumenti negoziali di valorizzazione dei "beni culturali, paesaggistici e ambientali"*, in *Rivista quadrimestrale dir. amb.*, 2020, p. 106.

³³ Si veda in particolare sul punto D. DE MARTINI, *Responsabilità per danni da attività pericolosa e responsabilità civile per danni nell'esercizio di attività pericolosa*, *Giur.It.*, 1973, I, 2, 978; M. COMPORATI, *Responsabilità civile per esercizio di attività pericolose*, in *Fondamento e funzione della responsabilità civile*, a cura di Buonocore e Majello, Napoli, 1975, p. 77.

³⁴ È il caso di Emeraude hoteliers un premio che viene riconosciuto da IHRA (international hotel restaurants association). Si rinvia sul punto al nostro *Travel and Tourism Contracts. Design of Sustainable Tourism Systems*, Antezza, 2013, p. 151 ss.

³⁵ V. supra nota 18 sul *Green Procurement*.

³⁶ Cfr. A. C. FERNANDO, *Business Ethic and Corporate Governance*, Pearson, 2010; AA.VV. *Corporate Social Responsibility*, R. MULLERAT - D. BRENNAN (a cura di), Kluwer Law International, 2010.

³⁷ Cfr. G. CONTE, *Codici etici e attività d'impresa nel nuovo spazio globale di mercato*, in *Contr.impr.*, 2006, I, p.108; ID., *La disciplina dell'attività di impresa tra diritto, etica ed economia*, in G. Conte (a cura di), *La responsabilità sociale dell'impresa*, Bari-Roma, 2008, p. 3; S. ROSSI, *Luci e ombre dei codici etici d'impresa*, in *Riv. dir. soc.*, 2008, I, p. 26; C. ANGELICI, *Responsabilità sociale di impresa, codici etici e autodisciplina*, in *Giur. Comm.*, 2011, II, p. 159; F. DEGLI INNOCENTI, *Rischio di impresa e responsabilità civile. La tutela dell'ambiente tra prevenzione e riparazione dei danni*, Firenze, 2014, p. 63.

³⁸ Matthes, Wonneberger, Schmuck (2014) *Consumers' green involvement and the persuasive effects of emotional versus functional ads*, in *Journal of Business Research*, (67. 9), p. 1885.

³⁹ Legrand, Sloan, Chen (2017) *Sustainability in the Hospitality Industry: Principles of sustainable operations*, Routledge: London.

⁴⁰ Possiamo elencare diversi vantaggi dell'investimento in franchising ecologici/sostenibili: i) opportunità di business ad alta fedeltà; ii) consumatori sensibili alla ricerca di prodotti affidabili; iii) accurata attenzione alle strategie di marketing all'avanguardia; iv) alto tasso di innovazione e creatività; v) buona facilità di accesso, economica e logistica; vi) riduzione dei costi.

⁴¹ Cfr. H.G. GADAMER, *Wahrheit und Methode. Grundzüge einer philosophischen Hermeneutik*, Tübingen, 1960, in particolare p. 277. Più recentemente J. ESSER,

Sostenibilità e diritto dei privati

Precomprensione e scelta del metodo nel processo di individuazione del diritto, trad. it. di G. Zaccaria e S. Patti, Napoli, 1983; G. ZACCARIA, *Ermeneutica e giurisprudenza. Saggio sulla metodologia di Josef Esser*, Milano, 1984, p. 47 ss.; P. NERHOT, *Il diritto, lo scritto, il senso. Saggio di ermeneutica giuridica*, trad. it., Ferrara, 1992, p. 61 ss.; G. FURGIUELE, *Note minime in tema di norma, ordinamento e interpretazione*, in *Studi in onore di G. Benedetti*, Napoli, 2008, p. 750 *Contra* G. MESSINA, *L'interpretazione dei contratti*, Macerata, 1906, ora in *Scritti giuridici*, vol. V, Milano, 1948, p. 153 ss.; C. GRASSETTI, *L'interpretazione del negozio giuridico con particolare riguardo ai contratti*, Padova, 1939 in part. p. 96 ss.; ID., *Intorno al principio di gerarchia delle norme di interpretazione*, in nota a Cass. 24 giugno 1940, n. 2079, in *Foro it.*, 1941, I, 511. I paragrafi 1, 4 riprendono il saggio Sara Landini (2022). Sostenibilità e “diritto dei privati” nel settore turistico. *Rivista trimestrale di Diritto dell'Economia*, pp. 100-124.

Indice degli autori

ENRICO AL MUREDEN

Professore ordinario di diritto privato presso l'Università di Bologna

ANTONINA ASTONE Professoressa associata di diritto privato presso l'Università degli Studi di Messina

ETTORE BATTELLI

Professore associato di diritto privato presso l'Università degli Studi di Roma Tre

GIOVANNI BERTI DE MARINIS

Professore associato di diritto dell'economia presso l'Università degli Studi di Perugia

MARCO CARLIZZI

Avvocato del Foro di Roma, dottore di ricerca in diritto commerciale – Università di Roma “Tor Vergata”

ENRICO CATERINI

Professore ordinario di diritto privato presso l'Università della Calabria

ANTONELLA CORRENTI Assegnista di diritto privato comparato presso l'Università degli Studi di Messina

MARCO FASCIGLIONE

Ricercatore di Diritto internazionale e di Tutela dei diritti umani, CNR-IRISS

ILARIA GARACI

Professoressa associata di diritto privato presso l'Università Europea di Roma

SARA LANDINI

Professoressa ordinaria di diritto dell'economia presso l'Università degli Studi di Firenze

FRANCESCO MEZZANOTTE

Professore associato di diritto privato presso l'Università degli Studi di Roma Tre

ROBERTA MONTINARO

Professoressa ordinaria di diritto privato presso l'Università di Napoli L'Orientale

ROSARIO PETRUSO

Professore associato di diritto privato comparato presso l'Università degli Studi di Palermo

GUIDO SMORTO

Professore ordinario di diritto privato comparato presso l'Università degli Studi di Palermo



IL TORCOLIERE • Officine Grafico-Editoriali d'Ateneo

Università di Napoli L'Orientale
stampato nel mese di giugno 2023



**UNIVERSITÀ DI NAPOLI
L'ORIENTALE**

Dipartimento di Scienze Umane e Sociali

Il libro esamina le questioni giuridiche più rilevanti legate all'evoluzione delle tecnologie digitali e, in particolare, allo sviluppo di sistemi intelligenti, al loro impatto sui diritti umani e alla imputazione delle responsabilità.

Gli autori esplorano le soluzioni in grado di promuovere e garantire la sostenibilità dell'innovazione, attraverso azioni preventive e la protezione *by design*. Del resto, le tecnologie digitali contribuiscono a migliorare la valutazione dei rischi, a promuovere la trasparenza e l'efficienza dei servizi digitali, nel rispetto degli obiettivi dello sviluppo sostenibile. Specifica attenzione è rivolta ai settori assicurativo, bancario e turistico.

ILARIA GARACI - Professore associato di Diritto privato nell'Università Europea di Roma, dove insegna Diritto privato ed Elements of Italian Private Law. È membro del Collegio dei docenti nel Corso di Dottorato in "Persona, benessere e innovazione", presso l'Università Europea di Roma. Relatrice in seminari e conferenze nazionali e internazionali, è autrice di due lavori monografici e di diversi contributi in materia di beni immateriali e tutela della persona, tutela del consumatore, responsabilità civile, rimedi restitutori, diritti dei minori di età.

ROBERTA MONTINARO - Professore ordinario di Diritto Privato, insegna Diritto privato e Diritto privato dell'economia digitale presso il Dipartimento di Scienze Umanistiche e Sociali dell'Università di Napoli L'Orientale. È coordinatore scientifico del Modulo Jean Monnet "DiCIT - Digital Citizenship in the European Union" e membro del collegio dei docenti del Dottorato Nazionale in Intelligenza Artificiale. È stata relatrice e coordinatrice scientifica di seminari e conferenze nazionali e internazionali. Autrice di monografie, ha pubblicato anche articoli e saggi in libri e riviste scientifiche, in italiano e in inglese. I suoi principali interessi di ricerca riguardano il diritto dei trust, la responsabilità civile, il diritto dei consumatori e il diritto delle tecnologie digitali.

ISBN 978-88-6719-276-2