PERCORSI

Diritto

La pubblicazione di questo volume è stata possibile grazie al contributo dell'Università degli studi di Padova – Centro interdipartimentale di ricerca per le decisioni giuridico-ambientali ed etico-sociali sulle tecnologie emergenti (CIGA)

GIORGIA GUERRA

LA SICUREZZA DEGLI ARTEFATTI ROBOTICI IN PROSPETTIVA COMPARATISTICA

Dal cambiamento tecnologico all'adattamento giuridico

SOCIETÀ EDITRICE IL MULINO

I lettori che desiderano informarsi sui libri e sull'insieme delle attività della Società editrice il Mulino possono consultare il sito Internet: **www.mulino.it**

ISBN 978-88-15-27976-7

Redazione e produzione: Edimill srl - www.edimill.it

Finito di stampare nel mese di ottobre 2018 presso LegoDigit s.r.l. - Lavis (TN)

INDICE

PREMESSA

> Un'intelligenza che dirige un corpo è qualcosa di molto diverso da un corpo e una mente sinergici.
>
> R. Cingolani e G. Metta, *Umani e umanoidi. Vivere con i robot*, Bologna, Il Mulino, 2015

«Comparative Law in action».

Nei primi mesi dell'anno, queste parole, riferite all'uso della comparazione quale metodo per risolvere casi di diritto commerciale internazionale, tanto mi fecero riflettere sul modo in cui stavo conducendo, a ben altre «latitudini», la mia ricerca.

Il dialogo avviato con studiosi afferenti al mondo scientifico (e non solo) per capire la complessa realtà analizzata, mi ha portata a sperimentare modi e strumenti «dinamici» della ricerca. A tal fine, sono grata, per il tempo dedicatomi, a tutti quei docenti afferenti alle Università di Padova (in particolare al Security and Privacy Research Group e Human Inspired Technology Research Centre); di Verona e del Politecnico di Milano, i quali hanno accettato di essere intervistati da me. Molte volte ho rimodulato l'analisi sulla base dei nostri dialoghi.

Un ringraziamento speciale è per due professori che «ci sono sempre»: Sergio Gerotto e Filippo Viglione del Dipartimento di Scienze Politiche, Giuridiche e Studi Internazionali dell'Università di Padova per i consigli e il supporto.

Il lavoro ha beneficiato dei preziosi suggerimenti della professoressa Cristina Amato dell'Università di Brescia, e della professoressa Erica Palmerini dell'Università Sant'Anna di Pisa. A loro va tutta la mia gratitudine, anche per aver trovato il tempo di leggere la bozza in piena estate.

Tutti i limiti dell'opera sono attribuibili solo a me.

Questo libro è dedicato a Roberto e Riccardo per l'inesauribile pazienza... torno subito! ... senza robot intorno!

INTRODUZIONE

1. *Il contesto*

Questo lavoro si colloca nel contesto degli studi dedicati al rapporto tra diritto e tecnologia. Esiste già una lunga tradizione storica che vede i giuristi occuparsi dei problemi posti dalle nuove tecnologie[1]. Solo negli anni più recenti, però, le analisi giuridiche hanno approfondito le dinamiche sottese al più complesso concetto di «cambiamento tecnologico», da cui queste pagine muovono.

Non è negli intenti dello scritto inoltrarsi nel dibattito relativo alla configurazione di una teoria generale della *law and technology*[2]. L'obiettivo, più modesto, si propone di utilizzare gli strumenti di indagine impiegati dal diritto comparato, *in primis* transnazionalità e apertura verso altri saperi[3], per analizzare il tema della sicurezza

[1] I primi scritti dedicati ai problemi giuridici delle nuove tecnologie sono apparsi sullo *Yale Law Journal* e sono risalenti alla fine dell'Ottocento. Per una ricostruzione della letteratura giuridica in materia si rinvia a K. Tranter, *The Law and Technology Enterprise: Uncovering the Template to Legal Scholarship on Technology*, in *Law Innovation & Tech*., 3, 2011, pp. 31-82. Anche la dottrina italiana ha contribuito significativamente allo studio della materia. Tra i tanti si rinvia a S. Rodotà, *Tecnologie e diritti*, Bologna, Il Mulino, 1995; e N. Irti ed E. Severino, *Dialogo fra diritto e tecnica*, Roma-Bari, Laterza, 2001 (già in *Contratto e impr.*, 2000, pp. 665 ss.). Questo lavoro muove, però, dal più ampio e inclusivo concetto di «cambiamento tecnologico», vedi *infra* par. 2.

[2] Per una ricostruzione del dibattito in materia si rinvia, tra i tanti, a G.N. Mandel, *Towards a General Theory of Law and Technology*, in *Minn J.L., Sci & Tech*, 8, 2007, pp. 441-644.

[3] Tra questi, mi sono avvalsa, in particolare, dell'emergente ambito degli studi interdisciplinari dedicati al rapporto tra diritto, regolamentazione e tecnologia. Nel panorama internazionale, un primo riferimento in materia è proposto da R. Brownsword, E. Scotford e K. Yeung, *Law,*

con riguardo al frutto della «nostra invenzione finale»[4]: la robotica.

Le potenzialità dei prodotti robotici stanno già mutando i limiti di ciò che l'uomo può fare, provocando cambiamenti profondi nella società civile, nel mercato del lavoro e in ogni ambito della vita quotidiana[5].

I tratti caratterizzanti quello che, a un tempo, è motore dell'*industry 4.0* e della *disruptive technology* pongono nuove sfide nella ricerca di un bilanciamento tra innovazione desiderabile ed esigenze di sicurezza[6]. D'altro canto, il problema del controllo degli effetti delle nuove tecnologie – noto come «dilemma di Collingridge» – è ricorrente, poiché «quando cambiare il corso di una tecnologia è ancora facile, non ne comprendiamo la necessità; quando il bisogno di un cambiamento è evidente è ormai difficile e costoso introdurlo»[7].

Il paradosso è già chiaro: da un lato, il futuro appare sempre più a portata di mano, migliorabile e modellabile; dall'altro, la pervasività e l'impatto del cambiamento tecnologico sui valori costituzionalmente tutelati, e sulla sicurezza delle stesse rivoluzionarie applicazioni, è condizione ineliminabile. Anzi, in alcune circostanze, l'incertezza cede il passo all'indeterminatezza.

La regolamentazione non si prefigge di raggiungere irrealizzabili scenari *0-risk*, quanto piuttosto di contenere il rischio entro limiti ritenuti ragionevoli[8]. L'obiettivo rima-

Regulation and Technology: The Field, the Frame and the Focus, in Idd., *The Oxford Handbook of Law, Regulation and Technology*, Oxford, Oxford University Press, 2017, p. 3.

[4] L'espressione è di J. Barret, *Our Final Invention: Artificial Intelligence and the End of the Human Era*, New York, Thomas Dunne books-St. Martin's Press, 2013.

[5] Per una lettura economica sul tema: C.B. Frey e M.A. Osborne, *The Future of Employment: How Susceptible Are Jobs to Computerisation?*, in *Technological Forecasting and Social Change*, 114/C, 2017, pp. 254-280.

[6] KPMG's 2017 Technology Innovation Survey, 2017.

[7] D. Collingridge, *The Social Control of Technology*, New York, St. Martin's Press, 1980.

[8] Sulla soglia di accettabilità del rischio nel campo della responsabilità da prodotto vedi G. Howells, *Consumer Safety in Europe: In Search of*

ne, in ogni caso, complesso. L'ampio scenario dei prodotti della convergenza tecnoscientifica rievoca una riflessione originatasi intorno alla governance europea della scienza, che il sociologo Brian Wynne ha riassunto in una efficace e provocatoria domanda: «safety or risk from precisely what?»[9].

In effetti, in apertura al *Münster Colloquia on EU Law and the Digital Economy*, il professor Reiner Schulze sembra «trasporre» questo stesso interrogativo entro il campo della robotica. Egli sintetizza i due profili che caratterizzano il discorso sul rischio correlato ai prodotti robotici, notando il palesarsi di tipi diversi di rischi e l'ampliarsi del numero dei soggetti coinvolti[10].

In realtà, laddove si consideri che la robotica gioca un ruolo chiave già da decenni, e solo occasionalmente è stata oggetto di vivaci dibattiti giuridici, non si riscontrerebbero elementi di criticità. Si tratta, però, per lo più, di applicazioni industriali. La robotica avanzata, i sistemi autonomi, la complessità degli algoritmi, così come le emergenti tecnologie digitali dell'Internet of Things (IoT), conducono alla creazione di prodotti e servizi che permettono nuove opportunità per la nostra economia e società. Questi prodotti creano, a loro volta, complessi *technological environments* che migliorano, significativamente, la quotidianità.

Alcuni esempi introducono i tratti caratterizzanti del cambiamento tecnologico.

Erica è il prototipo di umanoide più avanzato al mondo: dal 2018 legge il TG giapponese in prima serata.

La Volvo di Uber è il modello di macchina a guida automatizzata che ha, recentemente, causato il primo in-

the Proper Standard, in B.S. Jackson e D. Mcgoldrick, *Legal Visions of the New Europe*, London, Grahman and Trotman, 1993, pp. 293-302.

[9] B. Wynne, *Normalising Europe – And the World – Through Science: Risk, Uncertainty and Precaution*, in S. Rodotà e M. Tallacchini (a cura di), *Trattato di biodiritto. Ambito e fonti del biodiritto*, Milano, Giuffrè, 2010, p. 491.

[10] Così R. Schulze, *Münster Colloquia on EU Law and the Digital Economy. Liability for Robotics and in the Internet of Things*, presso Westfalische Wilhelms, Universitat Münster, Germany, 12-13 aprile 2018.

cidente mortale[11], circolando a Tempe in Arizona, dove i test di questo tipo di veicoli sono già autorizzati su strada pubblica[12].

E ancora si pensi al c.d. *eyeborg*, un «dispositivo» robotico simile a un'antenna, impiantato, in maniera permanente, nel cervello dell'inglese Neil Harbisson. Il dispositivo funziona come una telecamera e permette di ovviare al difetto visivo dell'acromatopia, convertendo i colori in onde sonore. Il signor Harbisson è il primo *cyborg* al mondo, riconosciuto dal governo britannico nel 2004.

Artefatto, veicolo, dispositivo, tre tipologie di applicazioni robotiche che introducono nuove variabili nei potenziali rischi correlati ai prodotti. E così, il tema della sicurezza dei prodotti assume tratti multidimensionali. Nella prospettiva della riflessione biogiuridica, la questione della sicurezza implica la considerazione del corpo come un «nuovo oggetto connesso» presentato, addirittura, come una «nano-bio-info-neuro-machine», per via dell'effetto del convergere delle quattro «province» della tecnoscienza. Emerge una nuova dimensione dell'umano[13].

Mutuando, metaforicamente, un termine dalla biologia, tra uomo e macchina (robotica) si crea, in molte circostanze, una relazione simbiotica, dai tratti ancora, per lo più, imprevedibili[14]: applicazioni come esoscheletri e protesi robotiche (*bionics*), le quali, collegate agli stimoli cerebrali

[11] L'incidente è accaduto a Tempe, Arizona, lo scorso 18 marzo 2018. Cfr. The Guardian, *Self-driving Uber Kills Arizona Woman in First Fatal Crash Involving Pedestrian*, 19 marzo 2018, consultabile all'indirizzo https://www.theguardian.com/technology/2018/mar/19/uber-self-driving-car-kills-woman-arizona-tempe.

[12] Self-Driving Vehicle Oversight Committee, Executive Order 2015-09, Self-Driving Vehicle Testing and Piloting in the State of Arizona, consultabile all'indirizzo http://azmemory.azlibrary.gov/digital/collection/execorders/id/752/.

[13] Così S. Rodotà, *Dall'umano al postumano*, in Id., *Vivere la democrazia*, Roma-Bari, Laterza, 2018, p. 133.

[14] Per una prospettiva giuridica si rinvia ad autorevole dottrina: S. Rodotà, *Tecnologie e diritti*, Bologna, Il Mulino, 1995. In psicologia: L. Gamberini e A. Spagnolli, *Towards a Definition of Symbiotic Relations between Humans and Machines*, in AA.VV., *Symbiotic Interaction*, Cham, Springer, 2017, pp. 1-4.

del soggetto ricevente, consentono di recuperare capacità fisiche perdute o di colmare specifici deficit biologici, promettono di rivoluzionare la dimensione fisica e culturale della corporeità umana.

Qualcuna di esse configura forme di «potenziamento» delle capacità dell'essere umano (c.d. *human enhancement*) che, oltre a costituire uno dei più controversi, e ambivalenti, temi nell'ambito della moderna biomedicina[15], (ri)mette in discussione la dimensione antropologica umana e l'impianto normativo posto a tutela dei diritti fondamentali dell'uomo.

Quando, invece, la robotica prende le forme dell'umanoide, la sicurezza del prodotto richiede un'analisi nella prospettiva della *human-robot interaction* (H-R interazione). Il robot c.d. sociale, o collaborativo (c.d. *cobot*), interagendo con l'uomo potrebbe generare effetti di illusione empatica, aumentando «il grave impatto emotivo e fisico che un tale attaccamento potrebbe avere sugli uomini»[16]. Ciò indurrebbe la società, e in particolare i gruppi più vulnerabili, a non differenziare ciò che è reale e autentico, da ciò che è illusorio[17].

La *self-driving car* esemplifica, invece, l'interdipendenza tra le condizioni ambientali e il funzionamento del prodotto quando sono impiegati i più avanzati algoritmi di machine learning. L'interconnessione, poi, incrementa, esponenzialmente, il numero delle questioni che si vanno profilando.

Tutti questi esempi delineano la natura multi-dimensionale della questione sicurezza relativa a un prodotto robo-

[15] In tal senso, D. Birnbacher, *L'ambivalenza etica dell'enhancement*, Roma, Edizioni Panorama della Sanità, 2014, pp. 27-42.

[16] Art. 3 della Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, 2015/2103(Inl).

[17] K. Darling, *Extending Legal Protection to Social Robots: The Effects of Anthropomorphism, Empathy, and Violent Behavior Towards Robotic Objects*, 23 aprile 2012, paper consultabile all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2044797. R. Calo, A.M. Froomkin e I. Kerr (a cura di), *Robot Law*, Cheltenham, Edward Elgar, 2016; *We Robot Conference 2012*, University of Miami, April 23, 2012, consultabile all'indirizzo https://ssrn.com/abstract=2044797 o http://dx.doi.org/10.2139/ssrn.2044797.

tico, la cui conoscenza dipende dalle specificità correlate: tecnologia (tipo di tecnologia, grado di innovazione, luogo e tempo); regolamentazione (tipo di regolazione, approccio normativo e conoscenza) e ricerca (disciplina, definizione e inquadramento del problema).

Il principale contesto geopolitico di riferimento dell'analisi è quello europeo. Due tratti centrali della policy europea sono di sicuro impatto. Il primo consiste nel promuovere lo sviluppo responsabile del progresso tecnoscientifico, principio ispiratore della governance delle tecnologie convergenti, che si è evoluto nella *responsible research and innovation* (Rri) policy: così efficacemente formulata, ma non (ancora) altrettanto efficacemente ancorata a parametri tecnico-giuridici, ha sicuramente il pregio di aver tratteggiato la linea di sviluppo nel promuovere ciò che è socialmente desiderabile, eticamente compatibile, e sostenibile, integrando tali valori fin dalle prime fasi di sviluppo della regolamentazione[18].

Il secondo tratto risiede nella costruzione di una *European data economy*, quale parte del *digital single market*. Parlare di economia digitale non significa parlare di un'economia a sé, o di uno specifico settore dell'economia. Piuttosto, i cambiamenti dovuti alla digitalizzazione conducono l'intera economia a diventare digitale[19]. Questa nuova realtà, basata

[18] Cfr. European Commission, *Options for Strengthening Responsible Research and Innovation*, Luxemburg, 2013. Parallelamente, gli studi in materia di regolamentazione del rischio nelle diverse politiche europee indicano che l'analisi debba andare oltre quella delle più ristrette nozioni di rischio e sicurezza per discutere lo scopo sociale dell'innovazione tecnologica e il contesto culturale entro il quale il cambiamento tecnologico prende forma. «The risk discourse is as complex and multifaceted as other inter- and transdisciplinary discourses of our time, which deal with terms and concepts that are in some way perceived to fundamentally reflect current changes of paradigms across modern western societies (such as for instance the terms "globalization", "governance" or "digitalization")». Così si legge in M. Weimer, *The Origins of «Risk» as an Idea and the Future of Risk Regulation*, in *European Journal of Risk Regulation*, 8, 1, 2017, pp. 10-17, spec. p. 11.

[19] Così notano S. Lohsse, R. Schulze e D. Staudenmayer, *Trading Data in the Digital Economy: Legal Concepts and Tools*, in Idd. (a cura di), *Trading Data in the Digital Economy: Legal Concepts and Tools. Münster*

sull'emergere di big data, si concretizza nello sviluppo di nuove ed emergenti tecnologie e servizi – *data-based products and services* – inclusi *cloud computing*, *blockchain* e prodotti che impiegano l'AI, i quali nel loro insieme si basano sul nuovo «ecosistema», già comunemente identificato con l'espressione di IoT. Ciò permette alle differenti applicazioni dei sistemi autonomi (robot) di connettersi, con importanti ricadute in punto di sicurezza e responsabilità.

La trasformazione in atto enfatizza il ruolo dell'Unione europea nel salvaguardare i valori della società, la struttura del mercato e dei sistemi politici, per incentivare le potenzialità dell'economia europea. Entro questo quadro, l'esigenza di garantire la sicurezza dei prodotti è tra gli obiettivi di primaria importanza: con essa i consumatori beneficiano di questi prodotti, evitando che nuove tipologie di rischi rimangano senza un'adeguata risposta.

2. *Il cambiamento tecnologico. La robotica*

Pare, preliminarmente, importante distinguere la nuova tecnologia dal più ampio concetto di cambiamento tecnologico. Tale distinzione, solo recentemente esaminata dalla dottrina giuridica straniera[20], è già da tempo oggetto di analisi sociologiche[21], storiche ed economiche[22].

Colloquia on EU Law and the Digital Economy III, Baden Baden, Nomos-Hart Publishing, 2017, p. 13.

[20] L. Bennett Moses, *Why Have a Theory of Law and Technological Change*, in *Minn. J.L. Sci. & Tech.*, 8, 2007, p. 589.

[21] Esiste una vasta letteratura sociologica sui diversi significati di cambiamento sociale. Per un'analisi si rinvia a: G. Bouthoul, *Traité de sociologie*, Bruxelles, Payot, 1954; e R.A. Nisbet, *Social Change*, Oxford, Oxford University Press, 1972. La sociologia è nata come studio del mutamento sociale e culturale. Il vero mutamento di paradigma nella sociologia avviene alla fine del XX secolo con la considerazione delle sottese dinamiche socioculturali che si contrappongono e si espandono.

[22] L'economia dell'innovazione, in particolare, si è cimentata già da tempo, cfr. C. Antonelli, *Economia dell'innovazione: cambiamento tecnologico e dinamica industriale*, Bari, Laterza, 1995.

In sintesi, non esiste una definizione di nuova tecnologia, così come non vi è indirizzo di trattamento giuridico unanime, neppure nell'ambito della giurisprudenza della Corte europea per i Diritti dell'Uomo, spesso chiamata a pronunciarsi in materia di diritti umani e tecnologie[23].

Per cambiamento tecnologico si intende, generalmente, un processo dinamico e biunivoco, lungo il quale la tecnologia modella le forze politiche, sociali ed economiche, le quali, a loro volta, plasmano le relazioni umane e le società[24]: differisce dal cambiamento sociale e dalle altre trasformazioni indotte dalla conoscenza tecnologica[25]. Secondo le scienze cognitive, il modo in cui la società percepisce, accetta e sfrutta la tecnologia, oppure, al contrario, rimane riluttante a essa, è determinato da alcuni meccanismi comuni – essenzialmente il dato biologico e le informazioni culturali e sociali – i quali informano le attitudini verso i rischi e le percezioni degli stessi[26]. Conseguentemente, il processo evolutivo del diritto, indotto dal cambiamento tecnologico, è la risultante di un insieme di variabili, tra cui quelle culturali, sociali ed economiche, ma anche biologiche. Un ragionamento giuridico sulla sicurezza dei prodotti hi-tech implicherebbe, quindi, l'adozione di approcci più ampi, per tener conto della c.d. *safety culture*[27].

[23] Cfr. T. Murphy e G.O. Cuinn, *Works in Progress: New Technologies and the European Court of Human Rights*, in *Human Rights Law Review*, 10, 2010, pp. 601-638. Lo studio si basa sull'analisi di 155 casi in materia di diritti umani e tecnologie giudicati dalla Corte europea dei diritti umani. I casi sono stati reperiti attraverso il database Hudoc e delineano che la giurisprudenza della Corte è senz'altro un riferimento importante nel processo di mappatura dei contorni della *Law and Technology*, ma ancora non ha un orientamento univoco.

[24] A. Rip e R. Kemp, *Technological Change*, in S. Rayner e E.L. Malone (a cura di), *Human Choice and Climate Change. Vol. II, Resources and Technology*, Columbus, Ohio, Battelle Press, 1998, pp. 327-399.

[25] Bennett Moses, *Why Have a Theory of Law and Technological Change*, cit., p. 589.

[26] G. Ajani, D. Francavilla e B. Pasa, *Diritto comparato. Lezioni e materiali*, Torino, Giappichelli, 2018, p. 14.

[27] Attraverso il concetto di *law as culture*, la riflessione comparatistica ha introdotto un'analisi delle regole giuridiche che analizzano quali pratiche sociali incidono sul significato attuale delle regole, dei concetti,

La prospettata transizione dalla «società dell'informazione» alla «società dell'algoritmo»[28], e la recente documentazione europea dedicata alla *digital economy* fanno pensare all'AI e alle applicazioni robotiche come parte di un cambiamento tecnologico. D'altro canto, nella Comunicazione *Artificial Intelligence for Europe*[29], la Commissione europea ha individuato tre sfide principali che necessitano di essere affrontate per prepararsi al cambiamento: preparare la società, che significa, innanzitutto, sviluppare nei cittadini europei le competenze digitali fondamentali e il pensiero critico, competenze che non sembrano, attualmente, poter essere sostituite dalle macchine (creatività e management); studiare l'impatto di automazione, robotica e AI sul lavoro; infine, dedicarsi alla formazione e preparazione degli stessi esperti di AI per creare le condizioni di eccellenza.

L'assenza di una precisa terminologia, e di un lessico omogeneo, rende difficoltoso individuare l'esatto rapporto tra AI e robotica, il quale non può ridursi a un mero binomio di genere e specie. Anzi, talvolta, non sono fenomeni sovrapponibili: l'ambito della robotica non esaurisce quello dell'AI; così come esistono forme di robotica che non sono

del loro impatto e del loro ruolo nella società. Tutte queste riflessioni costituiscono, pertanto, il sostrato idoneo per riflettere su ciò che incide sul livello di sicurezza delle applicazioni robotiche o della sua effettività. M. Van Hoecke e M. Warrington, *Legal Cultures, Legal Paradigms and Legal Doctrine: Towards a New Model for Comparative Law*, in *Int'l & Comp. L.Q.*, 47, 1998, pp. 495-536. Un'analisi di questo tipo si fonda sulle *cultural families*: l'attitudine rispetto a una regola giuridica, e il modo con cui essa è incorporata nella società, sono il principale oggetto di osservazione da condurre secondo l'approccio sociologico o antropologico (spec. p. 502).

[28] Così M. Bassini, L. Liguori e O. Pollicino, *Sistemi di intelligenza artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018, pp. 333-380, spec. p. 334.

[29] EU Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Artificial Intelligence for Europe*, Bruxelles, 25 aprile 2018, Com(2018) 237 final.

riconducibili nell'alveo dell'AI[30]. Anche le ripercussioni nella riflessione etica rappresentano un ulteriore indice del cambiamento. Nel 2002 venne introdotto uno specifico filone d'indagine: la c.d. roboetica[31], per analizzare i problemi legati all'accettabilità sociale dell'innovazione tecnologica, e all'etica dei ricercatori che lavorano nel settore.

La descrizione della tecnologia oggetto di osservazione è, naturalmente, indispensabile per capire l'oggetto di studio e la «portata» del cambiamento. È bene, dunque, prendere le mosse dalle tappe principali dell'evoluzione dell'AI[32].

Il primo segnale di svolta nell'ambito degli studi corpomente avviene nel 1950, quando Alan Turing pubblica, sulla rivista *Mind*, l'articolo *Computing Machinery and Intelligence*[33]. È la primordiale idea di un'intelligenza senza corpo: un'idea di «intelligenza artificiale in senso forte» (*Strong AI*). L'espressione «intelligenza artificiale» fu coniata, in seguito, nel 1956 dal matematico John McCarthy e, da allora, scienziati e filosofi non hanno smesso di riflettere intorno alla questione della «intelligenza» delle macchine. L'idea di paragonare i neuroni artificiali a quelli umani incontrò molti ostacoli, soprattutto sul finire degli anni Sessanta,

[30] *Ibidem*, pp. 335-336.

[31] G. Veruggio, *Euron Roboethics Roadmap*, Plenary Session, *CEPE, Seventh International Computer Ethics Conference*, University of San Diego, Usa, luglio 2007, consultabile all'indirizzo http://www.roboethics.org/index_file/Roboethics%20Roadmap%20Rel.1.2.pdf; e G. Veruggio, *The Birth of Roboethics*, Relazione all'International Conference on Robotic and Automation, Barcellona, 18 aprile 2005, in *Leadership Medica*, X/2007, consultabile all'indirizzo www. leadershipmedica.it, 2007.

[32] Il deep learning è definito dalla Comunicazione della Commissione europea del 25 aprile 2018 come un «game-changer for AI with a tremendous improvement in performance for specific tasks such as image or speech recognition, or machine translation. Training a deep learning algorithm to classify objects works by exposing it to a large number of labelled examples (e.g. pictures) that are correctly categorized (e.g. pictures of planes). Once trained, algorithms can correctly classify objects that they have never seen, in some cases with accuracies that exceed those of humans. Significant advances in these technologies have been made through the use of large data sets and unprecedented computing power».

[33] A. Turing, *Computing Machinery and Intelligence*, in *Mind, New Series*, 59, 1950, p. 433.

quando Marvin Minsky e Seymour Papert evidenziarono i limiti delle prime reti neurali artificiali[34]. E per questo si passa a ragionare intorno all'idea di «intelligenza artificiale in senso debole» (*Light AI*). A partire dagli anni Novanta, la ricerca si concentra sull'«agente intelligente» come entità. Fioriscono, quindi, gli studi sui software intelligenti, e sugli agenti intelligenti «incorporati» in un sistema fisico.

La convergenza tra le ricerche incentrate sul concetto di Light AI, e quelle focalizzate sullo sviluppo di un'*automa*, ha progressivamente condotto allo sviluppo della moderna robotica. Nel 1920, il drammaturgo ceco Capek conia il termine robot, che deriva dalla radice «robota» e significa «lavoro duro, forzato» e indica un «automa», una macchina costruita dall'uomo per svolgere funzioni di lavoro in sostituzione dell'uomo[35].

Negli ultimi sessant'anni, la robotica ha fatto progressi straordinari e dal campo aerospaziale e industriale[36], dove il robot è tipicamente «confinato» in uno spazio strutturato ad accoglierlo, promette, in tempi più recenti, di invadere gli ambienti comuni. I robot collaborativi, o sociali, per aiuto domestico, o utilizzati nei reparti ospedalieri per intrattenere soggetti vulnerabili sono un esempio[37]. Così come lo è l'auto a guida automatizzata, il cui mercato potenziale è stimato, entro il 2030, in circa 44 milioni di veicoli[38].

Secondo il parere del Comitato di bioetica e del Comitato nazionale per la biosicurezza, le biotecnologie e le scienze della vita, sugli sviluppi della robotica e della roboetica[39],

[34] M. Minsky e S. Papert, *Perceptrons*, Cambridge, The MIT Press, 1969.

[35] K. Capek, *Rossum's Universal Robots*, Firenze, Pegasus, 1920.

[36] Da ultimo, nella missione Rosetta, lanciata dall'Agenzia spaziale europea, il robot Philae atterrò per la prima volta su una cometa. Cfr. http://www.esa.int/Our_Activities/Space_Science/Rosetta/.

[37] Si veda l'esempio di Pepper nel cap. II.

[38] Camera dei Deputati (Servizio Studi), *La mobilità del futuro: l'auto a guida automatica*, Dossier n. 275 – Schede di lettura, 31 gennaio 2017, consultabile all'indirizzo http://documenti.camera.it/Leg17/Dossier/pdf/TR0391.pdf.

[39] Parere del 17 luglio 2017, proposto dal Cnb e dal Cnbbsv. Il parere propone la seguente distinzione: i robot senza corpo e quelli con

un elemento centrale da chiarire entro la riflessione etica e giuridica è la distinzione tra «corpo» (robot) e «cervello» (AI) e, al tempo stesso, la loro interconnessione (corpo e cervello non si possono separare, perché non è né il corpo né il cervello a dominare, ma è fondamentale il nesso, l'orchestrazione tra i due). I robot che hanno un corpo (*with body*), vanno distinti da quelli che non ce l'hanno (*without body*). Avere un corpo significa essere in grado di attuare dei movimenti, cioè di produrre lavoro fisico, a differenza di un computer che ha un corpo, ma è immobile. La possibilità di incorporare (*embeddedness*) l'AI nell'ambiente e nell'uomo forma una «invisibile infrastruttura tecnologica» per l'azione umana e crea un ambiente artificiale capace di modificare radicalmente la percezione e l'autopercezione dei soggetti[40]. Numerose sono le carte dei valori etici elaborate proprio al fine di orientare l'operato di ingegneri e informatici per incorporare in maniera responsabile e uniforme determinati valori fondamentali negli algoritmi quali, ad esempio, la tutela della riservatezza, la dignità, la giustizia e la trasparenza[41].

La varietà dei modi attraverso i quali la robotica si combina con altre tecnologie e crea servizi e prodotti, e i molteplici usi del termine rendono difficile individuare una definizione di robot condivisa. Richards e Smart definiscono il robot come «a constructed system that displays both physical and mental agency, but is not a live in the biological sense»[42].

Generalmente, si predilige una definizione ampia, per includervi molte applicazioni, estremamente diverse tra loro.

il corpo: entrambi possono essere «stupidi» o «intelligenti», cioè non dotati o dotati di «capacità cognitive». I primi hanno sempre bisogno dell'intervento umano per essere programmati. I secondi agiscono indipendentemente dall'input umano.

[40] S. Arnaldi, *L'immaginazione creatrice*, Bologna, Il Mulino, 2010.

[41] Tra le principali Carte dei valori etici spicca la Carta della Robotica, introdotta dalla Risoluzione del 16 febbraio 2017. Il testo è allegato alla Risoluzione.

[42] N. Richards e W. Smart, *How Should the Law Think about Robots?*, in R. Calo, A.M. Froomkin e I. Kerr, *Robot Law*, Cheltenham, Edward Elgar, 2016, pp. 3-22.

Seguendo le indicazioni tracciate dal pionieristico progetto pisano di Robolaw[43], è utile ricordare cinque caratteristiche identificative di un robot:

1. La natura: si riferisce a come un robot si manifesta, se sia *embedded* in un corpo, oppure no (es. *softbots*).

2. L'autonomia: non vi è una classificazione generale condivisa dei livelli di autonomia del robot, alcuni distinguono «l'autonomia forte» dall'«autonomia debole»[44]; altri distinguono i robot non autonomi, semi-autonomi da quelli completamente autonomi.

3. La funzione: si riferisce all'applicazione o al servizio fornito dal robot.

4. L'ambiente operativo: si riferisce al contesto d'utilizzo.

5. L'interazione uomo-robot: si riferisce al tipo e alla pervasività di relazione.

Non si tratta, in ogni caso, di un elenco esclusivo, poiché ci sono altre importanti caratteristiche che vengono in rilievo, come ad esempio, la capacità di eseguire un programma (software), per svolgere specifiche funzioni e, soprattutto, la complessità del programma stesso.

Sebbene la capacità di apprendimento automatico sia attualmente ancora, per lo più, in fase di sviluppo, e limitata a pochi e specifici settori, è bene dar conto di alcune distinzioni che si profilano importanti per l'impatto che potrebbero avere sulle regole di responsabilità. Sono in fase di studio diversi gradi di autoapprendimento: il machine learning e deep learning. Con il machine learning il computer (che potrebbe essere incorporato nei robot) impara dall'esperienza, o tecnicamente da un training[45]. In sostanza, gli algoritmi di machine learning usano metodi matematico-computazionali per apprendere informazioni

[43] Cfr. http://www.robolaw.eu.

[44] U. Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts*, Dordrecht, Springer, 2015.

[45] Intervista a Mauro Conti (professore di Informatica), Head of the Security and Privacy Research Group (Spritz), Director of UniPD node of Cini Cybersecurity National Lab, Università di Padova, 14 febbraio 2018. Per una lettura in materia si rinvia a I. Goodfellow, Y. Bengio e A. Courville, *Deep Learning*, Cambridge, The MIT Press, 2016.

direttamente dai dati, senza modelli matematici ed equazioni predeterminate. Gli algoritmi della machine learning migliorano le loro prestazioni in modo «adattativo», rispetto agli «esempi» da cui apprende. Si ritiene, generalmente, che la capacità di autoapprendimento possa seguire due diversi tratti distintivi: *i*) la «consapevolezza» dell'azione, simile alla volontà che in filosofia è caratteristica essenziale dell'agente morale; *ii*) l'abilità di interagire consapevolmente nel contesto operativo[46]. In un futuro, ancora lontano, il deep learning realizzerà un grado ancor più avanzato di apprendimento della macchina, poiché gli algoritmi permettono al software di apprendere come disegnare funzioni complesse, quali parlare e riconoscere immagini.

La capacità di autoapprendimento del machine learning può essere potenziata dal fenomeno della connessione tra robot, simile a quello che caratterizza l'intelligenza ambientale: i robot condividono intelligenza e capacità di calcolo in un grande repository centrale (il cloud) accessibile velocemente[47]. La connettività tra robot presenta nuovi problemi sia etici che giuridici. I diversi livelli di autonomia e la capacità di autoapprendimento sono caratteristiche essenziali che impattano in maniera rilevante sulla valutazione della sicurezza e sui profili di responsabilità. Entrambi verranno ripresi e discussi più approfonditamente nel capitolo II.

3. *«Research question» e «caveat»*

Il presente studio propone una riflessione sul poliedrico tema della sicurezza dei prodotti robotici, entro le diverse

[46] M. Gutman, B. Rathgeberg e T. Syed, *Action and Autonomy: A Hidden Dilemma in Artificial Autonomous Systems*, in M. Decker e M. Gutman (a cura di), *Robo- and Informationethics. Some Fundamentals*, Münster, Verlag, 2012, p. 231.

[47] R. Cingolani e G. Metta, *Umani e umanoidi. Vivere con i robot*, Bologna, Il Mulino, 2015, p. 31. Gli autori sottolineano che questa strategia sarà utile almeno finché non si sarà in grado di costruire sistemi computazionali più simili a quelli biologici.

prospettive di governance[48], di regolamentazione europea, e della responsabilità civile, per cogliere le linee evolutive degli adattamenti giuridici che si profilano necessari.

Ulteriore scopo sottotraccia del lavoro è, altresì, quello di far emergere se tali adattamenti riguardino anche il modo di fare ricerca giuridica, quando si ambisce ad analizzare aspetti relativi al cambiamento tecnologico.

Sono necessarie alcune precisazioni per delimitare l'oggetto e l'obiettivo d'analisi.

Innanzitutto, le applicazioni robotiche sono numerosissime, talmente diverse per funzione, utilizzo e forma, da dar luogo a una varietà di problemi giuridici, anche in punto di sicurezza[49], difficilmente riconducibili a unità. D'altro canto, appare inopportuno in conformità a quanto già osservato dalla dottrina italiana, configurare un corpo unitario di regole dedicato alla robotica[50]. Nessuna *law of the horse*, per riprendere l'espressione che ha identificato lo scontro intellettuale tra Easterbrook e Lessig: il primo, in apertura a un convegno, assimilava, provocatoriamente,

[48] L'origine del termine governance va rintracciato nelle attività intraprese dalle autorità politiche nel tentativo di modellare le strutture e i processi socio-economici. Sulle origini e sui diversi modi di intendere i significati del termine si rinvia a R. Mayntz, *La teoria della governance: sfide e prospettive*, in *Rivista italiana di scienza politica*, 29, 1999, pp. 3-22.

[49] Per una mappatura dei temi, in ambito civilistico, si rinvia a E. Palmerini, *Robotica e diritto: suggestioni, intersezioni, sviluppi a margine di una ricerca europea*, in *Resp. civ. e prev.*, 6, 2016, pp. 1816-1850.

[50] *Contra* R. Calo, *Robotics and the Lessons of Cyberlaw*, in *Cal. L. Rev.*, 103, 2015, pp. 513-532; A. Sandberg, *Law-abiding Robots?*, in *Oxford Martin Opinion*, 15 luglio 2016, consultabile all'indirizzo https://www.oxfordmartin.ox.ac.uk/opinion/view/340; G. Miller, *A Brief History of Robot Law*, in *Atlantic*, 17 marzo 2016, consultabile all'indirizzo http://www.theatlantic.com/technology/archive/2016/03/a-brief-history-of-robot-law/474156/. C'è anche chi configura la *Lex Robotica* similmente alla configurazione della *Lex Mercatoria*. Cfr. E. Stradella, *Approaches for Regulating Robotic Technologies: Lessons Learned and Concluding Remarks*, in E. Palmerini e E. Stradella, *Law and Technology. The Challenge of Regulating Technological Development*, Pisa, Pisa University Press, 2013, p. 345.

la *cyberlaw* a un diritto dei cavalli per indicarne l'inutilità[51]; mentre il secondo offrì, successivamente, la prospettiva opposta[52]. Chi scrive predilige, invece, un atteggiamento di c.d. «eccezionalismo» moderato[53]: le caratteristiche funzionali della nuova tecnologia, pur prive di precedenti, non sono di per sé sufficienti a introdurre eccezioni all'operatività delle regole e degli istituti civilistici tradizionali. Quest'ultima rimane una soluzione estrema[54].

La frammentarietà regolatoria in punto di sicurezza si coglie, immediatamente, pensando alle poche, diverse, applicazioni robotiche: la *driveless car technology*; le protesi robotiche, i macchinari industriali. Tutti prodotti che rientrano, per natura, nelle discipline legislative di settore, con precisi e diversi standard a cui riferirsi.

La trattazione unitaria, in questa sede, ha l'intento di offrire un quadro di riferimento entro il quale muovere i primi passi per individuare le diverse dimensioni del problema, intendendo, dunque, dare un'immagine unica alle molte sfaccettature che la caratterizzano. Molto, infatti, dipenderà dal tipo di robot considerato, dalle sue caratteristiche, dal livello di autonomia, dal contesto operativo, interazione

[51] F. Easterbrook, *Cyberspace and the Law of the Horse*, in *U. Chi. Legal F.*, 207, 1996, pp. 207-216.

[52] L. Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, in *Harv. L. Rev.*, 113, 1999, p. 501. Nel contesto specifico della robotica, per esempio, vi è chi ravvisa un assetto di caratteristiche essenziali diverse da internet e da altre tecnologie convergenti. L'assetto sarebbe tale da legittimare un diritto *ad hoc* per la stessa. Si pensi al modo in cui, in quest'ambito, si combinano scambio di informazioni (soprattutto nel caso di «connessione di robots») e potenziali danni fisici. R. Calo, *Robotics and the Lessons of Cyberlaw*, in *California Law Review*, 103, 2015, pp. 514-563.

[53] Cfr. L. Bennett Moses, *Adapting the Law to Technological Change: A Comparison of Common Law and Legislation*, in *UNSWLJ*, 26, 2003, p. 394; C. Tapper, *Judicial Attitudes, Aptitudes and Abilities in the Field of High Technology*, in *Monash ULR*, 15, 1989, p. 219.

[54] Aderisco a quella parte consistente della dottrina che nega la necessità di adottare una nuova regolazione *ad hoc* ogniqualvolta si sia di fronte a un cambiamento tecnologico. Al contrario, sulla necessità di rivedere le categorie giuridiche tradizionali si rinvia a N. Lipari, *Le categorie del diritto civile*, Milano, Giuffrè, 2013, pp. 11 ss.

con l'uomo o incorporazione nello stesso, o dalle capacità di interconnessione.

Ultima precisazione. Considero, quale premessa, le applicazioni robotiche alla stregua di prodotti. L'uso del termine «artefatti» nel titolo è motivato da una duplice consapevolezza: i ritrovati più evoluti dei sistemi autonomi (anche connessi), hanno fatto ipotizzare l'attribuzione di una diversa natura giuridica (*infra* cap. II); l'incertezza su tale natura giuridica e le caratteristiche funzionali, in tali casi, sembrano far sfumare la distinzione prodotto/servizio.

Gli esempi di applicazioni prese in considerazione nel volume appartengono, per lo più, all'ambito biomedicale, ai veicoli automatizzati, e al «mondo» degli umanoidi.

4. *Cambiamento tecnologico, «adattamento» giuridico… e metodi di ricerca*

Tre caratteristiche endemiche della robotica guidano alla scelta di altrettante prospettive d'analisi. Esse sono:

1. *la transnazionalità*. La transnazionalità è uno dei modi di essere del rapporto diritto, scienza e nuove tecnologie[55]. L'analisi della sicurezza dei prodotti in questione non può prescindere dai mutamenti in corso nelle tecniche sovranazionali di governance della tecnoscienza, e dal pacchetto di documenti europei che, a partire dal 2014, e con incredibile intensità tra il 2017 e il 2018, stanno mutando, in maniera determinante, le «coordinate» normative dello studio del tema;

2. *inclusione di conoscenze e metodi di indagine provenienti da discipline non giuridiche*. La convergenza tecnologica fa confluire i saperi scientifici e quelli provenienti dalle scienze sociali e umanistiche, mettendo in relazione concetti propri del diritto e di altre discipline. Per questo, i cambiamenti tecnologici richiedono l'adozione di un approccio

[55] A. Santosuosso, *Diritto, scienza e nuove tecnologie*, Padova, Cedam, 2016, p. 9.

«olistico» allo studio. La robotica è ambito interdisciplinare per eccellenza. Essa, per esempio, intrattiene un duplice legame con lo sviluppo delle neuroscienze e delle scienze cognitive. Da una parte, il progresso nella comprensione delle basi neurali e cognitive del comportamento dei sistemi viventi ha, spesso, stimolato lo sviluppo di sistemi robotici efficienti e in grado di operare in contesti ambientali relativamente poco strutturati. Dall'altra, in molti casi, la costruzione di robot ha fornito contributi significativi al progresso delle neuroscienze e delle scienze della mente (si veda il caso delle reti neurali). Nel corso dell'ultima decade, un contributo importante è fornito da un nucleo significativo di ricerche in diverse discipline, incluse quelle ingegneristiche, informatiche, studi sull'interazione computer-uomo (Hci, *human computer interaction*), sull'interazione uomo-robot (Hri, *human-robot interaction*), *science and technology studies* (Sts), e filosofia della tecnologia.

È necessario, dunque, favorire analisi interdisciplinari[56], e non solo multidisciplinari, per lo studio di temi tecnoscientifici, sebbene come integrare le conoscenze, in quale grado, con quali metodi siano problemi ancora aperti[57]. Negli anni più recenti, la comparazione ha fornito un apporto importante, essendo essa stessa intrinsecamente interdisciplinare[58]. È un metodo che accomuna tutte le scienze sociali, ed è in grado di creare, pertanto, un'interconnessione tra le ricerche

[56] Attribuendo al termine il significato più autentico, spiegato nel seguito di questo paragrafo, questo tipo di ricerca potrebbe essere realizzato solo disponendo dell'apporto di più esperti, appartenenti a diverse discipline.

[57] L'apporto del diritto comparato in materia è fondamentale. Si pensi alla nascita di corsi «Diritto& …» (diritto&genere; diritto&letteratura; diritto&tecnologie; diritto&musica ecc.) avvenuta all'interno di tale settore disciplinare.

[58] Il diritto è il prodotto della storia, della cultura, del linguaggio ecc. Tra i tanti, vedi M.A. Glendon, P. Carozza e C.B. Picker, *Comparative Legal Tradition in a Nutshell*, St. Paul, West Academic Publishing, 2008; U. Mattei, *An Opportunity Not to Be Missed: The Future of Comparative Law in the United States*, in *American Journal of Comparative Law*, 46, 1998, pp. 709-718.

affrontate in varie discipline, come la sociologia, l'antropologia, la psicologia, l'economia e la politica[59].

Questo ruolo appare fondamentale quando l'oggetto di indagine è tecnoscientifico, laddove «il rapporto tra paradigma giuridico e paradigma scientifico rivela la tensione verso una comprensione più larga dei fenomeni che esige la padronanza di strumenti disciplinari diversi e che ha anche la funzione di integrare il diritto in un contesto culturale più ampio»[60].

Diviene necessario differenziare i diversi gradi di integrazione dei saperi, distinguendo, pertanto, l'autentica e più profonda integrazione di disciplina – l'interdisciplinarità – dal più semplice accostamento delle stesse – c.d. multidisciplinarità[61]. Il contributo più recente degli studi comparatistici propone una tassonomia della ricerca giuridica che differenzia i tipi di *research question*, distinguendo quella tradizionale, di natura squisitamente giuridica, da quelle interdisciplinari, avendo cura, però, di indicare entro questo secondo tipo, diversi livelli di integrazione delle conoscenze, a seconda che essa si basi sulla formulazione

[59] M. Siems, *Comparative Law*, Cambridge, Cambridge University Press, 2014. Il concetto di *implicit comparative law* si basa fondamentalmente sull'idea che il metodo comparatistico è applicabile a tutte le scienze sociali.

[60] S. Rodotà, *Diritto, scienza, tecnologia: modelli e scelte di regolamentazione*, in *Riv. cri. dir. priv.*, 2004, p. 357. È stato notato anche che «nel campo delle scienze umane l'analisi comparativa svolge una funzione di sostituzione dell'analisi "sperimentale" che caratterizza le scienze naturali» Così Ajani, Francavilla e Pasa, *Diritto comparato*, cit., p. 5.

[61] Spesso il termine interdisciplinarità è usato in maniera a-tecnica per indicare, indifferentemente, diversi approcci e gradi di integrazione tra discipline. Ciò dipende dal fatto che non vi è uniformità di indirizzo nell'impiego dei prefissi «multi-», «inter-», «trans» e «cross-disciplinarità». In realtà, a seconda della connessione tra le stesse, dei metodi di lavoro, del risultato e della diffusione degli stessi, si distinguono studi multidisciplinari e transnazionali. Cfr. *American Heritage Dictionary of the English Language*, Boston, Houghton Mifflin Harcourt, 2000. Per una trattazione di questo specifico tema ci si permette di rinviare a G. Guerra, *An Interdisciplinary Approach for Comparative Lawyers: Insights from the Fast Moving Field of Law and Technology*, in *German Law Journal*, 3, 2018, pp. 580-612.

di un quesito di natura non solo giuridica (tipo 1); o più avanzate, se incorporano metodi di analisi non tipici delle scienze giuridiche, come ad esempio il metodo quantistico (tipo 2); o entrambi i profili, cioè quesito misto e metodi di indagine non solo giuridici (tipo 3)[62].

Nell'economia di queste pagine, ed entro i limiti della mia preparazione classica di giurista, mi accosto allo studio del tema in esame, con un approccio che possa, quanto meno, beneficiare di spunti multidisciplinari. È una necessità dettata dall'oggetto di osservazione. Ho cercato, infatti, prima di tutto, di capire le caratteristiche dei prodotti robotici e delle loro funzioni, così diverse a seconda del settore. Per fare questo, ho sviluppato un dialogo con esperti di varie discipline, *in primis* informatici e ingegneri.

Dal punto di vista operativo, ho integrato gli spunti ricevuti attraverso lo strumento delle interviste. Sebbene non sia strumento diffuso nelle ricerche giuridiche, l'intervista è impiegata nelle scienze sociali (sociologia, antropologia, psicologia ecc.)[63], tanto da poter sembrare un segno identificativo della riconciliazione fra gli studi comparatistici e i *socio-legal studies*, in conformità a quanto enfatizza la più recente riflessione sul metodo comparatistico[64]. Si tratta di

[62] M. Siems, *The Taxonomy of Interdisciplinary Legal Research: Finding the Way Out of the Desert*, in *Journal of Commonwealth Law and Legal Education*, 2009, pp. 5-17.

[63] R. Fideli e A. Marradi, *Intervista*, in *Enciclopedia delle Scienze Sociali*, Roma, Istituto della Enciclopedia Italiana, V, 1996, pp. 71-82. D'altro canto, si consideri che «la molteplicità degli approcci metodologici, sia qualitativi che quantitativi, rappresenta un punto di incontro, e un'occasione di collaborazione, fra studiosi appartenenti ad aree disciplinari e a tradizioni giuridiche diverse». R. Scarciglia, *Strutturalismo, formanti legali e diritto pubblico comparato*, in *Dir. Publ. Comp. ed Eu.*, 2017, pp. 649-667, spec. p. 650. L'autore parla del «mare della comparazione» per esprimere la pluralità di indagini di diversa natura che questa stessa disciplina ricomprende. Sull'adeguamento dei tradizionali metodi di ricerca delle scienze sociali, incluse quelle a carattere giuridico-comparatistico, alle trasformazioni della realtà globale, si veda F. Viglione, *I «confini» nel diritto privato comparato*, in *NGCC*, 2011, pp. 162 ss., spec. p. 164.

[64] Cfr. A. Riles, *Comparative Law and Socio-legal Studies*, in M. Reimann e R. Zimmermann (a cura di), *The Oxford Handbook of Comparative Law*, Oxford-New York, Oxford University Press, 2012, p. 777.

un «tassello» del lavoro che ha reso possibile un processo di apprendimento più dinamico delle complessità legate al cambiamento tecnologico[65].

3. Elementi di diritto, regolamentazione e tecnologia[66]. Un ruolo particolarmente importante nell'analisi del tema è assunto dall'emergente campo di studi dedicato al rapporto tra diritto, regolamentazione e tecnologia.

L'utilizzo di una «lente» di osservazione quale, ad esempio, quella fornita dalle tecniche di *techno-regulation* introduce nuovi strumenti per comprendere un problema, quello della sicurezza dei prodotti, che con riferimento alla robotica necessita di essere analizzata da varie angolature.

Se, per esempio, si pensa non solo in termini di regolamentazione *della* tecnologia, ma anche in termini di regolamentazione *attraverso* la tecnologia[67], i robot diventano sia oggetto della regolazione, sia protagonisti, con evidenti implicazioni sotto il profilo della sicurezza.

5. *Struttura del lavoro*

L'obiettivo di indagare la sicurezza dei prodotti robotici si sviluppa a più livelli. D'altro canto, quando un problema è complesso, il modo di affrontarlo

> dipende dalla sensibilità del ricercatore. Gli scenari che si aprono al comparatista sono diversi ove egli consideri […] i fattori iniziali su cui si basa la sua analisi e sulla base di questi costruisca degli insiemi sempre più piccoli, come, ad esempio, possiamo vedere

[65] Si è trattato di interviste qualitative condotte da me personalmente attraverso colloqui, con strumenti poco standardizzati e tracce di domande volte, per lo più, a cogliere i tratti peculiari del cambiamento tecnologico.

[66] Il significato dell'espressione *technology regulation* è solo in parte coincidente con quello di «regolamentazione della tecnologia», perché si riferisce, in senso lato, a un settore di studi promosso in Europa per lo più da studiosi del King College (London) e di Tilburg (The Netherlands).

[67] Distinzione introdotta da R. Brownsword e K. Yeung, *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Portland, Hart Publishing, 2008, p. 3.

nella classica descrizione di un frattale – elemento geometrico costituito da linee spezzate – attraverso la curva di Koch[68].

Ispirando la struttura del lavoro a questa stessa forma geometrica, ho considerato tre prospettive di analisi.

Nella prima (cap. I, par. 1) ho contestualizzato la questione della sicurezza dei prodotti robotici entro i modelli di governance europea applicati alle nuove tecnologie. Ciò al fine di cogliere i tratti essenziali che concretizzano gli obiettivi della strategia di *responsible research and innovation*[69], con specifico riguardo al ruolo attribuito alla tecnica del *by design*, e in particolare del *safe by design* (sicuro fin dalla progettazione).

Con la seconda parte (cap. I, parr. 2 e ss.), ho inquadrato la robotica entro il diritto europeo: dapprima, ripercorrendo i tratti essenziali della recente policy europea in materia di *digital economy* e AI, con particolare riguardo a quei documenti dedicati ai profili di sicurezza dei prodotti associati all'IoT e alla responsabilità per le emergenti tecnologie digitali; poi, con riferimento ai documenti più specifici dedicati alla robotica ho considerato le prime, e già ampliamente criticate, indicazioni del Parlamento europeo, e i riferimenti legislativi orizzontali e verticali in materia di sicurezza applicabili ai prodotti robotici[70].

Infine (cap. II), ho analizzato il tema entro il sistema coordinato della regolamentazione *ex ante* di sicurezza dei prodotti con quello *ex post* della responsabilità civile del

[68] R. Scarciglia, *Metodi e comparazione giuridica*, Padova, Cedam, 2016, p. 7.

[69] Sono stati fatti molti tentativi per ancorare il concetto di Rri a parametri specifici e concreti. I progetti, nati per lo più nell'ambito degli studi dei diritti umani, permettono di predisporre un sistema di regole sufficientemente flessibile ad accogliere le specificità delle nuove tecnologie.

[70] Si rinvia al cap. I, parr. 4 e 4.1 per i riferimenti a carattere orizzontale; e al cap. I, par. 5 per i riferimenti c.d. verticali, e cioè nelle discipline di settore applicabili.

fabbricante[71]. Il caso delle macchine *self-driving* è stato oggetto di trattazione specifica.

[71] La letteratura civilistica italiana è ricchissima di analisi in materia. Per una ricostruzione completa e recente si rinvia a E. Al Mureden, *La sicurezza dei prodotti e la responsabilità del produttore*, Torino, Giappichelli, 2017.

Capitolo primo

LA SICUREZZA DELLA ROBOTICA NEL QUADRO GIURIDICO EUROPEO DELLE TECNOLOGIE EMERGENTI

1. *Il passaggio da «risk-governance» a «innovation-governance» delle tecnologie convergenti in Europa*

Contenendo questa riflessione iniziale entro i limiti funzionali allo sviluppo del piano di indagine, pare utile ripercorrere, brevemente, la policy dell'Unione dell'Innovazione *responsible research and innovation* (Rri) *policy*, nonché l'evoluzione delle forme di regolazione della tecnologia. Quest'ultimo passaggio al fine di contestualizzare l'impiego di una tecnica, in particolare: il *by design*, declinato nello specifico ambito di applicazione della sicurezza (*safe by design*). Si tratta di strategie e tecniche che incidono, in ultima analisi, sul modo di garantire un elevato livello di tutela dei consumatori, sancito dalla Carta dei diritti fondamentali dell'Unione europea e nell'art. 169 Tfue.

Le questioni di governance poste dalla robotica sembrano, almeno a una prima analisi, analoghe a quelle che, in un passato recente, hanno caratterizzato le biotecnologie, le nanotecnologie, le tecnologie informatiche e le applicazioni derivanti dalle scienze cognitive[1]. Tutte hanno indotto il giurista a riflettere sul problema dell'obsolescenza delle regole giuridiche, a fronte della rapidità con la quale le tecnologie mutano l'oggetto sul quale si basa il framework giuridico in vigore. Tale fenomeno è nominato in vari modi: per Marchant è il *pacing problem*[2]; Brownsword si riferisce,

[1] Sul significato del termine governance vedi *retro* nota 48 p. 23. Si rinvia inoltre a D. Ruggiu, *Human Rights and Emerging Technologies. Analysis and Perspectives in Europe*, Singapore, Pan Standford Publishing, 2018.

[2] G.E. Marchant, B.R. Allenby e J.R Heckert, *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem*, Netherlands, Springer, 2011.

invece, alla c.d. *regulatory disconnection*[3]. Con riferimento alla robotica, la discontinuità nell'applicazione della regolamentazione si verifica, per esempio, tutte le volte in cui lo schema regolatorio, basandosi su standard minimi e prestabiliti di sicurezza, non è idoneo ad includere i nuovi profili di rischio emergenti dall'affidabilità del robot.

L'incorporazione nell'essere umano di una protesi robotica (es. esoscheletri robotici, ma anche impianti cocleari, o retinali, ossia l'orecchio e l'occhio artificiali) è uno degli esempi più chiari: sul piano della sicurezza dei prodotti, l'interazione con il sistema nervoso, non ugualmente riscontrabile in altri dispositivi, intuitivamente comporta una ridiscussione degli standard di sicurezza *premarket* dei dispositivi; mentre, invece, con riferimento alla tutela dei diritti umani e delle garanzie costituzionali delle persone con disabilità, i nodi tematici si sviluppano intorno al dibattito sul potenziamento umano[4].

In generale, la crescita del mercato dei prodotti robotici i quali combinano software, hardware, sensori e, da ultimo,

[3] R. Brownsword, *Rights, Regulation and the Technological Revolution*, Oxford, Oxford University Press, 2008. Per un approfondimento sul significato di *regulatory connection* e delle circostanze che determinano l'opposta situazione di *regulatory disconnection* (discontinuità regolatoria) si rinvia a R. Brownsword e M. Goodwing, *Law and the Technologies of the Twenty-first Century*, Cambridge, Cambridge Press University, 2012, pp. 63 ss. Pare interessante notare che tra le cause che inducono la *disconnection*, gli autori includono «a lack of correspondence between the form of words found in the regulation and the form that the technology now takes; at other times, the difficulty is that the original regulatory purposes no longer provide clear justificatory cover for the uses to which the technology is now put» (*ibidem*, p. 65). Per un esempio concreto si rinvia alle vicende *R. v. Secretary of State ex parte Quintavalle*, n. 325 (House of Lords, 13 marzo 2003); *R. (Quintavalle on behalf of Comment on Reproductive Ethics) v. Human Fertilisation and Embryology Authority*, n. 2785 (Court of Appeal, January 18, 2002). Tali casi segnarono la *disconnection* del *Fertilisation and Embriology Act* del 1990: il primo caso rileva che la definizione del concetto di «embrione» fornita nell'atto non era *technology-neutral*; nel secondo caso la «disconnessione» è determinata dalla diagnosi genetica preimpianto, non prevista dall'*Act*.

[4] Sul tema dello *human enhancement* si rinvia a L. Palazzani, *Il potenziamento umano. Tecnoscienza, etica e diritto*, Torino, Giappichelli, 2015.

prodotti in buona parte associati all'IoT, richiede ai governi e a una vasta gamma di esperti coinvolti, di migliorare la cooperazione internazionale per conformarsi ai nuovi *digital business models*.

È necessario notare, però, che le lacune normative sono aspetti «fisiologici» del diritto destinato a disciplinare i vari profili di un cambiamento tecnologico: non è compito del diritto anticipare le traiettorie di sviluppo di tale cambiamento[5]. È, invece, importante disporre di apparati e strategie regolatorie flessibili e aperti al panorama socio-tecnologico del presente, per creare le condizioni per uno sviluppo responsabile delle applicazioni future. Lo sviluppo delle nuove tecnologie è, infatti, un processo nel quale scienza, tecnologia e società co-evolvono in modo interdipendente.

Da qui, la necessità di coinvolgere nei processi regolatori stakeholder aventi diversi ambiti di specializzazione. I primi documenti europei dedicati alla robotica delineano, infatti, una maggior *expertise* del legislatore europeo nell'uso degli strumenti di partecipazione pubblica[6].

Generalmente, l'effettività di un modello regolatorio si misura sulla base degli obiettivi di policy raggiunti, e sui dati relativi alla *compliance* alle regole, o ai modelli comportamentali[7]. Tuttavia, la verifica degli effettivi risultati della governance delle tecnologie convergenti richiede un'analisi più ampia rispetto alla sola conformità normativa: la natura delle incertezze tecnoscientifiche, le quali caratterizzano le primissime fasi dell'implementazione, fa sì che il ruolo primario della regolamentazione sia quello di favorire il dialogo

[5] L. Bennett Moses, *Agents of Change: How the Law «Copes» with Technological Change*, in *Griffith Law Review*, 20, 4, 2011, p. 763.

[6] Per un'ampia disamina della governance e del rapporto tra essa e il diritto si rinvia a M.R. Ferrarese, *Diritto sconfinato. Inventiva giuridica e spazi nel mondo globale*, Roma-Bari, Laterza, 2006 e della stessa autrice, *La governance tra politica e diritto*, Bologna, Il Mulino, 2010.

[7] H. Opschoor e K. Turner, *Economic Incentives and Environmental Policies: Principles and Practice*, Dordrecht, Kluwer Academic Publishers, 1994.

tra gli attori sociali coinvolti, e di convincerli a prendere seriamente le loro responsabilità[8].

La promozione di un modello partecipativo al fine di affrontare e gestire la rilevanza sociale dell'incertezza tecnoscientifica è anche un modo per offrire una prospettiva più ampia di tutela della sicurezza in robotica[9], e in genere delle tecnologie, esistenti, emergenti e/o convergenti[10], intendendo con queste ultime riferirsi all'unificazione, combinazione e integrazione sinergica tra i quattro settori scientifici, nanotecnologie, biotecnologie, informatica e scienze cognitive (Nbic). Il modello di governance per cui si opta deve incentivare l'innovazione, gestendo i vari gradi di incertezza scientifica, i quali sono parametrati ai diversi stadi cognitivi della conoscenza del rischio: il pericolo, il rischio, l'incertezza e l'indeterminatezza. Ogni nuova propo-

[8] B. Dorbeck-Jung e B.M. Bowman, *Regulatory Governance Approaches for Emerging Technologies*, in D.M. Bowman, E. Stokes e A. Rip, *Embedding New Technologies into Society: A Regulatory, Ethical and Societal*, Singapore, Pan Stanford Publishing, 2017, pp. 35-59; European Commission Expert Group on Science and Governance, *Taking European Knowledge Society Seriously*, Luxembourg, Office for Official Publications of the European Communities, 2007, p. 40.

[9] Parla di «rilevanza sociale dell'incertezza» M. Tallacchini, *La costruzione giuridica dei rischi e la partecipazione del pubblico alle decisioni science-based*, in AA.VV., *Scienza e diritto nel prisma del diritto comparato*, Torino, Giappichelli, 2004, p. 339.

[10] Le differenze terminologiche sono chiarite da Palazzani, *Il potenziamento umano*, cit., p. 4. Anche se riferiti al fenomeno del potenziamento umano, pare utile riportare, in sintesi, i chiarimenti dell'autore circa le differenze terminologiche. Le tecnologie «esistenti» sono quelle già diffuse nella prassi e, dunque, oggetto di riflessione nell'ambito dell'etica medica e della bioetica. Le tecnologie emergenti si riferiscono agli ambiti nuovi di intervento che si stanno delineando in questi ultimi anni e, nel presente, in settori che solo recentemente sono stati analizzati dalla riflessione morale; con tecnologie convergenti non si intende una mera interconnessione interdisciplinare tra diversi ambiti della scienza. L'autore nota che l'innovazione – nel caso delle tecnologie convergenti – non è determinata dalla somma dei risultati delle quattro dimensioni della scienza, ma dal prodotto della loro interazione sistemica, il cui obiettivo è quello di intervenire direttamente sul corpo e la mente trasformando e perfezionando l'uomo e la stessa umanità. Sul concetto di convergenza tecnologica si rinvia anche a G. Pascuzzi, *Il diritto dell'era digitale*, Bologna, Il Mulino, 2016, pp. 17 ss.

sta regolatoria della Commissione europea, la quale affronti questioni scaturenti dall'impiego di AI e della robotica, deve ispirarsi all'*Innovation Principle*: principio che segue una serie di linee guida sviluppate proprio al fine di assicurare che le iniziative siano *innovation friendly*[11].

Metodi concreti, in altri termini, per far fronte agli ineliminabili «doni dello spirito maligno», mutuando una famosa espressione di Calabresi[12]. Tali effetti riecheggiano anche nelle riflessioni del sociologo tedesco Ulrich Beck, il quale negli anni Ottanta del secolo scorso osservava che «nella modernità avanzata la produzione sociale di ricchezza va sistematicamente di pari passo con la produzione sociale dei rischi»[13], includendo, altresì, fin dalle prime fasi di sviluppo e impiego dei ritrovati tecnologici, le questioni sollevate dal contesto socio-economico.

Ferma restando l'attualità di tali considerazioni, sia ragioni tecniche che quelle etico-sociali hanno indotto l'ordinamento europeo al passaggio da *risk-governance* a *innovation-governance*[14], per indicare la scelta di modelli più flessibili ad accogliere il cambiamento.

Tutto ciò appare come una logica conseguenza dell'importanza assunta dalla strategia di *responsible research and innovation* che integra *ab origine* questioni di rilevanza etica e sociale, e rappresenta un irrinunciabile punto di partenza per fondare lo sviluppo tecnologico sul rispetto dei valori dell'Unione di cui all'art. 2 del Tue[15].

[11] Cfr. https://ec.europa.eu/epsc/publications/strategic-notes/towards-innovation-principle-endorsed-better-regulation_en.

[12] G. Calabresi, *Il dono dello spirito maligno*, Milano, Giuffrè, 1996, pp. 11-12, contestualizza tali riflessioni a proposito dei danni da incidenti stradali provocati dalla diffusione delle automobili.

[13] U. Beck, *La società del rischio: verso una seconda modernità*, Roma, Privitera, 2000, p. 25.

[14] Expert Group on Science and Governance, *Taking European Knowledge Society Seriously*, cit., p. 40. Il passaggio è spiegato in dettaglio da uno degli autori del report B. Wynne, *Normalizing Europe – and the World – through Science: Risk, uncertainty and Precaution*, in S. Rodotà e M. Tallacchini (a cura di), *Ambito e Fonti del Biodiritto*, in S. Rodotà e P. Zatti (a cura di), *Trattato di Biodiritto*, Milano, Giuffrè, 2010, pp. 491 ss.

[15] L'art. 2 del Trattato dell'UE: «The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule

Ci sono già esempi recenti. La strategia europea a favore delle nanotecnologie si è orientata, fin dal 2004, verso la «sperimentazione di nuove e complementari forme di normatività», combinando strumenti giuridici di *command and control* con strumenti di *soft law*[16]. Seppur con diverse sfumature, tutte queste alternative tentano di informarsi alla Rri, spostando il fulcro degli obiettivi verso la promozione di un'innovazione responsabile.

La frammentarietà, la varietà delle fonti e la giovinezza delle materie accomunate dalla caratteristica del «convergere» sono, sicuramente, tra le ragioni principali che impediscono la strutturazione di un modello di inquadramento per le stesse. Eppure, la mole dei documenti europei sia di *hard law* che di *soft law* dedicati a quelle quattro province della tecnoscienza (Nbic) è, ormai, consistente.

1.1. *Rri policy, «responsible AI» e modelli di «governance»*

La Rri costituisce il sostrato della politica europea in materia di innovazione: su di essa si fondano i modelli di governance delle tecnologie convergenti che aspirano a ottenere l'avvallo sociale (c.d. «licenza sociale»[17]). La strategia è definita come segue:

> a transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view on the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products (in

of law and respect for human rights, including the rights of persons belonging to minorities». Gli Stati membri condividono una «society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail».

[16] M. Tallacchini, *Scienza e diritto. Prospettive di «co-produzione»*, in *Rivista di filosofia del diritto*, 2, 2012, pp. 313-336.

[17] R. Brownsword e H. Somsen, *Law, Innovation and Technology: Before We Fast Forward – A Forum for Debate*, in *Law, Innovation and Technology*, 1, 2009, pp. 1-73.

order to allow a proper embedding of scientific and technological advances in our society)[18].

Il concetto, che evoca quello della responsabilità sociale d'impresa[19], è stato introdotto nel 2011 dal commissario europeo Von Schomberg. Per la sua ampia e astratta formulazione, una miriade di progetti europei ha già tentato di ancorarlo a parametri e valori di riferimento idonei a conferire una valenza pratica alla logica a cui si ispira. Autorevole dottrina identifica le radici della Rri nell'impiego di un *design* regolatorio informato ai valori dell'ordinamento, all'etica applicata e, sebbene meno visibilmente, all'idea di *responsive regulation*, *risk governance* e processi partecipativi[20]. Ci sono, però, molti altri modi per sviluppare concretamente la Rri, tutti hanno in comune il coinvolgimento di un ampio numero di stakeholder nei processi di innovazione. Si possono, fondamentalmente, distinguere due approcci: il c.d. *product approach* per lo sviluppo di un metodo, o di linee guida, funzionali a caratterizzare l'innovazione come responsabile in un determinato contesto; e l'opposto, il c.d. *process approach*, con il quale si tenta di informare a essa le procedure e pratiche. Quest'ultimo è ben accolto da ingegneri, e altri professionisti coinvolti nello sviluppo della ricerca robotica, proprio perché permetterebbe di integrare, fin dalle prime fasi del *design* del robot, valori etici e indicazioni legislative.

Con riferimento specifico all'AI, la Commissione europea ha espresso la necessità che la Rri diventi il criterio guida

[18] R. Von Schomberg, *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, Luxembourg, Publications Office of the European Union, 2011, pp. 7-17.

[19] Così sottolineano R. Leenes, E. Palmerini, B.-J. Koops, A. Bertolini, P. Salvini e F. Lucivero, *Regulatory Challenges of Robotics: Some Guidelines for Addressing Legal and Ethical Issues*, in *Law, Innovation and Technology*, 9, 2017, pp. 1-44.

[20] B.J. Koops, *The Concepts, Approaches and Applications of Responsible Innovation. An Introduction*, in B.J. Koops *et al.* (a cura di), *Responsible Innovation 2: Concepts, Approaches and Applications*, Dordrecht, Springer, 2015, pp. 4-5.

per lo sviluppo di una *responsible AI*[21], che ponga al centro la persona. A tal proposito, la Commissione auspica che, entro la fine del 2018, siano predisposte da un gruppo di esperti e stakeholder – la *European AI Alliance* in cooperazione con lo *European Group on Ethics in Science and New Technologies* – delle linee guida per il rispetto dei diritti fondamentali in materia.

Tradizionalmente, i modelli impiegati per affrontare le incertezze multiple associate alle tecnologie convergenti, si sono sviluppati lungo tre direttrici: il *lassaiz-faire*; la proibizione (es. la clonazione umana); l'assenza di regolazione specifica (es. internet agli albori).

I sistemi di regolazione si basano su modelli *evidence-based*. Ciò avviene, a diverse latitudini, seppur con una diversa attribuzione di funzioni: nell'ordinamento europeo, per esempio, la funzione di *risk assessment*, attribuita a organismi specifici (es. Efsa) è separata da quella di *risk management*, attribuita alla Commissione europea; nell'ordinamento americano il quadro è frammentario e le due funzioni non sono divise[22]. In Europa, l'approccio *evidence-based* e quello *risk-based* sono stati, spesso, oggetto di dibattiti e critiche in favore di uno precauzionale che, dall'ambito della tutela ambientale *ex* art. 191 del Tfue, si è esteso ad altri ambiti rilevanti per la tutela della salute pubblica, incluse le biotecnologie[23], grazie prevalentemente all'opera giurisprudenziale

[21] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Artificial Intelligence for Europe*, Bruxelles, 25 aprile 2018, Com(2018) 237 final, p. 8, n. 27.

[22] *Modernizing the Regulatory System for Biotechnology Products*, 2017, il documento è consultabile all'indirizzo https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2017_coordinated_framework_update.pdf.

[23] M. Tallacchini, *Between Uncertainty and Responsibility: Precaution and the Complex Journey towards Reflexive Innovation*, in E. Vos, M. Van Assel e M. Everson (a cura di), *Trade, Health and the Environment: The European Union Put to the Test*, London-New York, Earthscan Routledge, 2014, pp. 74-88. Nel passaggio dalle biotecnologie alle nanotecnologie, e più recentemente, almeno in prospettiva futura, alla biologia sintetica,

che ha indotto le istituzioni europee ad assumere misure protettive della salute e sicurezza dei consumatori, anche in circostanze in cui i potenziali rischi non erano pienamente dimostrati[24].

L'Unione europea è un contesto particolarmente produttivo di sperimentazioni regolatorie, avviate al fine di affrontare la tensione tra rischio e innovazione, alla base del cambiamento tecnologico[25], e per far fronte al *law-lag*, sempre più inestricabilmente legato al *social-lag* ed *ethical-lag*, tutte dimensioni entro le quali il rischio tecnologico ha impatti diversi.

Nel corso dell'ultimo ventennio, il fiorire di numerosi nuovi modelli di governance delle tecnologie, alternativi a quelli classici, è fenomeno identificabile come *global legal pluralism*. Secondo una recente ricostruzione della dottrina[26], i principali modelli sono i seguenti: *i*) *anticipatory governance*, come ad esempio le proposte del Parlamento

il concetto originale di precauzione è stato arricchito con nuovi elementi di riflessione. Da un lato, l'idea di un «modello di partecipazione esteso» nella relazione tra scienza e società ha introdotto un metodo generale per raccogliere tutte le informazioni coinvolgendo attivamente i cittadini. Dall'altro, il concetto di precauzione si trova declinato nel principio di responsabilità al quale dovrebbero informarsi la ricerca e l'innovazione in materia di tecnologie emergenti. Tutti questi sviluppi verso un'innovazione responsabile sono accompagnati da importanti aspettative circa una governance globale della scienza e della tecnologia. Tuttavia, non è semplice capire fino a che punto la Rri possa essere effettivamente implementata. Con la strategia UE 2020, l'Unione mira a diventare l'Unione dell'Innovazione: la tecnologia diventa sia protagonista, sia oggetto dei processi di *risk management*, sia rispetto alla necessità di favorire l'innovazione entro il quadro giuridico multilivello che quello istituzionale del mercato interno.

[24] Per un'analisi sul rischio incerto di danno si rinvia anche a R. Montinaro, *Dubbio scientifico, precauzione e danno da prodotto*, in E. Al Mureden, *La sicurezza dei prodotti e la responsabilità del produttore. Casi e materiali*, Torino, Giappichelli, 2017, pp. 330 ss.

[25] F. Sabel e J. Zeitlin, *Experimentalist Governance in the European Union: Towards a New Architecture*, Oxford, Oxford University Press, 2012.

[26] Dorbeck-Jung e Bowman, *Regulatory Governance Approaches for Emerging Technologies*, cit., pp. 35-59. Si veda anche E. Pariotti, *Normatività giuridica e governance delle tecnologie emergenti*, in AA.VV., *Forme di responsabilità, regolazione e nanotecnologie*, Bologna, Il Mulino, 2011.

europeo e del Consiglio del 2009, per l'introduzione di regole specifiche sull'utilizzo di nanomateriali nei prodotti cosmetici, che si inserivano nel più ampio quadro di riforma della materia[27]; *ii*) *responsive regulation* che veicola i valori, quelli orientati dalla politica e dalle risorse, nei vari ambiti sociali; *iii*) la co-regolamentazione, che si riferisce a forme collaborative di regolamentazione (e di autocontrollo), da affiancare a quelle tradizionali di carattere pubblico al fine di creare un nuovo sistema regolamentativo[28]. La *iv*) *reflexive regulation theory* che promuove regole capaci di alimentare l'autodisciplina, invece che condizionare l'evoluzione dei comportamenti indicando i contenuti delle decisioni da adottare[29]; la *v*) *meta-regulation* esemplificata dal Codice di condotta per una ricerca responsabile nel campo delle nanoscienze e nanotecnologie della Commissione europea nel 2008[30], con la quale si promuovono strumenti di *self-regulation*, e schemi di *data reporting* sulla sicurezza dei materiali; e la *vi*) governance multipartecipativa, dove le discussioni intergovernative, le decisioni e le collaborazioni si svolgono con la partecipazione delle varie parti interessate e dei governi. La governance di internet è esempio per eccellenza[31].

1.2. *La sicurezza «by design»*

La crescente importanza acquisita dalla regolamentazione *by design* si riscontra soprattutto negli ambiti di impiego

[27] Regolamento del Parlamento Europeo e del Consiglio del 30 novembre 2009 sui Prodotti Cosmetici n. 1223/2009, in *GU L*, 342, del 22 dicembre 2009, p. 59.

[28] L. Senden, *Soft Law, Self-regulation and Co-regulation in European Law: Where Do They Meet?*, in *Electronic Journal of Comparative Law*, 9, 2005, pp. 1-27.

[29] G. Teubner, *Substantive and Reflexive Elements in Modern Law*, in *Law and Society Review*, 17, 1983, pp. 239-286.

[30] Commissione europea, *Raccomandazione per un Codice di condotta per una ricerca responsabile nel settore delle nanoscienze e nanotecnologie*, Bruxelles, 7 febbraio 2008.

[31] Cfr. Pascuzzi, *Il diritto dell'era digitale*, cit., p. 336.

della tecnologia informatica[32], ed esemplifica in modo evidente l'attuazione della Rri. Con riferimento al tema in esame, diventa essenziale cogliere l'importanza assunta da questa tecnica e dalla discussione relativa ai modelli di IT *designs*. In ottica *ex post* il tema sarà ripreso, in quanto il difetto di progettazione si preannuncia come l'ipotesi più verosimilmente configurabile in robotica (*infra* cap. II).

L'espressione *by design* allude all'inclusione delle regole giuridiche, sociali, ed etiche «fin dalla progettazione»[33]. Si tratta di un corollario della c.d. architettura, quale componente dello «strumentario» regolatorio indicato da Lessig, per affrontare i problemi giuridici della *cyberlaw*. La *regulatory tool-box* comprende il diritto, le norme sociali, il mercato, e l'architettura appunto (per esempio, la tecnologia in sé e per sé)[34]. Nella letteratura giuridica dedicata alla robotica questa stessa matrice rappresenta, spesso, lo schema secondo il quale si articola il discorso[35], poiché ognuno di questi strumenti ne modella lo sviluppo.

Il *by design* è divenuto sempre più popolare, contribuendo, così, a orientare, in maniera pragmatica, anche l'operato di ricercatori, ingegneri e tecnici. Basti pensare che nessun algoritmo è di per sé immune al pregiudizio: il fatto che sia un processo meccanico, non dovrebbe farci dimenticare che è stato scritto da esseri umani con valori e desideri precisi, i quali traspaiono nel software stesso[36]. Ciò comporterà

[32] Aspetti problematici connessi al profilo dell'*auto-enforcement* sono espressi nel caso *Marper v. The United Kindom* (European Court of Human Rights, 4 dicembre 2008), disponibile all'indirizzo https://hudoc.echr.coe.int/eng.

[33] Per un esame approfondito cfr. B.J. Koops e R. Leenes, *Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the «Privacy by Design» Provision in Data Protection Law*, in *International Review of Law, Computers & Technology*, 28, 2, 2014, pp. 159-171, consultabile all'indirizzo http://dx.doi.org/10.1080/13600869.2013.801589.

[34] L. Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, 6, 1999, p. 501.

[35] Leenes, Palmerini, Koops, Bertolini, Salvini, Lucivero, *Regulatory Challenges of Robotics*, cit., p. 7.

[36] Sul problema della mancanza di neutralità dell'algoritmo si rinvia a F. Pasquale, *The Black Box Society*, Cambridge, Harvard University Press, 2015.

una riflessione sui criteri di scelta dei valori che dovranno essere incorporati[37]. Quale forma di *techno-regulation*, il *design* di un prodotto influisce, altresì, sul comportamento del consumatore. Ricerche in vari ambiti disciplinari, tra le quali quelle dedicate alla *human-computer interaction* (Hci), *human-robot interaction* (Hri), e alla filosofia della tecnologia hanno rivelato che le componenti del *design* degli artefatti tecnologici – forma, modello e funzionalità – influiscono sulle risposte degli utenti a tali artefatti[38].

Com'è intuibile, nei robot collaborativi il *design* assume un ruolo centrale: essi si muovono, interagiscono con l'uomo e compiono azioni, le cui conseguenze hanno una rilevanza giuridica. Le regole «comportamentali» potrebbero essere incorporate *by design*[39]. Anche la forma e le sembianze di umanoidi incidono molto sulle reazioni che provocano nelle persone che ne fanno uso[40] (cfr. *infra* cap. II).

[37] R. Leenes e F. Lucivero, *Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behavior by Design*, in *Law, Innovation and Technology*, 6, 2014, pp. 193-220. Vedi *infra* il caso delle *self-driving car* (cap. II).

[38] Sulla «design-based regulation», o «techno-regulation», vedi R. Brownsword, *Rights, Regulation, and the Technological Revolution*, Oxford, Oxford University Press, 2008; e B. Van Den Berg, *Techno-elicitation: Regulating Behaviour through the Design of Robots*, gennaio 2011, consultabile all'indirizzo https://www.academia.edu/1760374/Techno-elicitation_Regulating_behaviour_through_the_design_of_robots. I dossi artificiali, o rallentatori, sono un esempio tipico di tecno-regolamentazione, poiché non impongono regole ma inducono a tenere un determinato comportamento: chi occupa la strada deve rallentare, per non creare danni al veicolo e perché non è confortevole viaggiare quando essi sono applicati sulla careggiata.

[39] Immaginando di costruire un'analogia con il mondo fantascientifico, verrebbe da pensare al codice come al positronic brain immaginato da Asimov. I. Asimov e R. Silverberg, *The Positronic Man*, Pan, Bantam Books, 1994.

[40] P. Salvini, C. Laschi e P. Dario, *Design for Acceptability: The Role of Human Factor in Designing Service Robots*, in *International Journal of Social Robotics*, 2, 2010, pp. 451-460. Gli autori analizzano l'accettabilità del *design* dei robot sociali, e propongono l'approccio della *Human-Tech Ladder* di Vincente.

Questo tipo di progettazione è già ampiamente usato per la protezione dei dati personali[41]: con *privacy by design* si intende l'incorporazione delle garanzie a tutela della protezione dei dati personali nelle tecnologie Ict, espressa nel 2009 in un documento, il *Data Protection Working Party*[42], e da ultimo introdotta con l'art. 25 del Regolamento UE 2016/679 in materia di protezione dei dati[43].

Il meccanismo in esame è utilizzato anche al fine di regolamentare la sicurezza, e pertanto prende il nome di *safe-by-design* (SbD)[44], per indicare l'insieme delle misure tecniche che gestendo non solo i rischi prevedibili, ma anche altri scenari dell'incertezza tecnoscientifica, affrontano i problemi di sicurezza, fin dalle prime fasi della progettazione delle nuove tecnologie.

Lo sviluppo dell'AI ha un impatto enorme su problemi di gestione della sicurezza dei prodotti. Prodotti «smart» possono essere progettati per adattarsi al comportamento del consumatore. Ciò significa che questi artefatti possono «relazionarsi» con i consumatori, attraverso comportamenti che non erano stati previsti e programmati dal progettista, e dai quali potrebbero scaturire rischi per la sicurezza. In questi casi, i prodotti di robotica avanzata potrebbero «adat-

[41] Cfr. A. Podsiadla, *What Robotics Can Learn from the Contemporary Problems of Information Technology Sector: Privacy by Design as a Product Safety Standard Compliance and Enforcement*, paper presentato alla conferenza *We Robot: Getting Down to Business*, Stanford, 8 aprile 2013.

[42] Data Protection Working Party, Working Party on Police and Justice, *The Future of Privacy. Joint contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 2009. Cfr. art. 29.

[43] 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.

[44] Nel corso dell'ultimo decennio, il SbD è stato impiegato anche nella gestione dei rischi derivanti dalle nanotecnologie e dalla biologia sintetica. I. van de Poel e Z. Robaey, *Safe-by-design: From Safety to Responsibility*, in *Nanoethics*, 2017, pp. 297-306. Secondo gli autori più che focalizzarsi sulle misure di *safety*, è opportuno identificare i profili di responsabilità del design (*responsibility for safety through design*).

tare» le loro azioni e prestazioni per ridurre o minimizzare il rischio, creando un più elevato livello di sicurezza.

Con riferimento al machine learning, dunque, il concetto di SbD si rivela particolarmente utile per affrontare situazioni impossibili da standardizzare: quando, per esempio, non è possibile conoscere le reazioni alle condizioni ambientali, le interazioni tra robot e uomo e l'entità di un eventuale danno[45]. Per esempio, nel programmare la sicurezza di ogni modello di *self-driving car*, si include il comando necessario a riprendere il controllo manualmente, e lasciare quindi all'uomo l'incombenza di una decisione difficile in situazioni di emergenza. Conseguentemente, la valutazione del *design* in sede *ex post* diventa un aspetto di cruciale importanza al fine di individuare eventuali malfunzionamenti e distribuire le responsabilità. Peraltro, proprio l'analisi di questo profilo esemplificherà il modo in cui le tecnologie innovative introducono elementi di indeterminatezza, i quali minano la certezza dell'applicabilità ed effettività delle regole convenzionali (vedi *infra* cap. II)[46].

2. *La sicurezza dei prodotti nell'«Internet of Things»*

Prima di definire il quadro normativo in tema di sicurezza applicabile a prodotti robotici secondo le coordinate normative orizzontali e verticali del diritto europeo, è opportuno ricostruire, nelle linee essenziali, un altro framework che, a partire dal 2014, va delineandosi in materia di *digital economy*: con essa la Commissione mira a creare un quadro programmatico chiaro e specifico per l'economia dei dati, affrontando, altresì, le incertezze giuridiche create dalle tecnologie emergenti basate sulla condivisione di dati. Anche questo diventa una parte essenziale del quadro di riferimento sovranazionale per identificare le caratteristiche emergenti

[45] Molti algoritmi eseguono opzioni di scelta sulla base di dati economici. Cfr. cap. II.

[46] S. Chopra e L.F. White, *A Legal Theory for Autonomos Artificial Agents*, Michigan, University of Michigan Press, 2011, p. 139.

del problema della sicurezza dei prodotti che il sistema giuridico deve garantire. Tale garanzia è, altresì, funzionale alla realizzazione di quanto stabilito *ex* art. 169 del Tfue.

Il 10 gennaio 2017, la Commissione europea pubblicò un pacchetto di documenti volti a costruire «un'economia dei dati europea»[47], ove tra le questioni emergenti è inclusa – secondo una strana logica[48] – quella relativa alla responsabilità per danni causati da un difetto di un dispositivo o di un robot connesso. Nel contesto delle tecnologie digitali emergenti esistono interdipendenze complesse e sofisticate, sia nella struttura di uno stesso prodotto (tra hardware e software), sia fra dispositivi interconnessi, poiché le tipiche componenti dei dispositivi connessi grazie all'IoT includono hardware, software, protocolli e standard di comunicazione.

La Commissione dedica particolare attenzione a tutte le nuove questioni poste dalla guida autonoma, relativamente ai fattori di imprevedibilità e indesiderabilità dell'azione, quali potenziali cause di danni a persone e cose[49]. Essi minerebbero, infatti, la certezza del diritto relativamente all'applicazione del quadro normativo esistente in materia di responsabilità e sicurezza. Anche per questo è stata avviata una parallela, e in parte sovrapponibile, consultazione sulla valutazione della Direttiva 85/374/Eec (vedi *infra* par. 4.1). L'importanza della questione della responsabilità delle emergenti tecnologie digitali è, da ultimo, testimoniata dalla recentissima Comunicazione della Commissione europea del 25 aprile 2018 dedicata all'*Artificial Intelligence for*

[47] Commissione europea, *Comunicazione della commissione al parlamento europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni «Costruire un'economia dei dati europea»*, Bruxelles, 10 gennaio 2017, Com(2017) 9 final.

[48] C. Wendehorst, *Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy*, in S. Lohsse, R. Schulze e D. Staudenmayer (a cura di), *Trading Data in the Digital Economy: Legal Concepts and Tools. Munster Colloquia on EU Law and the Digital Economy III*, Baden-Baden, Nomos-Hart Publishing, 2017, p. 327.

[49] Questo profilo è incluso, altresì, nel documento della stessa European Commission, *Staff Working Document Advancing the Internet of Things*, Swd(2016) 110.

Europe[50], e dal relativo documento di accompagnamento che si focalizza sul tema della *liability for emerging digital technologies*[51] (vedi *amplius*, par. 4.1).

Un altro riferimento importante in materia è rappresentato dal report dell'Organizzazione per la cooperazione e lo sviluppo economico (Oecd), intitolato *Consumer Product Safety in the Internet of Things*[52], che ha cura di definire, innanzitutto, l'IoT come un ecosistema «in which applications and services are driven by data collected from devices that sense and interface with physical world»[53].

Oggi, il mercato dei prodotti ospita una gran varietà di dispostivi e applicazioni connesse, ma poiché il fenomeno è considerato ancora agli albori, molte e inimmaginabili tecnologie potrebbero, tra qualche tempo, innescare cambiamenti importanti nella produttività, nell'impatto ambientale e nei modelli di business. L'IoT incorpora una serie di nuove tecnologie che migliorano la funzionalità dei prodotti e offrono nuove opportunità ai consumatori, creando nuovi mercati per prodotti non previamente esistenti[54].

Anche l'Oecd focalizza l'attenzione sulle macchine a guida automatizzata. È proprio in virtù della connessione a internet che questi veicoli avvisano il conducente circa la presenza di eventuali pericoli legati alle condizioni atmosferiche o alle condizioni stradali o della vettura stessa, di modo

[50] European Commission, *Artificial Intelligence for Europe*, cit.

[51] European Commission, *Staff Working Document. Liability for Emerging Digital Technologies*, Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Artificial Intelligence for Europe*, Com(2018) 237 final.

[52] Oecd, *Consumer Product Safety in the Internet of Things*, in *Oecd Digital Economy Papers*, n. 267, 29 marzo 2018, consultabile all'indirizzo http://dx.doi.org/10.1787/7c45fa66-en.

[53] *Ibidem*, p. 8 del documento. In sintesi, l'IoT comprende tre elementi: 1) sensori che collezionano i nostri dati e quelli dell'ambiente; 2) gli smart, che decodificano il significato dei dati e rispondono agli stessi; 3) gli attuatori che intervengono su dispositivi e ambiente.

[54] L'allegato I dello *Staff Working Document* elenca le caratteristiche delle *emerging digital technologies*.

che essi possano adattarsi da remoto, o autonomamente. Sono in via di sviluppo anche tecnologie che permettono a un veicolo di connettersi con altri dispositivi, inclusi quelli domestici. La connettività rivoluzionerà, dunque, il mercato automobilistico. Basti pensare che la percezione automatizzata, inclusa la capacità visiva ha, quasi, raggiunto le *performance* dell'occhio umano, e i progressi nella percezione sono seguiti dall'introduzione di algoritmi sempre più sofisticati con elevate capacità di ragionamento, inclusa la capacità di programmare e prevedere[55]. Per esempio, un veicolo automatizzato potrebbe essere in grado di rilevare la presenza di un pallone che rimbalza sulla careggiata, riconoscendo che quel pallone potrebbe essere seguito da un bambino. A questo punto, il veicolo potrebbe prevedere tutte le variabili della situazione e, conseguentemente, programmare le sue azioni sulla base di queste.

I benefici dell'IoT in termini di sicurezza, quelli già in essere, e quelli potenziali per i consumatori sono numerosi, come per esempio la possibilità di rafforzare il livello di protezione dei consumatori, e rendere la vita più facile, aumentando efficienza e sostenibilità.

Non mancano, naturalmente, i rischi potenziali per la sicurezza dei prodotti associati all'impiego dell'IoT. Sebbene non vi siano ancora dati disponibili, la complessità dell'ecosistema permette già di delineare i principali rischi.

Nel 2017, la *US Consumer Product Safety Commission* ha identificato alcune categorie di potenziali rischi[56], tra i quali:

i) il *malfunzionamento* del prodotto causato da un difetto o derivante da un aggiornamento. L'aspetto critico è legato alla possibilità di aggiornare il software del dispositivo, o applicazione dell'IoT, successivamente alla fase in cui tale servizio di aggiornamento rientra tra gli obblighi contrattuali del produttore. Le modificazioni apportate al software

[55] Stanford University, *One Hundred Year Study on Artificial Intelligence (AI100)*, consultabile all'indirizzo https://ai100.stanford.edu.

[56] US Consumer Product Safety Commission (Cpsc), *Potential Hazards Associeted with Emerging and Future Technologies*, 2017, consultabile all'indirizzo https://www.cpsc.gov.

possono influire sul funzionamento del dispositivo, o possono diventare esse stesse causa di un malfunzionamento qualora il dispositivo, proprio in seguito all'aggiornamento, interrompa la connessione con gli altri dispositivi. Tale «difetto» potrebbe, per esempio, inavvertitamente, disattivare un dispositivo di sicurezza, o farlo funzionare in maniera non conforme a quanto atteso;

ii) la *perdita di connettività e l'obsolescenza* del prodotto. Se il prodotto sfrutta la connessione per funzionare in modo sicuro, la perdita di connettività potrebbe avere dirette e immediate implicazioni per la sicurezza;

iii) la *qualità e l'integrità dei dati* quando essi supportano la funzione di sicurezza. La costruzione di un *safety design* si basa sull'utilizzo di dati, questo implica che quei dati debbano necessariamente essere esatti, accurati e autentici;

iv) i *danni fisici*. Rispetto alla casistica classica, il tipo di dispositivi utilizzati con l'IoT hanno spesso un rapporto molto stretto con il corpo del consumatore. Spesso si tratta di dispositivi indossabili.

Guardando alle nuove tipologie di rischi, va osservato un tratto comune che anticipa una considerazione, oggetto di ulteriori attenzioni nel prosieguo di queste pagine: la *digital security* diventa una questione rilevante anche entro il tema classico della sicurezza dei prodotti. Con lo sviluppo inarrestabile dell'IoT, l'utilizzo di informazioni digitali potrebbe configurare problemi che vanno ben oltre la tutela di dati dei consumatori, dal momento che l'integrità degli stessi potrebbe essere propedeutica al corretto funzionamento del prodotto stesso[57].

Sia il Parlamento europeo, che la *US Federal Trade Commission* (US Ftc)[58] hanno espresso le loro preoccupa-

[57] Per un'analisi sulla sicurezza dei sistemi informatici si rinvia a Pascuzzi, *Il diritto dell'era digitale*, cit., pp. 349 ss.

[58] US Federal Trade Commission, *Internet of Things Privacy and Security in a Connected World Ftc Staa Report*, 2015, consultabile all'indirizzo https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. La US Commission ha notato che, tra gli altri rischi, «unauthorized persons might exploit security vulnerabilities to create risks to physical safety in some cases».

zioni in merito alle implicazioni della sicurezza informatica nella prospettiva della tutela della sicurezza dei prodotti dei consumatori.

Molti governi hanno già avviato una discussione su quelle che sembrano essere le tre principali questioni di policy da affrontare[59]: *a*) l'impatto dell'IoT sulla distinzione tra hardware, software, prodotto e servizio; *b*) l'individuazione di chi è responsabile per la sicurezza dei prodotti[60], e la distribuzione delle responsabilità in caso di danno da difetto; *c*) i profili di comunicazione del rischio[61].

In fondo, si tratterà di affrontare anche problemi che in parte si sono già profilati nel recente passato, e che si complicano ulteriormente nell'IoT. L'applicabilità della regolamentazione sulla sicurezza da prodotto e le regole di responsabilità si basano, per esempio, sulla distinzione tra vendita di prodotti e fornitura di servizi che disciplina in maniera diversa ciascun scenario. I dispositivi o le applicazioni nell'IoT possono presentarsi come una combinazione di beni e servizi. Inoltre, la stessa qualificazione del software quale prodotto cui applicare la normativa sulla responsabilità da prodotto difettoso è stata a lungo oggetto di dibattiti[62]. Per opera dell'IoT, l'interazione tra

[59] L'*American Bar Association*, per esempio, ha già indicato che ogni dispositivo connesso dev'essere considerato unico e, pertanto, non è possibile individuare un approccio *one size fits all* per regolare l'IoT. American Bar Association, *Consumer Product Safety Administration Seeks Collaboration in Managing Internet of Things*, consultabile all'indirizzo https://www.americanbar.org/news/abanews/aba-news-archives/2017/05/consumer_productsaf.html, accesso marzo 2018.

[60] Se il malfunzionamento del software deriva da un aggiornamento avvenuto successivamente alla vendita e non eseguito dal produttore, potrebbe non essere chiaro chi sia il responsabile del difetto. Il quadro si complica ancora di più quando il funzionamento del prodotto dipende da dati provenienti da prodotti basati sull'AI. Vedi *amplius* cap. II.

[61] Oecd, *Consumer Product Safety in the Internet of Things*, cit., p. 21 del documento.

[62] Un lungo dibattito dottrinale caratterizza il problema della natura giuridica da attribuire al software. C'è chi, in passato, ha sostenuto che i software fossero assimilabili a opere letterarie. È interessante la constatazione che la difficoltà di concettualizzare i malfunzionamenti derivanti dai programmi dei computer in termini di responsabilità da prodotto

hardware e software raggiunge un livello elevatissimo di complessità[63], e il funzionamento («comportamento») di molti prodotti dipende dal software e dai dati che risiedono sia nel prodotto che all'esterno dello stesso, e più esattamente nel c.d. cloud[64].

3. *La Risoluzione del Parlamento europeo del 16 febbraio 2017: finalità, caratteristiche e criticità*

La strategia europea in materia di robotica si differenzia rispetto alle precedenti dedicate alle tecnologie convergenti, poiché favorisce, fin dalle prime fasi di sviluppo, la predisposizione di una normativa *ad hoc* relativamente ai profili civilistici. Questo orientamento è stato accolto con molte perplessità dalla dottrina.

Ripercorro, brevemente, l'evoluzione della policy europea in materia. Nel 2013, sulla base di un progetto precedente

dei sistemi deriva dal fatto che i programmi devono essere considerati «within a range of categories as they undergo the transformation from "birth" as algorithms to execution as part of a computer. In addition, issues concerning the malfunction of programs or software are often tightly bound to issues involving hardware». Così M.C. Gemignani, *Product Liability and Software*, in *Rutgers Computer & Tech. L.J.*, 8, 1981, p. 173.

[63] Attorno all'IoT ruotano protocolli, piattaforme informatiche di interscambio e tecnologie abilitanti, le quali consentono di combinare funzioni di hardware, software, dati e servizi per ottenere nuovi prodotti in cui la componente «fisica» è connessa con quella intangibile. Gli intangibili collegati agli oggetti attraverso internet acquisiscono un plusvalore potenzialmente elevato, in funzione delle nuove prospettive di sfruttamento economico derivanti dal network. La connettività tra oggetti, il *network-web* (come piattaforma virtuale di interscambio) e gli intangibili rappresentano una leva di creazione di valore soprattutto se le risorse immateriali interagiscono tra di loro nell'ambito di un portafoglio sinergico di *Intellectual Property* (IP). Così rileva R.M. Visconti, *Internet delle cose, networks e plusvalore della connettività*, in *Dir. Industriale*, 6, 2016, p. 536.

[64] Sul fenomeno del *cloud computing* vedi il documento del Gruppo di lavoro per la protezione dei dati, Parere 5/2012 sul cloud computing, adottato il 1° luglio 2012, p. 5, consultabile all'indirizzo http://ec.europa.eu/justice/policies/privacy/index_en.htm.

di tre anni, la Commissione europea pubblicò il programma *RockEU Coordination Action*, con il quale favoriva gli studi sull'integrazione della robotica nella *day-to-day life* di utenti e imprese[65]. In seguito, fu pubblicata la *Strategic Research Agenda for Robotics in Europe 2014-2020*, accompagnata dalla *Multi-Annual Roadmap* (Mar), per affrontare i dettagli tecnici e di mercato[66].

I lavori per il documento in oggetto iniziano nel 2015, quando la Commissione giuridica del Parlamento europeo predispose un Progetto di relazione per un'azione in materia[67]. Esso è culminato, più tardi, nella pubblicazione della Risoluzione del 16 febbraio 2017, con la quale il Parlamento europeo ha recato raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica.

Si tratta di un documento fondato sull'art. 114 Tfeu di importanza strategica per l'Europa, poiché considera in maniera trasversale l'impatto della robotica: dai veicoli automobilistici (parr. 24-29); ai droni (par. 30); dai robot collaborativi (parr. 31-32), ai robot a scopo medicale (parr. 33-35). Proprio questa caratteristica è, però, già stata indicata come un aspetto di debolezza dalla dottrina che mette in guardia dal rischio di analisi generiche, prive di risvolti operativi. Ciò confermerebbe l'impossibilità di ragionare in termini di diritto unitario della robotica (vedi cap. I, par. 5)[68].

La Risoluzione offre indicazioni sul trattamento giuridico da riservare alle diverse questioni cruciali in futuro. Innanzitutto, appare di prim'ordine la necessità di definire l'oggetto, cioè: il robot.

[65] Il progetto è parte del Programma Horizon 2020.

[66] Sparc, *The Partnership for Robotics in Europe, Robotics 2020 Multi-annual Roadmap*, Horizon 2020 Call Ict-2017 (Ict-25, Ict-27 e Ict-28), il 2 dicembre 2016. Consultabile all'indirizzo https://www.eu-robotics.net/sparc/about/roadmap/index.html.

[67] Committee on legal affairs, *Draft Report with recommendations to the Commission on Civil Law Rules on Robotics*, 2015/2103/Inl, 31 maggio 2016.

[68] E. Palmerini, *Regulating Robotics in Europe: A Perplexed View*, in *Jusletter IT*, 23, 2017.

«Creare una definizione generalmente accettata di robot e di intelligenza artificiale che sia flessibile e non ostacoli l'innovazione» è esigenza espressa nelle parole introduttive della Risoluzione (punto C). Per questo, il Parlamento invita la Commissione a proporre definizioni comuni di sistemi ciberfisici, di sistemi autonomi, di robot autonomi intelligenti e delle loro sottocategorie, prendendo in considerazione le caratteristiche di un robot intelligente.

Sulla base di questa constatazione, diventa passaggio essenziale identificare la natura giuridica del robot, da cui dipende la disciplina applicabile e il relativo regime di sicurezza[69]. Il punto 59 lett. *E*) ed *F*) del documento avanza la proposta – già ampliamente criticata – di introdurre la nozione di «persona elettronica», per facilitare la registrazione, la gestione dei danni e la predisposizione di un adeguato sistema assicurativo. Tuttavia, perché lo sforzo definitorio sia funzionale all'individuazione di regole operative, non è sufficiente considerare le caratteristiche che determinano un robot (autonomia, capacità di autoapprendimento ecc.). Piuttosto, a partire da queste, e in base ai diversi livelli di ognuna di tali caratteristiche, la distinzione in sotto-categorie è fondamentale al fine di disciplinarli. D'altro canto, l'industria e i ricercatori stessi si stanno già muovendo in questo senso, proponendo diverse tassonomie basate sulle conseguenze funzionali di applicazioni aventi diversi livelli di autonomia. Gli esempi forniti dall'industria automobilistica e dalla chirurgia robotica sono significativi (cap. II, parr. 3.1 e 7).

La *robot liability* costituisce il *trait d'union* dei vari temi e problemi giuridici affrontati nel documento. Oggi, anche tale aspetto deve essere considerato alla luce del più ampio quadro di riferimento composto dai documenti della Com-

[69] Il Parlamento europeo afferma che «più i robot sono autonomi, meno possono essere considerati come meri strumenti nelle mani di altri attori (quali il fabbricante, l'operatore, il proprietario, l'utilizzatore ecc.)» (Risoluzione, lett. AB). In realtà, tale assunto è già stato ampiamente criticato in dottrina, poiché questa caratteristica non sembrerebbe, in ogni caso, legittimare l'attribuzione al robot di una natura giuridica diversa da quella di prodotto.

missione europea e dell'Oecd, pubblicati successivamente alla Risoluzione.

A una prima lettura, il documento sembra intriso di tentativi volti a mantenere un equilibrio tra rispetto della sicurezza e regole che incentivano, o quanto meno non ostacolano, l'innovazione. In tema di normazione, sicurezza e protezione, il punto 22 evidenzia che la questione definitoria delle norme e dell'interoperabilità è fondamentale nell'ambito delle tecnologie di robotica e di AI. Per questo, viene incentivato il processo continuo di armonizzazione delle norme tecniche. In particolare, è auspicabile che ciò sia fatto in coordinamento con gli organismi europei di normazione e con l'Organizzazione internazionale di normazione.

A tal proposito, anche l'istituzione di un'Agenzia europea robotica potrebbe giocare un ruolo chiave nello stabilire standard di sicurezza sovranazionali.

Parlare di sicurezza implica anche affrontare il problema relativo alla necessità di testare i robot in condizioni reali, in particolare nelle città e sulle strade, per individuare gli eventuali rischi connessi, i modi di gestione più efficaci degli stessi, nonché il loro sviluppo tecnologico successivo alla fase puramente sperimentale di laboratorio. Questo, però, fa ipotizzare numerosi problemi: lentezza nei collaudi; problemi di monitoraggio; e il controllo del test, tanto che il Parlamento europeo invita la Commissione a elaborare criteri uniformi in tutta l'Unione per identificare le aree in cui autorizzare i collaudi dei robot.

Il documento affronta, poi, i problemi connessi all'impatto dei robot sui principi costituzionali della dignità, uguaglianza, libertà e autodeterminazione e la protezione dei dati personali.

In sintesi, la proposizione di un intervento unitario potrebbe favorire eccessivamente la robotica rispetto ad altri contesti tecnologici, ovvero ostacolarla completamente. In altre parole, tale opzione regolatoria – peraltro difficilmente praticabile – minerebbe il principio di «neutralità tecnologica», secondo il quale la regolamentazione non dovrebbe discriminare talune tecnologie a favore di altre e, allo stesso

tempo, non dovrebbe nemmeno creare condizioni eccessivamente favorevoli per alcune di esse[70].

3.1. *La robotica nelle fonti europee: tra «hard law», «soft law» e «self regulation»*

In associazione alla promozione di strumenti legislativi, a cui rinvia il punto 65 della Risoluzione invitando la Commissione a presentare una proposta di Direttiva relativa a norme di diritto civile sulla robotica[71], sono numerosi gli input che lo stesso documento offre per l'implementazione di strumenti non legislativi[72], necessari ad approntare una disciplina flessibile e funzionale a favorire la partecipazione degli stakeholder.

Si tratta di strumenti sia di *soft law* che di *self regulation*. La differenza principale sta nel loro rispettivo rapporto con l'*hard law*: mentre i primi si fondano sul processo partecipativo (es. raccomandazioni); i secondi, sostanzialmente, indicano una categoria di atti proposti dalle associazioni di categoria (es. codici di condotta). Entrambi sono già ampiamente utilizzati per le tecnologie emergenti, anzi va constatato che il modello di governance affermatosi in Europa è caratterizzato dall'interazione tra la normativa giuridica, una serie

[70] B.J. Koops, *Should Ict Regulation be Technology-Neutral?*, in B.J. Koops, M. Lips, C. Prin e M. Schellenkens (a cura di), *Starting Points for Ict Regulation. Deconstructing Prevalent Policy One-liners*, The Hague, T.M.C. Asser Press, 2006, pp. 77-108. Il principio è recepito anche a livello legislativo: nel contesto italiano, per esempio, nella disciplina delle reti e dei servizi di comunicazione elettronica, esso è espresso dall'art. 4 del d.lgs. 259/2003.

[71] Al punto 51 la Risoluzione chiede alla Commissione di presentare, sulla base dell'art. 114 Tfue una proposta di atto legislativo sulle questioni giuridiche relative allo sviluppo e all'utilizzo della robotica e dell'AI prevedibili nei prossimi 10-15 anni.

[72] G.E. Marchant, *Soft Law: New Tools for Governing Emerging Technologies*, in *Bulletin of the Atomic Scientists*, 2, 2017, pp. 108-114. Esiste un numero assai esteso di contributi dottrinali sulle caratteristiche strutturali. Tra i tanti, si rinvia a U. Morth, *Soft Law in Governance and Regulation: An Interdisciplinary Analysis*, Cheltenham, Edward Elgar, 2004.

di strumenti di *soft law*, e la cooperazione di diversi attori (pubblici come autorità governative, soggetti privati, quali Ong, imprese, multinazionali)[73]. Basti pensare alla strategia sicura, integrata e responsabile per le nanoscienze e nanotecnologie della Commissione europea[74], o al Codice di condotta per una ricerca responsabile nel settore delle nanoscienze e nanotecnologie, divenuto un vero e proprio prototipo di codice in materia[75]. Anche la biologia sintetica è un esempio: a essa non sono ancora dedicati atti legislativi, i primi dibattiti negli Stati Uniti hanno prediletto l'impiego delle tecniche in parola[76]. Nel maggio del 2006, a Berkley, più di 300 ricercatori, rappresentanti governativi, politici, bioeticisti, economisti, psicologi, antropologi, filosofi e membri della stampa si radunarono in una conferenza, *Synthetic Biology 2.0*, per discutere i futuri sviluppi della biologia sintetica, e in quella sede i delegati adottarono una Dichiarazione per modelli di governance inclusiva, basati su strumenti di *self-regulation*[77].

[73] Il ricorso alla *soft law* può favorire anche la concretizzazione di valori e principi (ad esempio, il principio di precauzione e i diritti umani) e a dar loro attuazione attraverso meccanismi che possono ottenere risultati più incoraggianti degli strumenti di *hard law*, per quanto risultino sostanzialmente informali e operino solo su base volontaria. Vedi *amplius*: D. Ruggiu, *Diritti e temporalità. I diritti umani nell'era delle tecnologie emergenti*, Bologna, Il Mulino, 2012, p. 158; e D. Ruggiu e E. Pariotti, *Governing Nanotechnologies in Europe: Human Rights, Soft Law, and Corporate Social Responsability*, in H. Van Lente, C. Coenen, K. Konrad, L. Krabbenborg, C. Milburn, F. Seifert, F. Thoreau e T. Zulsdorf (a cura di), *S. Net 2011 Conference Volume*, Heidelberg, Ios press (Aka).

[74] Commissione europea, Comunicazione del 12 maggio 2004, *Verso una strategia europea a favore delle nanotecnologie*, Com(2004) 338 def che ha una funzione prelegislativa e si articola in una serie di atti inquadrabili nella categoria di *soft law*.

[75] Commissione europea, *Raccomandazione per un Codice di condotta per una ricerca responsabile nel settore delle nanoscienze e nanotecnologie*, cit.

[76] E. Stokes, *Recombinant Regulation: EU Executive Power and Expertise in Responding to Synthetic Biology*, in M. Weimer e A. De Rujter, *Regulating Risk in the European Union. The Co-production of Expert and Executive Power*, Oxford, Hart Publishing, 2017, pp. 59-81.

[77] *Declaration of the Second International Meeting on Synthetic Biology*, 29 maggio 2006, consultabile all'indirizzo http://syntheticbiology.org/SB2Declaration.html.

La regolamentazione della robotica è materia posta nella zona di intersezione tra l'area di operatività del *soft law* e quella di *self-regulation*[78], e la relazione tra norme tecniche ed etiche emerge chiaramente nel campo del *soft law*[79].

Pensando alla robotica, sia come strumento di regolamentazione che come oggetto in sé e per sé da regolamentare, e riferendosi, quindi, a una vasta gamma di applicazioni, si profilano due considerazioni. La prima: le norme implicano la circolazione di valori etico-sociali, i quali emergono dalla sfera privata[80]. I problemi di sicurezza per la persona che si relaziona con il robot da compagnia presuppongono una riflessione più approfondita sul ruolo dei governi come garanti dei valori costituzionalmente tutelati entro i cambiamenti tecnoscientifici.

La seconda considerazione è la seguente: con il *soft law* si orientano scelte fondamentali sottese all'introduzione delle tecnologie robotiche, ma lo stesso non può disciplinare altri tipi di problemi, per i quali la robotica diventa «oggetto» stesso del problema giuridico da risolvere, come nel caso dello *human enhancement*. Per definire giuridicamente il risultato dell'integrazione tra persona e tecnologia (es. *cyborg*), gli standard rimangono degli strumenti cui il giudice potrebbe solo ispirarsi, essendo la materia relativa a diritti fondamentali[81].

Tra i documenti di *self-regulation*, la Risoluzione promuove il codice etico-deontologico degli ingegneri robotici, il quale mira a essere una guida cui i professionisti possono ispirarsi nello svolgere la loro attività. La Risoluzione confi-

[78] E. Stradella, *Approaches for Regulating Robotic Technologies: Lessons Learned and Concluding Remarks*, in E. Palmerini e E. Stradella, *Law and Technology. The Challenge of Regulating Technological Development*, Pisa, Pisa University Press, 2013, pp. 335-358.

[79] *Ibidem*, p. 338.

[80] O. Dawn, *Common Values and the Public-private Divide*, London, Butterworths, 1999; A. McHarg, *The Constitutional Dimension of Self-regulation*, in F. Cafaggi, *Reframing Self-regulation in European Private Law*, Alphen aan del Rijn, Kluwer, 2006.

[81] Stradella, *Approaches for Regulating Robotic Technologies*, cit., p. 356.

gura un quadro etico di orientamento per la progettazione, i protocolli, la produzione e l'uso di robot, a integrazione delle raccomandazioni e dell'*acquis* nazionale e dell'Unione già esistente. L'etica, o nella specie la roboetica, ha assunto un'importanza centrale, anche a livello domestico, con il rapporto pubblicato dal Comitato nazionale di bioetica (Cnb). D'altro canto, «la volontà costante di integrare scienza e valori rappresenta il tratto più caratteristico dell'identità epistemica europea, la peculiare cifra della politica e del diritto della scienza in Europa»[82].

È significativo il fatto che una specifica commissione *ad hoc* del Ministero dei Trasporti tedesco abbia stilato delle linee guida per i principi etici a cui ispirare il *design* del software delle *self-driving cars*. Ciò significa, per esempio, che le auto a guida automatizzata dovranno essere programmate per «accettare» di provocare danni ad animali o cose, qualora questo sia necessario a evitare un infortunio a una persona; esse non potranno in nessun caso fare distinzione tra le persone secondo criteri di età, sesso e costituzione fisica.

La riflessione in materia suggerisce l'introduzione dello studio dell'etica nei corsi di ingegneria e informatica[83]. L'integrazione di studi interdisciplinari nei curricula universitari pare un'esigenza crescente al fine di comprendere i problemi dell'AI, della robotica e delle tecnologie digitali emergenti. Vengono, per esempio, incentivati corsi di «diritto, psicologia e AI».

3.2. *La centralità delle norme tecniche: rinvio*

Rodotà aveva osservato che «la diffusione della robotica, come già avvenuto con l'elettronica, porta a una concentra-

[82] M. Tallacchini, *Politiche della scienza contemporanea: le origini*, in S. Rodotà e M. Tallacchini (a cura di), *Trattato di Biodiritto. Ambito e fonti del Biodiritto*, Milano, Giuffrè, 2010, pp. 53-79.

[83] A tal riguardo indicazioni si trovano nella Comunicazione della European Commission, *Artificial Intelligence for Europe*, cit., p. 13 del documento.

zione del potere nelle mani di soggetti che ne controllano la dimensione tecnica»[84].

In effetti, la creazione di standard tecnici internazionali applicabili alla robotica rappresenta, almeno in parte, una risposta al problema dell'obsolescenza delle norme: gli standard rispondono «più velocemente» agli adattamenti necessari per cogliere le nuove caratteristiche tecniche-funzionali, adeguando i metodi di valutazione del *risk assessment* alle nuove applicazioni.

Va notato che potrebbe non essere un'operazione semplice la predisposizione di standard per la robotica avanzata, a causa di un aspetto in via di implementazione nella ricerca: l'autoapprendimento.

In un'ottica *ex post* è verosimile che questa caratteristica contribuisca a configurare con frequenza l'ipotesi di danno da prodotto conforme agli standard di sicurezza legislativi[85].

Il ruolo delle norme tecniche è trattato unitariamente all'analisi dei profili di responsabilità civile nel capitolo II.

3.3. *I modelli giuridici orientali quali fonte di ispirazione della Risoluzione*

Nel passare in rassegna i problemi emergenti associati alla robotica e le linee di sviluppo degli interventi giuridici, i redattori della Risoluzione guardano sia alle iniziative degli Stati membri, sia alle iniziative che hanno avuto luogo in altri contesti giuridici, nonché al loro coordinamento. Molti paesi, nel corso del 2017, hanno avviato studi previsionali per analizzare l'impatto dell'AI sulle leggi in vigore (incluse quelle in materia di proprietà intellettuale e responsabilità) e per capire, eventualmente, come aggiornarle. Alcuni, tra questi sono, già da diverso tempo, competitivi in materia

[84] S. Rodotà, *Dall'umano al postumano*, in S. Rodotà (a cura di), *Vivere la democrazia*, Bari, Laterza, 2018, p. 142.

[85] Il problema è ampliamente trattato, anche in chiave comparatistica da Al Mureden, *La sicurezza dei prodotti e la responsabilità del produttore. Casi e materiali*, cit., p. 3.

robotica, poiché rispetto a quanto avvenuto altrove, essi hanno avviato con anticipo la riflessione giuridica: si tratta, *in primis* dei paesi dell'Est asiatico, come Giappone, Cina e Corea del Sud, i quali hanno già introdotto i robot nei contesti quotidiani[86].

Nell'economia di queste pagine, posso solo accennare alle iniziative avviate negli ordinamenti richiamati, poiché il tema meriterebbe ben più ampia trattazione, anche per cogliere fino a che punto le differenze storico-culturali influiscono sul modo di regolamentare il progresso. Di certo, l'avanguardia giapponese nella produzione di robot in generale, e in special modo di umanoidi, è stata favorita dal credo shintoista che attribuisce un'anima a tutte le cose. Per questo motivo, lungi dall'essere il ritratto di Frankenstein come accade in Occidente[87], i robot sono considerati «compagni» del cittadino giapponese[88].

L'esperienza nipponica ha un ruolo chiave. Il governo nipponico ha supportato costantemente i successi dell'industria robotica, che rappresentano un terzo di quella globale, incentivando così l'avvio di riflessioni giuridiche in anticipo rispetto a quanto avvenuto altrove. I robot collaborativi e delle macchine a guida automatizzata rappresentano i principali settori di investimento[89]. Dal 2012, il Giappone

[86] Così osserva R. Calo, *Open Robotics*, in *Md. L. Rev.*, 70, 2011, p. 571.

[87] I. Asimov, *The Machine and the Robot*, in *Science Fiction: Contemporary Mythology*, 1978, pp. 250-253.

[88] Le stesse propensioni culturali (*biases*) alla base delle differenze globali sul modo di considerare i robot indicano che, entro il medesimo contesto culturale, tali attitudini «si polarizzano» nelle direzioni descritte. Leenes, Palmerini, Koops, Bertolini, Salvini e Lucivero, *Regulatory Challenges of Robotics*, cit., p. 21.

[89] Per una dettagliata analisi delle iniziative politiche e delle questioni giuridiche in materia di macchine a guida automatizzata relative al territorio giapponese si rinvia a T. Matsuo, *The Current Status of Jananese Robotics Law: Focusing on Automated Vehicles*, in E. Hilgendorf e U. Seidel (a cura di), *Robotics, Autonomics, and the Law. Legal Issues Arising from the Autonomics for Industry 4.0 Technology Programme of the German Federal Ministry for Economic Affairs and Energy*, Baden-Baden, Nomos, 2017, p. 151.

promuove standard di sicurezza per i robot collaborativi[90], dato il ruolo assunto dagli umanoidi e i frequenti contatti che essi hanno con le persone. Dal 2003, invece, sono utilizzate le *Tokku*, ossia le zone speciali, entro le quali vengono testati i robot in condizioni ambientali reali.

Nel 2014, il Giappone ha inaugurato la *Robot Revolution Initiative*[91]: una strategia che promuove la competitività del paese, sia attraverso tecniche di regolamentazione, sia attraverso forme di *deregulation*.

L'esteso documento individua tre pilastri a basamento della c.d. *robot barrier-free society*, una società cioè in cui uomo e robot coesistono e cooperano, al fine di: 1) potenziare la capacità creativa dei robot; 2) assumere un ruolo leader nel campo della robotica; 3) predisporre una strategia per una nuova era robotica.

Il governo giapponese ha riconosciuto che le tecniche in vigore per la protezione di *cybersecurity* e *safety* sono insufficienti per identificare e gestire i potenziali rischi di danni derivanti dall'utilizzo dei robot. Per questo, la strategia prevede l'adozione di una standardizzazione globale, in modo che i robot giapponesi non siano sistemi isolati, ma dotati di hardware e software compatibili e interconnessi a infrastrutture comuni. Se, in passato, l'adozione di standard comuni è stata promossa dalle associazioni di categoria giapponesi, ora gli standard Iso hanno assunto un ruolo chiave. Il Giappone ha istituito il *Council for a Robot Revolution*

[90] Cfr. C. Harper e G. Virk, *Towards the Development of International Safety Standards for Human Robot Interaction*, in *Int'l J. Social Robotics*, 2, 2010, pp. 231-232, consultabile all'indirizzo http://www.springerlink.com/content/k6r222j243303912/. L'implementazione di tali standard con riguardo ai robot collaborativi non è stata semplice, complice il background giuridico nipponico in materia di responsabilità da prodotto. Per una lettura sul tema si rinvia a M.A. Behrens e D.H. Raddock, *Japan's New Product Liability Law: The Citadel of Strict Liability Falls, but Access to Recovery Is Limited by Formidable Barriers*, in *U.Pa.J. Int'l Bus. L.*, 16, 1995, p. 669.

[91] Si tratta della The Headquarters for Japan's Economic Revitalization, *New Robot Strategy, Japan's Robot Strategy – Vision, Strategy, Action Plan*, 10 febbraio 2015, consultabile all'indirizzo http://www.meti.go.jp/english/press/2015/pdf/0123_01b.pdf.

Initiative (paragrafo 1 del documento), un centro di controllo con la funzione di garantire le informazioni necessarie per collaborare nella formulazione di standard internazionali, incentivandone l'adozione per i robot e i dispositivi interconnessi e interoperativi. Infine, i robot costituiscono una pietra miliare del piano «Society 5.0» che sulla base dello sviluppo tecnologico implementato con il piano «Industry 4.0», si propone ora di guardare oltre, per costruire una *smart society*[92].

L'ordinamento in esame dimostra grande apertura verso la costruzione di un quadro regolatorio internazionale per la cooperazione Giappone-Europa. È la stessa strategia giapponese a richiamare quella europea, quale modello di riferimento, esprimendo la necessità di andare oltre il miglioramento dell'accessibilità agli standard, per assicurare la competitività dell'industria robotica.

Analoghi intenti si trovano nelle iniziative di altri paesi orientali. Il governo coreano ha già adottato varie leggi in materia di robotica, dimostrando di accogliere i suggerimenti di statisti e politologi i quali, rispetto al problema della decrescita demografica e dell'invecchiamento della popolazione, hanno identificato nei robot collaborativi, o domestici, una soluzione alle esigenze sociali. L'*Intelligent Robots Development and Distribution Promotion Act* del 2010 ha predisposto un piano per lo sviluppo dell'industria robotica e per promuovere la sicurezza, e così il *basic plan for an intelligent robot*, pubblicato sulla base dell'art. 5 dello stesso Act. Sono molte anche le iniziative legislative in settori specifici: nel 2016, per esempio, il *Moto Vehicle Management Act* definì le auto a guida autonoma (art. 2); l'*Aviation Act* ha introdotto il concetto di drone. La *Korean Food and Drug Administration* (Kfda) sta discutendo se qualificare il robot intelligente biomedicale alla stregua di

[92] Il piano «Society 5.0» giapponese è stato proposto nel corso del 5th Science and Technology Basic Plan, marzo 2017, come progetto nazionale dal primo ministro giapponese il quale ha espresso la volontà di «realize a future, where people's lives and society are optimized by making full use of innovative technologies such as IoT, AI, robots, and Big Data».

un dispositivo medico, includendolo nel *Medical Device Act*, e tenendo conto che, in base al diritto coreano e all'interpretazione della Suprema corte coreana[93], il software non è un bene mobile ai sensi della normativa sulla responsabilità da prodotto, analogamente a quanto accade al programma informatico e alle informazioni archiviate[94].

Con il piano *Made in China 2025* adottato il 7 luglio 2015[95], e ispirato direttamente al piano tedesco «Industrie 4.0» del 2013[96], Pechino si è posta obiettivi ambiziosi: produrre il 70% dei robot industriali impiegati entro il proprio territorio; l'80% delle macchine ibride o a guida automatizzata; il 70% dei dispositivi medici avanzati, l'80% dei componenti per macchinari tecnologicamente avanzati. Inoltre, nel dicembre del 2016, il Consiglio di Stato cinese ha introdotto un piano quinquennale per finanziare e promuovere tecnologie emergenti, come il *cloud computing* e l'IoT.

4. *La normativa europea applicabile alla robotica: riferimenti a carattere orizzontale*

È operazione preliminare la ricerca di riferimenti regolatori applicabili, in modo trasversale, ai prodotti robotici. Accettando la definizione di robot quale mero artefatto

[93] Così nell'esperienza giurisprudenziale della Suprema corte coreana n. 745 del 12 aprile 2002.

[94] Conseguentemente, i consumatori danneggiati dal malfunzionamento di un programma non possono ottenere alcun riconoscimento e risarcimento del danno in base alla normativa sulla responsabilità da prodotto. L'impiego di AI acuirà tale questione, per questo il governo coreano sta ipotizzando di introdurre un emendamento in materia di responsabilità del produttore.

[95] Il piano è disponibile all'indirizzo: http://english.gov.cn/2016special/madeinchina2025/.

[96] L'espressione «Industrie 4.0» è stata introdotta dal Ministero federale dell'eduzione e della ricerca e dal Ministero federale dell'economia e della tecnologia per indicare la quarta rivoluzione industriale orientata alla produzione intelligente. «Quarta» poiché successiva a quella della macchina a vapore (Prima), della produzione di massa (Seconda), elettronica e digitale (Terza). Cfr. Roth, *Industrie 4.0 – Hype oder Revolution?*, *Einführung und Umsetzung von Industrie 4.0*, 2016, p. 5.

meccanico, il quadro di *hard law* europeo che viene in esame è quello funzionale ad assicurare standard minimi di sicurezza per la messa in commercio.

Pensando allo smartphone, esempio di robot tele-operato[97], la prima analogia si delinea tra robot e macchina, in virtù dell'esteso ambito di applicazione della Direttiva 2006/42/CE del Parlamento europeo e del Consiglio del 17 maggio 2006 relativa alle macchine[98]. Con i termini «macchina» e «quasi-macchina»[99], gli artt. 1 e 2 includono prodotti che presentano delle parti o delle componenti collegate tra loro in un insieme. La Direttiva sulle macchine è stata recentemente oggetto di valutazione avviata dalla Commissione europea[100],

[97] È il robot composto da un set di parti mosse da motori controllati da persone fisiche tramite specifiche interfacce. In base al glossario tecnico della *Strategic Research Agenda (Sra) for Robotics in Europe*, consultabile all'indirizzo https://www.eu-robotics.net/cms/upload/topic_groups/SRA2020_SPARC.pdf.

[98] 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.

[99] In base all'art. 2 lett. *a*) si definisce «macchina»: «– insieme equipaggiato o destinato ad essere equipaggiato di un sistema di azionamento diverso dalla forza umana o animale diretta, composto di parti o di componenti, di cui almeno uno mobile, collegati tra loro solidamente per un'applicazione ben determinata, – insieme di cui al primo trattino, al quale mancano solamente elementi di collegamento al sito di impiego o di allacciamento alle fonti di energia e di movimento insieme di cui al primo e al secondo trattino, pronto per essere installato e che può funzionare solo dopo essere stato montato su un mezzo di trasporto o installato in un edificio o in una costruzione, – insiemi di macchine, di cui al primo, al secondo e al terzo trattino, o di quasi-macchine, di cui alla lett. *g*), che per raggiungere uno stesso risultato sono disposti e comandati in modo da avere un funzionamento solidale, – insieme di parti o di componenti, di cui almeno uno mobile, collegati tra loro solidalmente e destinati al sollevamento di pesi e la cui unica fonte di energia è la forza umana diretta». La lett. *g*) art. 2, invece, definisce «quasi-macchine»: «insiemi che costituiscono quasi una macchina, ma che, da soli, non sono in grado di garantire un'applicazione ben determinata. Un sistema di azionamento è una quasi-macchina. Le quasi-macchine sono unicamente destinate ad essere incorporate o assemblate ad altre macchine o ad altre quasi-macchine o apparecchi per costituire una macchina disciplinata dalla presente Direttiva».

[100] Consultabile all'indirizzo http://ec.europa.eu/growth/sectors/mechanical-engineering/machinery_en.

il cui esito ha indicato che alcune disposizioni dovrebbero essere oggetto di emendamento poiché non contemplano, espressamente, l'impiego di tecnologie digitali nei macchinari.

Il quadro è, poi, composto dalle normative in materia di sicurezza e tutela dei consumatori, e cioè dalla Direttiva 2001/95/CE del Parlamento europeo e del Consiglio del 3 dicembre 2001 relativa alla sicurezza generale dei prodotti[101], aggiornata dal pacchetto sulla sicurezza varato con la Comunicazione della Commissione del 2013[102]; dalla Decisione 768/2008/CE relativa a un quadro comune per la commercializzazione dei prodotti; dal Regolamento 765/2008/CE[103]; dalla Direttiva sulla responsabilità del produttore per prodotto difettoso; e dalla Direttiva 99/44/CE sulla vendita dei beni di consumo. Con riferimento, poi, all'impiego di AI si deve includere anche la Direttiva 2014/53/EU sulle apparecchiature radio[104], poiché, infatti, un *Expert Group on Reconfigurable Radio Systems* collabora, attualmente, con la Commissione per valutare la possibilità di adottare uno o più atti funzionali ad affrontare la questione della connettività entro l'ambito della Direttiva in parola (*ex* art. 3(3)).

Ai nostri fini, ci soffermiamo sulla disciplina della sicurezza osservando, innanzitutto, che si realizza attraverso l'ampio ricorso a clausole generali, con le quali vengono indicati i requisiti essenziali di sicurezza, ovvero gli obiettivi da conseguire ma non le modalità, le quali vanno adattate al singolo prodotto o all'operatività concreta della macchina.

[101] In *GU* L, 11/4, del 15 gennaio 2002.

[102] *Comunicazione della Commissione Pacchetto sicurezza dei prodotti e vigilanza del mercato*, 13 febbraio 2013, Com(2013) 74 final.

[103] Regolamento (CE) 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il Regolamento (Cee) 339/93.

[104] 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.

Il pacchetto «sicurezza dei prodotti e vigilanza del mercato»[105], adottato dalla Commissione quale insieme di misure volte a semplificare e rendere più omogenee le norme applicabili ai prodotti non alimentari conferma la tendenza verso l'adozione di un nuovo indirizzo metodologico per la formazione di un quadro di regole ordinate secondo principi e precetti di portata generale e uniformi, come già avviene per altre materie del diritto privato europeo[106]. La sicurezza ha un carattere transfrontaliero, e come la precedente Direttiva (Dsgp), la proposta di nuovo Regolamento impone determinati obblighi agli operatori economici e cerca, al contempo, di razionalizzare e semplificare le interazioni tra il Regolamento e la legislazione dell'UE.

È opportuno notare che, in linea di continuità con quanto avvenuto per l'adozione dell'attuale Dsgp, la base giuridica rimane l'art. 114 Tfue relativo all'istituzione del funzionamento del mercato interno. Questa scelta è stata, in un primo tempo, identificata dalla dottrina come «un'occasione persa», in quanto, a tale disposizione, si sarebbe potuta affiancare quella di cui all'art. 169 Tfue per la tutela della salute[107]: l'accesso a prodotti sicuri gioca, infatti, un

[105] Il pacchetto comprende: *i*) una proposta di nuovo Regolamento sulla sicurezza dei prodotti di consumo; *ii*) una proposta di Regolamento unico sulla vigilanza del mercato dei prodotti nell'Unione europea – Com(2013) 76 del 13 febbraio 2013 – che enuclea 20 azioni concrete da realizzare entro il 2015 per migliorare la vigilanza del mercato nell'ambito del quadro normativo attuale e fino all'entrata in vigore delle nuove norme; *iii*) la comunicazione «prodotti più sicuri e conformi per l'Europa», che delinea un piano pluriennale per la vigilanza del mercato (Com(2013) 74 del 13 febbraio 2013); *iv*) una relazione sull'attuazione del Regolamento (CE) 765/2008, compresa una valutazione finanziaria che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e abroga il Regolamento (CE) 339/93 del Consiglio – Com(2013) 77 del 13 febbraio 2013.

[106] Un chiaro esempio è fornito dal diritto alimentare. Tra i tanti si rinvia a F. Casucci e P. Saccomanno, *Il diritto agroalimentare*, in G.A. Benacchio e F. Casucci (a cura di), *Temi e istituti di diritto privato dell'Unione Europea*, Torino, Giappichelli, 2017, pp. 67-85, spec. p. 75.

[107] La lacuna è stata messa in evidenza da M.E. Arbour, *Securitè des produits, sante des consommateurs, responsabilites et constitutions: synergies compares*, in *McGill J.L. & Health*, 7, 2013-2014, pp. 169, 176. Va, però,

ruolo essenziale nella tutela della salute, ed ecco perché i beni giuridici tutelati dalle disposizioni risultano inestricabilmente connessi[108]. I progressi tecnoscientifici intensificano il legame tra gli obiettivi di protezione dei consumatori (art. 38 della Carta) e di tutela della salute (art. 35 della Carta dei diritti fondamentali dell'UE). D'altro canto, sebbene l'Unione europea si limiti a una competenza di sostegno in materia di tutela della salute, di fatto tale tutela è inclusa nell'azione comunitaria e incide in modo determinante sulla definizione e l'attuazione di tutte le altre politiche e azioni, in sintonia con la natura trasversale del diritto alla salute[109].

Il testo della proposta di Regolamento non è, tuttavia, rimasto insensibile alle critiche. È stato, infatti, modificato per chiarire che: «la proposta è basata sull'articolo 114 del Tfue, al quale si riferisce anche l'articolo 169 del Tfue, al fine di garantire un livello elevato di protezione della salute e della sicurezza di tutti i consumatori europei e l'instaurazione di un mercato interno dei beni di consumo». Viene, così, messo in luce che la normativa sulla sicurezza generale dei prodotti deve contribuire al raggiungimento degli obiettivi di cui all'art. 169 del Tfue (considerando 3), e che vi è, pertanto, ancora bisogno di un quadro legislativo orizzontale che colmi le lacune esistenti e assicuri la protezione dei consumatori non altrimenti garantita.

dato conto che il punto 3 della proposta di Regolamento («elementi giuridici della proposta») esplicita il legame tra gli obiettivi di tutela del mercato unico e della salute, laddove afferma che «nell'ambito del mercato interno, in cui i prodotti possono circolare liberamente, disposizioni efficaci sulla sicurezza dei prodotti possono essere adottate solo a livello dell'Unione. Si tratta di un approccio necessario per assicurare un elevato livello di protezione dei consumatori (in linea con l'articolo 169 del Tfue), nonché per impedire agli Stati membri di adottare norme diversificate sui prodotti che comporterebbero un'ulteriore frammentazione del mercato unico».

[108] I. Benöhr, *EU Consumer Law and Human Rights*, Oxford, Oxford University Press, 2013, p. 74.

[109] Vedi *amplius* F. Casucci e S.F. Fusco, *La tutela della salute umana*, in G.A. Benacchio e F. Casucci (a cura di), *Temi e istituti di diritto privato dell'Unione Europea*, Torino, Giappichelli, 2017, pp. 155 ss.

A ogni buon conto, si tratta di una regolamentazione «a geometria variabile» della sicurezza, composta, cioè, da meccanismi eterogenei e operanti su una dimensione multilivello lungo tutto l'intero ciclo di vita del prodotto. La definizione di specifiche tecniche o qualitative volontarie, alle quali prodotti, processi di produzione o servizi attuali o futuri possono conformarsi sarà resa più critica dalle caratteristiche della robotica avanzata (vedi *infra* cap. II, par. 3)[110].

4.1. *La Direttiva sulla responsabilità da prodotto difettoso e la realtà che cambia*

Anche la disciplina europea sulla responsabilità da prodotto difettoso ha un carattere trasversale e risulta, quindi, in linea di principio, applicabile a tutti i prodotti robotici. La necessità di rivedere il testo per adattarlo, ovvero studiarne una versione c.d. *Liability 2.0*, si ravvisa in due iniziative parallele.

Da un lato, la consultazione pubblica relativa alla costruzione di una *European Data Economy* indica la necessità di rivedere aspetti di responsabilità, dall'altro la Commissione europea ha lanciato un'altra consultazione pubblica per la valutazione della Direttiva 85/374/Eec sulla responsabilità da prodotto difettoso[111], allo scopo di raccogliere pareri circa le seguenti questioni: *i*) se, e fino a che punto, il regime di responsabilità oggettiva soddisfi ancora l'obiettivo di garantire un adeguato livello europeo di tutela per danni da

[110] L'obiettivo è espresso dal Regolamento (UE) 1025/2012 del Parlamento europeo e del Consiglio del 25 ottobre 2012 sulla normazione europea, che modifica le Direttive 89/686/Cee e 93/15/Cee del Consiglio nonché le Direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/Cee del Consiglio e la decisione 1673/2006/CE del Parlamento europeo e del Consiglio, in *GU L*, 316/12, del 14 novembre 2012.

[111] Tutte le notizie sono consultabili all'indirizzo http://ec.europa.eu/growth/content/public-consultation-rules-liability-producer-damage-caused-defective-product-0_en.

prodotto difettoso; *ii*) se risponde alle esigenze indicate dagli esperti; *iii*) se risolva, adeguatamente, i problemi connessi allo sviluppo tecnologico.

Come delineato dall'Oecd (vedi par. 2), sono molti i profili di responsabilità connessi, soprattutto, all'emergere dell'IoT: essa implica una sofisticata interdipendenza tra una varietà di «cose», oggetti fisici, software, infrastruttura internet, e una varietà di attori coinvolti, fabbricatori del prodotto, fabbricatori dei sensori, produttori del software, fornitori dell'infrastruttura, inclusi gli utenti finali, e ogni altro soggetto che interviene nella vendita dei diversi servizi in questo *environment*. Ciò complica, naturalmente, l'individuazione dei molteplici soggetti che potrebbero essere ritenuti responsabili per danno o malfunzionamento del prodotto.

Distribuire le responsabilità, in un così intricato ecosistema, è poi un'operazione complicata dalla diversificata composizione dei prodotti: *a*) parti tangibili e dispositivi (sensori, attuatori, hardware); *b*) diverse componenti del software e applicazioni; *c*) i dati stessi; *d*) i servizi *e*) la connettività[112].

Così, per esempio, la qualità e disponibilità dei dati diventa essenziale per il buon funzionamento dei prodotti. Dati errati o alterati (per esempio, per un problema di connettività o di attacco hacker) potrebbero essere causa del malfunzionamento del sistema.

La composizione e il funzionamento dei prodotti dell'IoT ripropongono la questione della combinazione tra prodotto e servizio, e conseguentemente della sovrapposizione dei diversi regimi di disciplina cui soggiacciono. Se, dunque, la fornitura di dati attraverso l'IoT è considerata un servizio, i problemi correlati al malfunzionamento non rientrano nell'ambito di applicabilità del regime di responsabilità da prodotto, e ciò potrebbe far pensare che il corrente sistema

[112] Fin quando i dispositivi associati all'IoT, e pertanto connessi, sono qualificati come beni mobili, sono prodotti che rientrano nell'ambito di operatività della Direttiva sulla responsabilità da prodotto difettoso.

non risponda, in modo idoneo, ai nuovi problemi che si profilano[113].

Al termine della consultazione, la Commissione ha preannunciato che pubblicherà un documento guida interpretativo per chiarire i concetti della Direttiva. Le questioni di responsabilità saranno analizzate dalla Commissione con l'ausilio dell'Expert Group on Liability, il quale dovrà considerare anche quali diversi approcci adottare tra quelli indicati dalla comunicazione *Building a European Data Economy*. Qualora, invece, un nuovo intervento regolatorio sia considerato necessario, dovrà esserne, altresì, discussa l'attribuzione della natura orizzontale o settoriale.

5. *I riferimenti verticali: le discipline di settore*

Nella parte introduttiva, è stata evidenziata la varietà delle applicazioni robotiche. Questa variegata realtà fa sì che, come avviene in generale per tutti i prodotti, qualora quello oggetto d'esame appartenga a una specifica categoria, la disciplina e il relativo schema regolatorio della sicurezza sono quelli della legislazione di settore.

Tali discipline si presentano, allora, in numero potenzialmente elevatissimo. Basti pensare alla disciplina nel settore dell'aviazione, laddove è già emersa la necessità di modificare il Regolamento 216/2008[114] per adeguare le norme alle specificità dei droni e favorirne lo sviluppo del mercato. Dovrebbero, dunque, «essere eliminati gli

[113] I risultati sono stati presentati dagli esperti durante il workshop *Digital Revolution: Challenges for Contract Law in Practice*, organizzato dall'Università di Münster, 1-2 ottobre 2015. Le relazioni sono contenute in R. Schulze e D. Staudenmeyer (a cura di), *Digital Revolution: Challenges for Contract Law in Practice*, Baden-Baden, Nomos, 2016.

[114] Regolamento (CE) 216/2008 del Parlamento europeo e del Consiglio, del 20 febbraio 2008, recante regole comuni nel settore dell'aviazione civile e che istituisce un'Agenzia europea per la sicurezza aerea, e che abroga la Direttiva 91/670/Cee del Consiglio, il Regolamento (CE) 1592/2002 e la Direttiva 2004/36/CE, in *OJ L*, 79, del 19 marzo 2008, pp. 1-49.

ostacoli normativi non giustificati, ma le norme essenziali di sicurezza dovrebbero rimanere in vigore o, laddove inesistenti, essere sviluppate»[115]. Altri esempi sono: la disciplina in materia di armi, in riferimento allo sviluppo del mercato degli «armamenti autonomi»; la legislazione in materia di sicurezza sul lavoro e la sua applicabilità ai c.d. «robot operai»[116]; la disciplina sulla sicurezza stradale, con riferimento allo sviluppo di tecnologie di automazione avanzata per il trasporto.

Anche la disciplina dei prodotti biomedicali assumerà un'importanza centrale dato il rapido sviluppo dei prodotti robotici biomedicali, che includono applicazioni tra loro diversissime, come robot chirurgici; protesi robotiche; capsule mediche intelligenti.

L'*eyeborg* richiamato nell'introduzione ben configura uno dei principali problemi emergenti quando si tratta di applicare la legislazione di settore: la difficoltà di utilizzare il sistema classificatorio vigente al fine di far ivi rientrare i prodotti più innovativi. Le questioni classificatorie accomunano le esperienze giuridiche, sia di *civil law* che di *common law*, nell'analisi delle risposte giuridiche ai problemi dello sviluppo tecnologico[117]. Naturalmente, non si tratta di un mero problema definitorio, poiché dalla classificazione dipen-

[115] Documento di lavoro che accompagna la *Proposta di Regolamento del Parlamento Europeo e del Consiglio recante regole comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che abroga il Regolamento CE n. 216/2008 del Parlamento europeo del Consiglio*, COM(2015) 613 Final.

[116] Peraltro, è stato constatato che mentre ad oggi i robot sostituiscono i robot operai, i futuri progressi dell'AI renderanno possibile anche la sostituzione delle professioni impiegatizie. Si veda il Parere del Comitato economico e sociale europeo sul tema «Fornire e sviluppare le competenze, incluse le competenze digitali, nell'ambito di nuove forme di lavoro: nuove politiche ed evoluzione dei ruoli e delle responsabilità», 2017/C 434/06, in *GU* del 15 dicembre 2017. Il parere del Cese sul tema *Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società*, adottato il 31 maggio 2017, in *GU C*, 288, del 31 agosto 2017, p. 1.

[117] G.N. Mandel, *Legal Evolution in Response to Technological Change*, in R. Brownsword, E. Scotford e K. Yeung, *The Oxford Handbook of Law, Regulation and Technology*, Oxford, Oxford University Press, pp. 225 ss.

dono le regole di sicurezza applicabili, la regolamentazione dell'immissione in commercio, e di tutte le fasi di controllo post-market, nonché il regime di *enforcement*.

Un significativo esempio è offerto dalle nanotecnologie biomedicali[118]. Il problema definitorio riscontrato rispetto a prodotti medici che si presentano «combinati» è stato affrontato, con anticipo, dall'ordinamento americano, particolarmente attento all'identificazione di dettagliate definizioni ormai di competenza della Food and Drug Administration (Fda): negli ultimi decenni, l'agency ha ampliato la sua competenza, chiarendo la definizione e la tipologia di appartenenza di numerosi nuovi prodotti medici ancora non definiti e regolamentati[119]. Le categorie tradizionali, nelle quali i diversi prodotti vengono catalogati a seconda degli effetti chimici o meccanici che scaturiscono dalla loro applicazione sul corpo umano, contemplano i medicinali, i dispositivi medici, i materiali biologici o una loro combinazione, qualora fossero assemblati due o più componenti tra quelli appena menzionati[120]. Le produzioni su nanoscala hanno permesso di realizzare combinazioni di materiali assolutamente inedite, potendo esitare in artefatti terapeutici o diagnostici, ove risulta impossibile separare gli effetti chimici dagli altri. Conseguentemente, tali strumenti non possono classificarsi né come farmaci, la cui definizione è basata sugli effetti chimici generati, né come dispositivi caratterizzati da effetti meccanici. Già negli anni Novanta, con la pubblicazione del *Safe Medical Device Act*,

[118] Cfr. G. Guerra, *Nanomedicina e diritto: un primo approccio*, in *Danno e resp.*, 2006, pp. 1029-1039.

[119] Il fenomeno è ben descritto da L.R. Horton, *Over the Counter Drug Authority Issues: Selected Topics*, in *Food & Drug L.J.*, 48, 1993, p. 545; S.B. Foote e R.J. Berlin, *Can Regulation Be as Innovative as Science and Technology? The Fda's Regulation of Combination Products*, in *Minn. J.L. Sci.& Tech.*, 6, 2005, p. 619.

[120] Nell'ordinamento statunitense le definizioni di farmaco e dispositivo medico si trovano, rispettivamente, alle lett. *g*) e *h*) dell'art. 321 *g*) del *Federal Food, Drug and Cosmetic Act* (21 Usc 355). La definizione di materiale biologico è invece contenuta nell'*Fda Modernization Act* (Fdama) art. 123 *d*); infine il prodotto combinato viene definito nel 21. Cfr. 3.2 *e*), 2004.

l'ordinamento statunitense aveva riconosciuto una nuova categoria di prodotti, definiti «combinati», per fronteggiare i problemi dovuti all'identificazione di dispositivi medici frutto di tecnologie emergenti[121]. In Europa, il problema del dispositivo medico combinato è stato affrontato in tempi più recenti, con il Regolamento Dispositivi Medici (UE) 2017/745 (Mdr), che abroga la Direttiva 93/42/Cee (Mdd), applicabile a partire dal 26 maggio 2020[122].

[121] La Food and Drug Administration, l'agenzia statunitense responsabile della sicurezza di molti prodotti alimentari, farmaci a uso umano e veterinario, agenti terapeutici di origine biologica, dispositivi medici, prodotti radioattivi e cosmetici, con l'approvazione del *Fda Modernizazton Act* (Fdama), ha predisposto la regolamentazione del prodotto combinato attraverso il *Safe Medical Device Act* del 1990 (Federal Health Law, L. No 101-629, par. 16). La Fda ha cominciato a occuparsi di nanostrumentazione fin dalla fine degli anni Novanta, sulla scia delle polemiche sollevate qualche anno prima per aver avviato in ritardo le sue pratiche istruttorie sulle applicazioni di prodotti tecnologicamente innovativi. A testimonianza del fatto che l'innovazione tecnologica richiede sovente adattamenti dell'apparato regolativo preesistente, nel 2002 è stato approvato il *Medical Device User Fee and Modernization Act*. Per la tipologia di problematiche poste dalla nanomedicina, la Fda aveva già compiuto i primi passi al fine di non tradire quella *proud tradition* relativa all'elevato grado di fiducia che la società statunitense ripone nel ruolo della stessa *agency* di garante della sicurezza e salute pubblica. Recentemente, la Fda ha proposto un modello di regolamentazione che permetterebbe di superare il modello tradizionale (*product by product basis*) e di scegliere l'autorità preposta a disciplinare il prodotto combinato in base al suo *primary mode of action*, ovvero al predominante modo di agire del prodotto. Nel sistema vigente, i prodotti combinati sono valutati da un apposito centro: l'*Office of Combination Products* (Ocp). Il centro «ensure the prompt assignment of combination products to agency centers, the timely and effective pre-market review of such products, and consistent and appropriate post-market regulation of like products subject to the same statutory requirements to the extent permitted by law» (21 Usca, par. 353, (g)(4).

[122] Regolamento Dispositivi Medici (UE) 2017/745 (Mdr), che abroga la Direttiva 93/42/Cee (Mdd) entra in vigore il 25 maggio 2017, con 1° step il 26 novembre 2017 (Organismi Notificati) e termine definitivo con abrogazione della Direttiva 93/42/Cee (dispositivi medici) e Direttiva 90/385/Cee (dispositivi medici impiantabili attivi), inserite entrambe nel Regolamento, a decorrere dal 26 maggio 2020, in *GU L*, 117/92, del 5 maggio 2017.

Anche la robotica biomedicale ha già presentato analoghi problemi. Il documento *Liability for Emerging Digital Technologies* del 25 aprile 2018 ha dato conto, infatti, che lo *European Standardization Organizations* sta lavorando sugli standard per prodotti «combinati», per affrontare il problema delle sovrapposizioni tra diverse regolamentazioni di sicurezza[123].

A tal proposito, si deve rilevare che il nuovo Regolamento si presenta come il primo modello normativo che considera il software, sia come accessorio, sia come dispositivo[124]. Il robot chirurgico (es. robot chirurgico Da Vinci) è classificato alla stregua di un dispositivo disciplinato dal Regolamento 2017/745, e la fase di sperimentazione così come i requisiti di conformità non sono, quindi, trattati diversamente rispetto alla tradizionale strumentazione chirurgica, sebbene presenti caratteristiche *sui generis*: la complessa interazione tra macchina e uomo[125], e i rischi di interferenza esterni dovuti alla connettività del sistema. Questi ultimi non sono, però, contemplati dai requisiti di funzione, progettazione e costruzione della regolamentazione, previsti nel Regolamento 2017/745. Anche le c.d. capsule intelligenti, o robotiche, alimentate al litio, dotate di «zampe» o «eliche», e utilizzate per distruggere i blocchi nei vasi sanguigni, o per curare i tumori, presentano rischi

[123] European Commission, *Staff Working Document. Liability for Emerging Digital Technologies*, cit.

[124] Cfr. Considerando 19, artt. 14.2, 17 ecc.

[125] Altri modelli simili al Da Vinci dovrebbero uscire a breve. Cfr. http://www.verbsurgical.com/; https://www.transenterix.com/; https://titanmedicalinc.com/. Nell'ambito della chirurgia robotica sono attualmente in fase di sviluppo progetti volti a implementare il grado di autonomia del robot chirurgico. Il progetto Saras, per esempio, si propone di creare un vero e proprio «assistente robotico»: un sostituto del chirurgo, il quale dovrà capire in che fase dell'operazione ci si trova, cosa il chirurgo si aspetta e come muovere gli strumenti in modo da eseguire il task senza disturbare gli strumenti teleoperati dal chirurgo principale. Informazioni apprese in dialogo con il prof. Riccardo Muradore (ingegnere informatico, ricercatore), intervistato dall'autore, Dipartimento di informatica, Università di Verona, Verona, Italia, 24 febbraio 2018. Coordinatore del progetto H2020 Saras, *Smart Autonomous Robotic Assistant Surgeon*.

inediti fino a ora, relativi, ad esempio, all'eventuale blocco del dispositivo nel corpo[126].

Le protesi robotiche, in particolare quelle c.d. ibride, composte, cioè, da parti biologiche e da parti meccaniche che si interfacciano (es. arto meccanico) offrono uno spunto interessante per riflettere sulle diverse conseguenze, anche di rilevanza etica e filosofica, cui può giungere una diversa classificazione. Tali dispositivi rendono labile, e problematico il confine tra terapia, *restitutio ad integrum*, e lo *human enhancement*, ossia la *transformatio ad optimum* che si verifica quando le capacità umane, fisiche o cognitive vengono potenziate. Alcuni dispositivi realizzano entrambe le funzioni, c.d. *dual use*[127].

Un altro ambito assai significativo è rappresentato dai veicoli a guida automatizzata. Rinviando al capitolo II una più ampia trattazione del tema, è utile, in questa sede, ricordare che le *driveless cars* rimetteranno in discussione i fondamenti della legislazione pubblicistica europea sulla sicurezza degli autoveicoli, formulata tra gli anni Cinquanta e Sessanta: garantire la ragionevole sicurezza del veicolo attraverso l'identificazione delle caratteristiche strutturali idonee a uniformare gli standard di qualità per agevolare il commercio delle autovetture. Il problema sotteso al quadro legislativo europeo è relativo al coordinamento tra standard di sicurezza emanati in momenti diversi e da fonti diverse: in un primo momento, a partire dal 1958, attraverso la ratifica dell'accordo *Inland Transport Division della United Nations Economic Commission for Europe* (Unece)[128], gli

[126] Il principale rischio delle capsule endoscopiche è il blocco delle stesse nell'intestino. Le diverse ipotesi di rischio e le varie percentuali di rischio mi sono state illustrate dal dott. Marco Zenati (Chief of Cardiac Surgery, Harvard Medical School, Boston), intervistato dall'autore, Università di Verona, 30 ottobre 2017.

[127] Per una ricostruzione dell'ampio dibattito sul tema del potenziamento umano si rinvia a F. Lucivero e A. Vedder, *Beyond Therapy v. Enhancement? Multidisciplinary Analyses of a Heated Debate*, Pisa, Pisa University Press, 2014.

[128] L'accordo è stato stipulato a Ginevra nel 1958. Cfr. http://www.unece.org/leginstr/trans.html.

Stati aderivano, su base volontaria, agli standard minimi di sicurezza ivi codificati; poi, negli anni Settanta, l'Unione europea cominciò a emanare propri standard attraverso la Direttiva 70/156/Cee[129], e sul finire degli anni Novanta, con la decisione del Consiglio Ce 97/836, l'UE ha aderito alla Convenzione Unece. Infine, la Direttiva quadro 2007/46/CE ha sostituito la Direttiva 70/156/Cee istituendo un quadro per l'omologazione dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, componenti, ed entità tecniche destinati a tali veicoli[130]. Nulla dice sul punto la Direttiva 2010/40/UE, principale riferimento normativo che delinea un quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto[131].

[129] Direttiva 70/156/Cee del Consiglio, del 6 febbraio 1970, concernente il ravvicinamento delle legislazioni degli Stati membri relativa all'omologazione dei veicoli a motore e dei loro rimorchi, in *GU L*, 42, del 23 dicembre 1970.

[130] Direttiva 2007/46/CE del Parlamento europeo e del Consiglio, del 5 settembre 2007, che istituisce un quadro per l'omologazione dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, delle componenti e delle entità tecniche destinati a tali veicoli (Direttiva quadro), in *GU L*, 263, del 9 ottobre 2007, pp. 1-160. In questo modo, l'UE consente l'omologazione delle auto prodotte da paesi extra UE aderenti all'accordo Unece. Gli Stati Uniti non hanno aderito a quest'ultimo accordo, pertanto, i produttori americani che vogliano commercializzare le loro auto in Europa dovranno conformarsi agli standard previsti dalla Direttiva 2007/46/CE. Mentre, invece, i produttori europei che volessero commercializzare le loro auto in Usa devono rispettare gli standard previsti dal *Federal Motor Vehicle Safety Standard* (Fmvss) e ottenere l'omologazione rilasciata dalla *National Highway Traffic Safety Agency* (Nhtsa).

[131] *OJ L*, 207, del 6 agosto 2010. Pare utile notare, però, che l'art. 11 della Direttiva indica che gli Stati membri provvedano affinché le questioni relative alla responsabilità, riguardo alla diffusione e all'utilizzo delle applicazioni e dei servizi Its, siano trattate conformemente al diritto dell'Unione, in particolare della Direttiva 85/374/Cee. Vedi anche la Comunicazione della Commissione europea relativa ad «una strategia europea per i sistemi di trasporto intelligenti cooperativi, prima tappa verso una mobilità cooperativa, connessa e automatizzata» Com(2016) 766 final.

6. *Prime considerazioni di sintesi*

L'Unione europea accoglie la realtà che muta attraverso la convergenza di diverse tecniche regolatorie, in funzione *multitasking*[132].

AI e robotica hanno, dunque, trovato un contesto regolatorio europeo già favorevole: per questo, il concetto di *responsible* AI diventa corollario della Rri. Esso implica l'inclusione di valori etici e giuridici *attraverso* la stessa tecnologia, ad esempio, progettando la sicurezza di un artefatto robotico *by design.* Si tratta di un meccanismo che testimonia, peraltro, il ricorso a modelli regolatori inclusivi e partecipativi (par. 1.1). Modelli che richiedono il superamento dei «silos» disciplinari.

Il contributo principale di queste pagine consiste nell'aver delineato il composito quadro europeo in materia di sicurezza dei prodotti il quale, frutto del coordinamento tra le misure orizzontali (par. 4) e le discipline di settore (par. 5), risulta già flessibile e dettagliato. Le consultazioni pubbliche e le altre recentissime iniziative manifestano, inoltre, la volontà di intervenire in tempi rapidi per adeguare, o trasformare, laddove necessario, la regolamentazione sulla quale impatta il cambiamento tecnologico.

Le questioni di sicurezza emergenti per i prodotti robotici coincidono in parte con quelle poste negli ultimi anni da altre applicazioni tecnoscientifiche: è un esempio la «combinazione» di parti di prodotti, che comporta la sovrapposizione di diversi regimi regolatori di sicurezza. A tal proposito, gli organismi internazionali stanno studiando degli standard di sicurezza idonei a essere applicati a prodotti «combinati»[133].

[132] La prospettiva *multitasking* è proposta da S. Rodotà, *Technology and Regulation: A Two-way Discourse*, in E. Palmerini e E. Stradella, *Law and Technology. The Challenge of Regulating Technological Development*, Pisa, Pisa University Press, 2013, p. 27.

[133] Si rinvia a Oecd, *Consumer Product Safety in the Internet of Things*, cit.

Altri profili, invece, sono inediti, come quelli connessi all'autonomia e, in prospettiva futura, alla capacità di autoapprendimento della robotica avanzata attraverso esperienza e interazione. Entro quest'ultimo gruppo di problemi, sicuramente l'area di sovrapposizione tra sicurezza dei prodotti e (cyber)security, ossia la sicurezza dei sistemi informatici, dovuta alla, sempre più diffusa, connessione di oggetti (robotici) alla rete, si sta delineando di centrale importanza.

Queste ultime questioni appaiono più evidenti in relazione all'emergere della robotica del futuro: diventano elementi di analisi non trascurabili la manifattura del robot, il tipo di interazione uomo-macchina, la velocità delle comunicazioni, e il cloud che permetterà l'accumulo di esperienza e capacità sviluppate dall'AI di questi robot[134]. Tuttavia, nonostante i tanti tratti *sui generis* per l'impatto che preannunciano, si tende a prediligere la rimodulazione delle regole esistenti, in luogo dell'approccio unitario, ancorché promosso dalla già dibattutissima Risoluzione del 2017 (par. 2). Ad indicarlo sono, altresì, le numerose iniziative in materia di Digital Single Market Strategy (Dsm)[135], IoT, European Data Economy, i recenti documenti sulla responsabilità per le tecnologie

[134] R. Cingolani e G. Metta, *Umani e umanoidi. Vivere con i robot*, Bologna, Il Mulino, 2015.

[135] Si rinvia alla Amended proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods, amending Regulation (EC) No. 2006/2004 of the European Parliament and of the Council and Directive 2009/22/EC of the European Parliament and of the Council and repealing Directive 1999/44/EC of the European Parliament and of the Council, 31.10.2017, Com(2017) 637 final; Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, 9.12.2015, Com(2015) 634 final; Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods, 9.12.2015, Com(2015) 635 final. Proposta di direttiva del Parlamento europeo e del Consiglio, Determinati aspetti dei contratti di fornitura di contenuto digitale, Com(2015) 634 Def. del 9 dicembre 2015; Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo delle Regioni, Strategia per il mercato unico digitale in Europa, Com(2015) 192 final.

digitali emergenti, nonché le consultazioni avviate per la revisione della Direttiva sulla responsabilità per prodotti difettosi e quella sulle macchine.

Capitolo secondo

RIPENSARE IL TEMA DELLA SICUREZZA DEI PRODOTTI ROBOTICI NELLA PROSPETTIVA DELLA RESPONSABILITÀ CIVILE

1. *Innovazione e sistema sicurezza-responsabilità: lo stato dell'arte*

Per riprendere l'immagine iniziale, questo capitolo analizza il tema della sicurezza entro il «frattale» civilistico.

L'osservazione sul campo di diverse applicazioni robotiche ha permesso di identificare la varietà e complessità dei quesiti giuridici che si stagliano all'orizzonte[1]: la trasparenza delle operazioni di calcolo compiute dall'algoritmo; l'affidabilità del software di guida automatizzata; l'identificazione dei criteri per valutare i sofisticati dispositivi diagnostici intelligenti sono solo alcuni esempi.

Non è semplice individuare un chiaro ed effettivo quadro rimediale applicabile, quale condizione essenziale per ottenere la fiducia dei consumatori, e di conseguenza la diffusione di queste tecnologie.

Le pagine che seguono fanno emergere quali concetti e regole del sistema sicurezza-responsabilità necessitano di essere adattati. A tal fine, il presente paragrafo introduttivo sintetizza, nelle linee essenziali, l'operatività di tale schema in contesti produttivi già innovativi.

La comparazione giuridica ha fornito un contributo fondamentale nello studio della sicurezza dei prodotti[2],

[1] Questo capitolo ha beneficiato, in modo particolare, del dialogo con molti esperti, informatici, ingegneri ma anche psicologi specializzati in *human-machine interaction*. Le tipologie di prodotti oggetto di osservazione sono state principalmente: protesi mediche, chirurgia robotica assistita, robot collaborativi usati per lo più nei reparti medici, *self-driving cars*. Tutti i miei interlocutori sono afferenti all'Università di Padova (centro Spritz; Hit Research Center), Università di Verona e Politecnico di Milano.

[2] Nel nostro ordinamento la disciplina è contenuta negli artt. 101-113 del codice del consumo (cod. cons.).

promuovendone la lettura coordinata con le regole di responsabilità del fabbricante (artt. 114-127 cod. cons.)[3].

Il modello giuridico di riferimento è, in prim'ordine, quello americano entro il quale il coordinamento tra tutela preventiva e quella rimediale avviene in modo sistematico, in virtù dell'operatività della *preemption clause*[4]: essa definisce una sorta di percorso valutativo che riduce la discrezionalità interpretativa del giudice nei giudizi per danno da prodotto, predeterminando la prevalenza degli standard di sicurezza federali su quelli statali, e il rapporto tra standard e azione di responsabilità[5].

L'interdipendenza in parola è da tempo studiata anche dalla letteratura giuseconomica: considerate singolarmente, entrambe le alternative istituzionali sono incapaci di assicurare una prevenzione ottimale dei danni, poiché lo strumento della responsabilità gioca un ruolo cruciale nel valutare i rischi reificatisi nei singoli casi; mentre, invece, la regolamentazione amministrativo-legislativa è funzionale alla prevenzione di macro categorie di rischi, poiché «argina» il verificarsi di danni, tutti potenzialmente uniformi. Ed è la stessa riflessione giuseconomica a fornire gli elementi di

[3] Per un riferimento al contesto europeo si rinvia a F. Cafaggi (a cura di), *The Institutional Framework of European Private Law*, Oxford, Oxford University Press, 2006, pp. 191-244. Il diritto del consumatore all'utilizzo di prodotti sicuri emerge dalla giurisprudenza della Corte europea dei diritti dell'Uomo; dalla Carta sociale europea e dalla Convenzione internazionale sui diritti economici, sociali e culturali e dai codici di condotta delle Nazioni Unite. Cfr. H. Micklitz, *The International Dimension of Product Safety*, in M. Fallon e F. Maniet, *Product Safety and Control Process in the European Community*, Lovain-la-Neuve, Éditions Larcier, 1990, pp. 215 ss.

[4] La *preemption clause* regola, sia in modo esplicito (*express preemption*) che implicito (*implied*), il valore da attribuire allo standard: se esso identifica il livello massimo di sicurezza, non sarà possibile configurare un'azione di responsabilità; se, invece, è considerato una soglia minima, allora il rispetto non esime il produttore dalla responsabilità per i danni da prodotto. Casi di scuola sono: *Medtronic, Inc. v. Lohr*, n. 95-754 (United States Supreme Court, 26 giugno 1996); *Cipollone v. Liggett Group*, Inc., n. 90-1038 (United States Supreme Court, 24 giugno 1992).

[5] S. Shavell, *Liability for Harm versus Regulation of Safety*, in *Legal Stud.*, 13, 1984, p. 482.

analisi per rileggere, criticamente, l'effetto delle scelte relative all'allocazione del regime di responsabilità oggettiva per danno da prodotto difettoso e all'investimento *ex ante* in sicurezza dei prodotti: l'allocazione della responsabilità oggettiva per danno da prodotto difettoso in capo al produttore comporterebbe un aumento del prezzo del prodotto nel mercato[6].

Da lungo tempo, la riflessione civilistica si concentra sulla relazione *torts and innovation*[7]. Ne rappresenta un corollario quella parte degli studi dedicati al principio di precauzione che, lungi dall'identificarlo solamente quale presupposto legittimante l'azione di autorizzazione regolamentare preventiva, gli attribuiscono, invece, la valenza di criterio ermeneutico sistematico nella prospettiva della responsabilità civile: la combinazione dell'analisi del rischio con i doveri precauzionali, intesi come la messa in atto delle «conoscenze e delle tecnologie precauzionali» è implicita nella valutazione della causalità giuridica[8].

[6] R. Posner, *Economic Analysis of Law*, New York, Aspen Publishers, 2007, p. 180. Sul bilanciamento tra esigenze di sicurezza e della produzione si rinvia a S. Rodotà, *Modelli e funzioni della responsabilità civile*, in *Riv. crit. dir. priv*., 1984, pp. 585 ss.

[7] Per una ricostruzione del dibattito A. Stein e G. Parchomovsky, *Torts and Innovation*, in *Mich. L. Rev.*, 107, 2008-2009, p. 285.

[8] Così U. Izzo, *La precauzione nella responsabilità civile. Analisi di un concetto sul tema del danno da contagio per via trasfusionale*, Università degli studi di Trento, 2007 (la prima edizione è edita da Cedam, 2004), spec. p. 303, consultabile all'indirizzo http://eprints.biblio.unitn.it/1253/1/izzo_precauzione_RC_DEFINITIVO.pdf. L'opera analizza il fondamento epistemico della precauzione e affronta minuziosamente l'impatto dell'approccio precauzionale nelle regole operazionali della responsabilità civile. La dottrina non accoglie unanimemente tale impiego del principio. In altri termini, non sempre viene avvalorata la «teoria normativa» che si basa, peraltro, sulle numerose pronunce della Corte di Giustizia, dove il principio è criterio valutativo nel giudizio di responsabilità, vedi G. Tomarchio, *Il principio di precauzione come norma generale,* in L. Marini e L. Palazzani (a cura di), *Il principio di precauzione tra filosofia, biodiritto e biopolitica*, Roma, Studium, 2008. Per altri, il principio rimane un criterio di condotta di fronte al rischio, ne dà conto anche M.G. Stanzione, *Principio di precauzione e diritto alla salute. Profili di diritto comparato*, in *Comparazione e diritto civile*, 2016, pp. 1-34. Autorevole dottrina afferma che il principio è criterio

Una categoria di prodotti, in continuo aumento, è protagonista delle moderne analisi giuridiche: i c.d. *unavoidable unsafe products.* Con tale espressione, il sistema giuridico statunitense identifica quei prodotti che, pur utilizzati secondo il ragionevole uso previsto, presentano un *residue of unavoidable risk*, ossia un significativo margine di dannosità ineliminabile in base allo stato di conoscenze scientifiche del momento. Si pensi, a titolo esemplificativo, alla *litigation* in materia di danno da prodotto farmaceutico; danno da ingestione di alimenti contenenti percentuali di sostanze chimiche potenzialmente dannose per la salute; prodotti derivanti da tabacco, e al problema delle onde elettromagnetiche, correlato all'uso di determinati prodotti, come i cellulari.

Non vi è in dottrina e in giurisprudenza una chiara distinzione tra rischiosità intrinseca e rischio da ignoto tecnologico[9]. In ogni caso, il diritto privato si è occupato, già da tempo, dell'alea da rischio tecnologico per valutare su quali soggetti gravino i costi di eventi dannosi non evitabili al momento della predisposizione delle cautele richieste secondo i parametri della diligenza tecnica[10].

ispiratore della legislazione e dei provvedimenti amministrativi a tutela della salute e non può condurre ad un'espansione incontrollata della responsabilità civile. Così E. Al Mureden, *La responsabilità per esercizio di attività pericolose a quarant'anni dal caso Seveso*, in *Contratto e impresa*, 3, 2016, p. 648. Dello stesso autore si veda anche *Principio di precauzione, tutela della salute e responsabilità civile*, Bologna, Libreria Bonomo, 2008, laddove l'autore, a partire dalle norme che collegano il principio di precauzione con quelle in tema di responsabilità del produttore (artt. 114-127 cod. cons.), indaga i possibili riflessi del principio di precauzione e di norme sottese a logiche precauzionali sulle regole generali che governano la responsabilità civile.

[9] F. Santonastaso, *Principio di «precauzione» e responsabilità d'impresa: rischio tecnologico e attività pericolosa «per sua natura». Prime riflessioni su un tema di ricerca*, in *Contratto e impresa/Europa*, I, 2005, pp. 21 ss.; F. Stella, *Il rischio da ignoto tecnologico e il mito delle discipline*, in AA.VV., *Il rischio da ignoto tecnologico*, Milano, Giuffrè, 2002, p. 3.

[10] Il nostro ordinamento è giunto a soluzioni non sempre coerenti. Ne dà atto L. Mormile, *Il principio di precauzione fra gestione del rischio e tutela degli interessi privati*, in *Riv. dir. econ., trasporti e ambienti*, 2012, p. 247.

Il rischio connesso al progresso tecnologico sfugge al giudizio di difettosità assunto a fondamento della disciplina armonizzata del legislatore europeo, per diversi motivi: anche nel caso in cui si trattasse di un rischio originario, l'onere della prova assumerebbe i tratti di una *probatio diabolica*[11]. Ecco, dunque, la *ratio* della prova liberatoria per «rischio da sviluppo», ai sensi dell'art. 118 del Codice del Consumo.

Questo capitolo si svilupperà come segue: i paragrafi *sub* 2 e 3 sono dedicati all'inquadramento del tema della sicurezza dei prodotti robotici entro il sistema sicurezza-responsabilità, delineando le caratteristiche funzionali, e di altra natura, le quali rappresentano elementi di discontinuità, o eccezionalità; i paragrafi *sub* 4 considerano l'impiego degli standard di sicurezza per la robotica, al fine di coglierne i cambiamenti emergenti soprattutto con riferimento alla robotica collaborativa e alla questione del danno da prodotto conforme agli standard; i paragrafi *sub* 5 ripercorrono i profili di responsabilità con specifica attenzione alla responsabilità da prodotto e da malfunzionamento dell'algoritmo; il paragrafo 6 delinea le proposte di schemi di indennizzo alternativi della responsabilità. Il paragrafo 7 focalizza l'analisi sul contesto specifico delle auto a guida automatizzata. Infine, seguono alcune considerazioni conclusive.

2. *Il sistema sicurezza-responsabilità e la robotica: tra adattamenti e nuovi paradigmi*

L'inquadramento di molti prodotti robotici entro il tradizionale sistema civilistico sicurezza-responsabilità pone diversi problemi. Le macchine intelligenti hanno uno sviluppo «opaco»: le caratteristiche dei sistemi di AI più avanzati e le questioni relative al controllo dell'azione robotica potrebbero privare di efficacia tale sistema di regole, ovvero metterne in discussione la *ratio*.

A una prima osservazione, la robotica avanzata non pare presentare una rischiosità intrinseca, almeno secondo la de-

[11] Un esempio è tratto dal contesto della chirurgia robotica.

finizione anticipata. Pertanto, non rientra nella categoria dei prodotti inevitabilmente insicuri. Ciò trova conferma nelle prime righe del già citato *Staff Working Document* della Commissione europea in materia di *liability for emerging digital technologies*, laddove si legge: «these new products and services are not inherently less safe than traditional products»[12].

Il richiamo alla categoria degli *unavoidable unsafe products* – al fine di prenderne le distanze – non è, dunque, casuale. Ciò non toglie che sia ugualmente funzionale ad analizzare la tecnologia che qui ci occupa, l'identificazione delle analogie con vicende giurisprudenziali concernenti prodotti *low-tech* e imperniate intorno alla definizione di difetto e all'operabilità dell'esimente per rischi da sviluppo[13].

Chiarito ciò, è necessario chiedersi se l'architettura del sistema sicurezza-responsabilità sia adeguata ad allocare le responsabilità e distribuire i costi degli eventuali danni da artefatti robotici. Tali regole dovrebbero contemperare l'esigenza di incentivare l'innovazione e arginare, anche sul versante della responsabilità civile, il c.d. *technology chilling effect*[14].

[12] European Commission, *Staff Working Document. Liability for Emerging Digital Technologies*, Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Artificial Intelligence for Europe*, Bruxelles, 25 aprile 2018, Com(2018) 237 final.

[13] Si pensi ai numerosi casi di farmaci difettosi tra cui il talidomide, la cerivastatina, l'antinfiammatorio e antidolorifico Vioxx, a base di rofexocib e il Bextra. Cfr. A. Fiori e D. Marchetti, *Medicina legale della responsabilità medica*, in *I danni da prodotti e da dispositivi medici*, Milano, Giuffrè, 2009.

[14] Su questo profilo la *scholarship* statunitense si è distinta per numero e autorevolezza dei contributi. Tra i tanti, si ricorda: W.K. Viscusi e M.J. Moore, *Rationalizing the Relationship between Product Liability and Innovation*, in P.H. Schuck, *Tort Law and the Public Interest. Competition, Innovation, and Consumer Welfare*, 1991, pp. 125 ss.; P.W. Huber e R.E. Litan (a cura di), *The Liability Maze: The Impact of Liability Law on Safety and Innovation*, Washington, Brookings Institution Press, 1991; G. Parchomovsky e A. Stein, *Torts and Innovation*, in *Michigan Law*

I primi studi giuridici «previsionali» circa l'impatto della robotica su tale sistema delineano orientamenti diversi. Secondo il giudice Karnow, la complessità delle macchine che interagiscono con l'ambiente circostante sfugge al concetto di prevedibilità tipico della *tort law*, così come la linearità causale, che fonda il giudizio di responsabilità, non pare più un adeguato parametro di valutazione[15].

Diversamente, Vladeck[16] e Hubbard[17] sostengono che il sistema corrente delle regole in esame sia pronto a rispondere alle esigenze di tutela, di compensazione, e *deterrence* rispetto ai danni provocati dagli artefatti robotici, almeno nel breve termine.

Hubbard, in particolare, osserva che, al momento attuale, i robot rispettano un elevato livello di sicurezza, e si chiede se i costi, di cui la società deve farsi carico per predisporre gli standard di sicurezza di tali prodotti, non siano troppo elevati: peraltro, la sicurezza sarebbe solo uno dei valori sociali con i quali l'innovazione tecnologica dovrebbe essere bilanciata. L'autore formula questa osservazione considerando l'impatto delle decisioni degli innovatori (*venture capitalists*, produttori, progettisti) sull'investimento in sviluppo della robotica. Sottolinea l'importanza di fondare tali scelte sulla razionale comparazione dei possibili benefici economici dell'innovazione robotica con i costi, inclusi i costi per la compensazione di eventuali danni e per predisporre misure regolatorie adeguate. Le difficoltà sottese a tale operazione non mancano, poiché si tratta di decisioni da prendere in situazione di incertezza: i risultati della scelta non sono perfettamente prevedibili, in quanto dipendono da molteplici variabili, non tutte conoscibili, come, ad esempio, i c.d.

Review, 107, 2008, p. 285; anche in *Cardozo Legal Studies Research Paper*, n. 209, consultabile su Ssrn, https://ssrn.com/abstract=1028346.

[15] E.A. Karnow, *The Application of Traditional Tort Theory to Embodied Machine Intelligence*, in R. Calo, A.M. Froomkin e I. Kerr, *Robot Law*, Cheltenham, Edward Elgar, 2016, p. 51.

[16] D.C. Vladeck, *Machines without Principals: Liability Rules and Artificial Intelligence*, in *Washington Law Review*, 89, 2014, p. 117.

[17] F.P. Hubbard, *'Sophisticated Robots': Balancing Liability, Regulation and Innovation*, in *Fla. L. Rev.*, 66, 2014, p. 1803.

«bias» cognitivi dei consumatori; le reazioni degli utilizzatori (es. avversione al rischio); la concorrenza; la congiuntura economica; la politica monetaria e fiscale[18].

Per Hubbard, quindi, chi considera inadeguato il sistema corrente sicurezza-responsabilità per la robotica, spesso, omette di verificare se sussista un bilanciamento tra innovazione e responsabilità per focalizzarsi solo su uno dei due «piatti della bilancia»: gli incentivi all'innovazione; ovvero, la funzione di compensazione della responsabilità civile. Per di più, le critiche – osserva lo stesso Hubbard – si fondano su eccessive aspettative nutrite verso le funzioni della responsabilità civile, senza tenere adeguatamente conto del ruolo degli strumenti assicurativi nel meccanismo di compensazione.

Altra parte della dottrina, invece, condivide, parzialmente, tali posizioni: il nuovo «ecosistema collaborativo» della robotica, basato sulla condivisione delle risorse esterne (vedi *infra* il fenomeno del *cloud robots*)[19], preannuncia la necessità di esaminare i nuovi elementi che impatteranno sulla responsabilità del produttore del robot. Le difficoltà di accertamento degli elementi costitutivi della fattispecie di danno da prodotto robotico[20], e l'ampliamento della gamma delle circostanze,

[18] Secondo la teoria delle decisioni, le opzioni di scelta, in condizioni di incertezza, variano a seconda della strategia prescelta: se si adotta una strategia aggressiva, c.d. di *maxi-max*, massimizzando la produzione, i potenziali benefici superano le perdite, individuando per ciascuna alternativa (tecnologia tradizionale *vs.* tecnologia nuova), il massimo risultato possibile e poi scegliendo, fra questi, il valore massimo assoluto. Se si adotta, invece, una strategia più prudente c.d. *maxi-min*, si individua per ciascuna scelta l'esito peggiore (cioè, il minimo) e si sceglie tra questi il caso migliore, da cui la denominazione. Vi è, inoltre, un modello di compromesso, conosciuto come criterio di Hurwicz. Si tratta di modelli astratti, difficilmente applicabili in maniera pura nella realtà.

[19] Cfr. R. Calo, *Open Robotics*, in *Md.L. Rev.*, 70, 2011, p. 571; e dello stesso autore *Robotics and the Lessons of Cyberlaw*, in *Calif. L. Rev.*, 103, 2015, p. 513.

[20] *In primis* il nesso di causa tra difetto e danno occorso. Per una ricostruzione del profilo di interesse si rinvia a C. Castronovo, *La nuova responsabilità civile*, Milano, Giuffrè, 2006, pp. 692-693; e A. Fusaro, *Danno da prodotti pericolosi o difettosi: regole di riferimento ed incertezze ermeneutiche*, in *Riv. crit. dir. priv.*, 2, 2015, pp. 203 ss.

le quali possono assurgere a fonte di rischi, sono problemi ricorrenti nel panorama della *law & technology*. Sebbene, secondo le stime dell'*Occupational Safety and Health Administration* del Dipartimento del Lavoro degli Stati Uniti, i casi di danni causati dai robot siano, per lo più, incidentali[21], in breve tempo, la casistica potrebbe complicarsi, e dare luogo a rilevanti questioni di diversa natura.

3. *Il prodotto robotico e le sue peculiarità*

Ciò che sembra mutare, con le applicazioni robotiche, è l'origine dei rischi. Per un verso, come già ricordato, i robot non presentano profili di rischiosità intrinseca. Ingegneri e informatici paragonano spesso il robot, dotato di un basso grado di autonomia, a un tostapane, per spiegare, ai non addetti ai lavori, il livello di «semplicità» della loro AI: eventuali rischi da essi derivanti non originano certo nella componentistica o nelle loro fattezze strutturali.

Per altro verso, i seguenti elementi sembrano introdurre rilevanti differenziazioni rispetto ai prodotti hi-tech già presenti sul mercato: l'interazione con l'ambiente circostante, la locomozione, la circostanza che i robot sociali, con i loro tratti antropomorfi inducano sentimenti di empatia, e la connessione di risorse tra robot.

I robot avanzati minano il rapporto intercorrente tra controllo umano, possibilità di evitare l'evento dannoso e l'imputazione della responsabilità[22].

Come espresso nell'introduzione, questa considerazione non deve indurre automaticamente a ravvisare la necessità di una normativa *ad hoc* in materia. Essa potrebbe, invece, orientare l'analisi giuridica verso un approccio settoriale e casistico, identificando specifici tratti distintivi che innescano il cambiamento nell'analisi giuridica e nella disciplina applicabile.

[21] Si rinvia al sito https://www.osha.gov/.

[22] Si pensi, in prospettiva futura, all'impatto della c.d. *computer-brain interface*.

Qui di seguito sono elencati in dettaglio quali profili peculiari emergono. Sia per la rapidità con la quale evolve il campo in esame, sia per la diversificazione delle applicazioni robotiche, a seconda delle tipologie, la descrizione non ha carattere esaustivo, ma il più semplice intento di fornire una prima descrizione delle tipologie di rischi che si delineano: essi potrebbero incidere, in maniera nuova, o diversa, su ciò che deve considerarsi «ragionevolmente sicuro», introducendo inedite preoccupazioni per la sicurezza della persona[23].

L'interazione con l'ambiente circostante. La condivisione dell'ambiente con persone e altri oggetti può dar luogo a movimenti e reazioni «non programmate» delle macchine robotiche: può avvenire, per esempio, che il robot non si arresti davanti a un ostacolo, o risponda in un modo non corretto agli stimoli ricevuti per un malfunzionamento dei sensori[24]. La necessità di predisporre contesti ambientali realistici per i test dei robot è, infatti, uno degli aspetti centrali delle *policies* nel campo della robotica: come anticipato, già nel 2003, per esempio, il governo giapponese aveva previsto la creazione di aree *Toku Special Zone for Robotic Empirical Testing and Development*, zone speciali per testare i robot umanoidi. Nel campo della guida autonoma, il profilo in esame è centrale in virtù della condivisione dei percorsi stradali con altri veicoli tradizionali e con i pedoni.

L'interazione con l'uomo. Nel settore dei robot collaborativi, a introdurre nuovi fattori di rischio sono le tipologie di contatto con gli uomini, le funzioni dei robot e le abilità di interazione con gli uomini[25]. In prospettiva futura, il machine

[23] A. Van Wynserghe, *Understanding the Complexity of Care in Context and Its Relationship to Technical Content: The Greatest Challenge for Designers of Care Robots*, in B. van de Berg e L. Klaming (a cura di), *Technologies on the Stand: Legal and Ethical Questions in Neurosciences and Robotics*, 2011, p. 340, consultabile all'indirizzo https://pure.uvt.nl/portal/files/1328301/Berg_Technologies_on_the_stand_110509_publishers_embargo_1_y.pdf. L'autore enfatizza l'importanza di comprendere la complessità delle pratiche mediche e le conseguenze che esse hanno sulla progettazione dei robot sociali.

[24] Vedi *infra* riferimenti all'intervista con il prof. Bascetta.

[25] Il progetto dedicato allo studio dell'interazione uomo-macchina (*human-robot interaction*), consultabile all'indirizzo http://humanrobotin-

learning potrebbe introdurre una nuova variabile destinata a incidere sul rischio: la capacità di compiere azioni autonomamente che li fa assimilare ad agenti, e non più a prodotti. Il machine learning impiega tecniche di AI avanzate, ossia programmi informatici in grado di imparare dall'esperienza e migliorare, così, le proprie abilità nel tempo[26]. L'idea di un computer che «impari da solo» è, per lo più, una metafora, e non implica che un sistema informatico riesca a replicare le avanzate capacità cognitive alla base dell'apprendimento umano. L'espressione, più propriamente, indica che, attraverso gli algoritmi, le macchine «apprendono» in senso funzionale: riescono a mutare la loro azione per migliorare le loro *performance* circa un obiettivo, a seconda della loro «esperienza». Al momento, robot che impiegano algoritmi di questa natura sono usati per identificare i flussi di dati e automatizzare così compiti complessi, o fare previsioni[27]. Con riferimento alle loro capacità, tuttavia, un autorevole giurista americano, Cass Sunstein, ha già notato che «at the present state of the art artificial intelligence cannot engage in analogical reasoning or legal reasoning»[28]. In altri termini, le sofisticate capacità cognitive richieste per un ragionamento giuridico non sono, al momento, replicabili attraverso i sistemi di AI[29].

teraction.org/3-emergence-of-hri-as-a-field/. L'iniziativa è trattata anche da U. Pagallo, *Il diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Torino, Giappichelli, 2014, p. 303.

[26] H. Surden, *Machine Learning and Law*, in *Washington Law Review*, 89, 1, 2014, consutabile all'indirizzo https://ssrn.com/abstract=2417415. S. Russell e P. Norvig, *Artificial Intelligence: A Modern Approach*, Harlow, Pearson College Div, 2010, p. 693.

[27] Nella società odierna, questi algoritmi sono usati in una varietà di applicazioni commerciali, inclusi i motori di ricerca, per il riconoscimento facciale, per riconoscere le frodi, per l'estrazione di dati. Un esempio tipico sono i sistemi per filtrare le email «spam».

[28] C.R. Sunstein, K. Ashley, K. Branting e H. Margolis, *Symposium: Legal Reasoning and Artificial Intelligence: How Computers «Think» Like Lawyers*, in *U. Chi. L. Sch. Roundtable*, 8, 1, 2001, p. 19.

[29] In ogni caso, si deve dare atto che i sistemi di AI sono già utilizzati dagli studi legali: «Ross» basato sull'AI Watson di Ibm, la canadese Kira Systems Luminance sviluppata dai matematici di Cambridge University, Intraspexion che promette di offrire servizi c.d. di *preventive law*, start

La connessione tra robot. A interessare, in modo trasversale, diverse applicazioni, è il fenomeno del *cloud computing*, che attraverso tecnologie di archiviazione informatica, consente un accesso più agevole a un insieme di risorse condivisibile[30]. L'estrazione dei dati dal cloud remoto che archivia le informazioni segue modalità di *data mining* e *processing* tipiche dei *big data*, ovvero l'insieme di tecniche e metodologie che hanno per oggetto l'estrazione di un sapere o di una conoscenza, a partire da grandi quantità di dati (attraverso metodi automatici o semi-automatici), e l'utilizzo scientifico, industriale o operativo di questo sapere. Il *data mining* di informazioni eterogenee, condotto anche attraverso un'interoperabilità di diversi database, è idoneo a generare significativi incrementi di valore. Per i robot convenzionali, ogni singolo compito – muovere un piede, raccogliere un oggetto, riconoscere un viso – richiede una significativa quantità di dati pre-programmati e processati. Conseguentemente, sistemi robotici sofisticati, come gli umanoidi, hanno bisogno di avere in dotazione computer molto potenti. I cloud robotic permettono di scaricare una grande quantità di dati da server remoti. Molto promettente appare la prospettiva che i robot possano, attraverso i servizi *cloud-based*, espandere le loro capacità e aumentare le loro abilità.

Quando i robot condividono le informazioni/istruzioni disponibili, attraverso il cloud, si configura un fenomeno

up come Legal radar che monitora nel tempo l'evoluzione legislativa e propone variazioni contrattuali e Premonition che può indicare il miglior avvocato per la specifica causa in base a determinati parametri (tipologia di causa, numero di cause vinte, onorario, giudici assegnati ecc.). Il rapporto tra automazione e processo legale è affrontato dagli *scholars* fin dagli anni Sessanta. Cfr. F. Pasquale e G. Cashwell, *Four Futures of Legal Automation*, in *UCLA L. Rev. Disc.*, 63, 2015, p. 26.

[30] E. Guizzo, *Cloud Robotics: Connected to the Clouds, Robots Get Smarter*, in *Ieee Spectrum*, 2011, pp. 16-18. L'idea di connettere un robot a un personal computer esterno non è nuova: nel 1990 il prof. Masaki Inaba dell'Università di Tokyo aveva studiato il concetto del «remote brain», per indicare la separazione fisica tra i sensori e i motori dal software che permette di programmare le azioni.

che viene identificato come cloud robot[31]. In caso di danno provocato da robot, ciò complicherebbe l'onere probatorio: la Risoluzione, infatti, ha proposto di introdurre per determinate tipologie di robot una scatola nera che registri le informazioni circa le operazioni effettuate dalla macchina, e che hanno contribuito alle sue decisioni[32].

Le implicazioni di questa stretta interazione tra robot e rete appaiono di portata ancor maggiore. Un robot è costituito da un gran numero di sistemi e sottosistemi, si tratta di una rete, la quale, a sua volta, supporta un grandissimo flusso di informazioni. Secondo un approccio sistematico, infatti, il robot è una rete di parti fisiche che svolgono funzioni, ma l'essenza del robot è l'informazione «che vi scorre». Quindi, la connessione di un robot alla rete comporta un'espansione delle sue possibilità operative e delle azioni materiali che si possono costruire. Il cloud permette ai robot di accedere a un vasto sistema di risorse di dati che non potrebbero essere contenute nella loro memoria. Ecco, quindi, un nuovo modo di intendere il robot, non più come una macchina fisica tradizionale, autonoma oppure controllata da un operatore, ma come un insieme di parti, non necessariamente interconnesse fisicamente, ma collegate fra di loro attraverso l'informazione. Si può pensare a un sistema robotico intelligente che opera in un cantiere, in

[31] Il tema è stato oggetto del workshop *Connected Robots for Health: Challenges for Responsible Robot Design*, organizzato dalla Brocher Foundation, Ginevra 15-16 giugno 2017, report inedito.

[32] Il punto 12 dei «principi etici» della Risoluzione pone l'accento sul principio della trasparenza: dovrebbe sempre essere possibile conoscere la logica alla base di ogni decisione presa con l'ausilio dell'AI, la quale abbia un impatto rilevante sulla vita di una o più persone; ritiene che debba sempre essere possibile ricondurre i calcoli di un sistema di AI a una forma comprensibile per l'uomo. Il settore automobilistico, con l'auto a guida autonoma, è uno dei principali ambiti interessati. Vedi *infra* par. 7. La scatola nera è, altresì, funzionale ad allocare le responsabilità: secondo le indicazioni dell'Agenzia tedesca Reuters, se dalle registrazioni della scatola nera emerge che l'autista era al comando della vettura, allora quest'ultimo è responsabile per l'incidente in oggetto. Se, al contrario, al momento dell'incidente il sistema di guida autonoma era attivo, allora la colpa ricade sul costruttore della vettura.

cui gli occhi sono droni e le braccia ruspe, governato da un centro di comando che può anche essere dall'altra parte del pianeta[33].

Se i robot funzionano come delle piattaforme, adoperando un software *open source*, essi potrebbero essere manipolati da terzi eseguendo, così, programmi non controllabili dal produttore[34]. Il giurista è chiamato, sempre più spesso, ad allargare la prospettiva d'indagine.

A questo proposito, e solo al fine di guardare alle potenziali cause di malfunzionamento, pare utile tener conto che, nel campo degli studi dedicati all'interazione uomo-robot è stato elaborato uno schema di difetti dei robot a opera di Vasic e Billard[35]. Si tratta di una sorta di tassonomia dei difetti, ricostruita tenendo conto della specifica interazione uomo-robot, dove il malfunzionamento può derivare da difetti ingegneristici, errori umani, condizioni ambientali, e dall'interazione uomo-robot, o robot-robot, o robot-ambiente circostante.

3.1. *Le origini dei nuovi problemi: dalle caratteristiche tecniche a quelle funzionali*

Due tra le caratteristiche principali dei robot, elencate nell'introduzione, rappresentano, spesso, il punto di partenza di ogni analisi giuridica in materia: l'autonomia e la capacità di autoapprendimento.

[33] I calcolatori che implementeranno l'intelligenza di questo super robot potrebbero essere più d'uno. Tutti questi robot, collegati in cloud, costituiranno, di fatto, i vari livelli dell'intelligenza. Un esempio sono i centri di smistamento robotizzati di Amazon, dove gran parte del lavoro di immagazzinamento e trasporto delle merci viene svolto da robot collegati alla rete mondiale di gestione della produzione, della vendita e del trasporto dei prodotti commercializzati.

[34] Si tratta dell'ipotesi di rischio informatico. R. Calo, *Open Robotics*, in *Maryland Law Review*, 70, 3, 2011, consultabile all'indirizzo https://ssrn.com/abstract=1706293.

[35] M. Vasic e A. Billard, *Safety Issues in Human-Robot Interactions*, in *Proceedings of the 2013 Ieee-Ras International Conference on Robotics and Automation*, Karlsruhe, 6-10 maggio 2013.

In realtà, bisogna constatare che diversi livelli di entrambe danno vita ad applicazioni robotiche estremamente diverse tra loro: quando esse sono presenti a un livello elementare, le applicazioni risultano più «semplici»; laddove, invece, i livelli sono molto elevati, le applicazioni robotiche eseguono complesse sequenze di algoritmi, si pensi alla robotica sociale o alle macchine a guida autonoma (livello 3 e 4).

La prospettiva offerta dagli studi dedicati alla *human-robot interaction* appare, in particolar modo, utile al giurista per capire la natura e il grado di autonomia di un prodotto robotico. Secondo questi studi, l'autonomia robotica è un concetto ampio, che si riferisce alla capacità di svolgere compiti, processi e raggiungere obiettivi. Essa influisce sui compiti che la stessa macchina è in grado di compiere, sul livello e la frequenza delle interazioni con gli operatori umani, e sull'affidabilità con la quale un determinato robot può muoversi in un ambiente. La determinazione del grado di autonomia di una macchina non avviene per mezzo di una scienza esatta, sebbene le conoscenze della meccanica guidino i progettisti alla determinazione delle azioni da programmare. Gli esperti di *H-R interaction* sottolineano, inoltre, come sia importante chiedersi non tanto che cosa il robot fa, ma soprattutto che cosa potrebbe fare ed entro che limiti. Prospettive, queste ultime, sottese alla riflessione etica sulla desiderabilità sociale degli stessi[36].

Sebbene, dunque, sia preliminarmente importante identificare il grado di autonomia dell'artefatto, non esiste, al momento attuale, una classificazione ufficiale dei livelli di autonomia. Una distinzione diffusa è tra sistemi completamente autonomi e quelli semi-autonomi. I primi non utilizzano nessun comando esterno imposto da utilizzatori o altri sistemi, spesso sono robot che non hanno le sembianze di un robot. In agricoltura, un esempio è fornito dalle

[36] J.M. Beer, A.D. Fisk e W.A. Rogers, *Toward a Framework for Levels of Robot Autonomy in Human-robot Interaction*, in *Journal of Human-Robot Interaction*, 3, 2, 2014, pp. 74-99. Gli autori offrono un'utile ricostruzione sintetica del concetto di autonomia con riferimento alla letteratura robotica. Cfr. tabella 1 del saggio, p. 76.

forme più avanzate di giardino verticale in grado di gestire condizioni variabili: per esempio, attuare varie strategie per salvare una pianta in deperimento. I sistemi semi-autonomi dipendono dall'azione umana.

In ogni caso, va constatato che l'abilità di un robot di soddisfare obiettivi implica che la stessa macchina esegua numerose sequenze algoritmiche c.d. intermedie. A tal proposito, spesso, si sente affermare che il programmatore non necessariamente ha previsto, e anticipato, tutte le azioni che un robot potrebbe compiere, poiché è lo stesso robot a valutare i dati e gli impulsi ricevuti dal mondo esterno liberamente, per questo l'azione che ne risulta potrebbe essere inaspettata o imprevedibile. Tuttavia, questo assunto non pare condivisibile, poiché se una macchina sta eseguendo un programma per il quale era stata progettata, si pensi all'esempio del *ro-dog* che accompagna un non vedente, tutte le operazioni algoritmiche intermedie che compie sono esattamente quelle previste dal programmatore. Potrebbe, invece, essere la complessità della macchina e le diverse competenze richieste a complicare l'individuazione dei soggetti responsabili, direttamente, o in quanto vicari[37], per le decisioni o azioni robotiche[38].

In diversi ambiti, sono state proposte delle classificazioni dei gradi di autonomia. Il settore automobilistico (*infra* par. 7), e quello della chirurgia robotica forniscono due esempi[39].

[37] Sulla responsabilità vicaria, tra i tanti, si rinvia alla voce *Responsabilità per fatto altrui*, in R. Scognamiglio, *Noviss. Digesto it.*, XV, Torino, Utet, 1968, p. 699, il quale propone di utilizzare il criterio della pertinenza; e R. Ruffolo, *La responsabilità vicaria*, Milano, Giuffrè, 1976, pp. 111 ss.; e C.M. Bianca, *Diritto civile*, 5, *La responsabilità*, Milano, Giuffrè, 2015, p. 737.

[38] Così anche A. Bertolini, *Robots and Liability – Justifying a Change in Perspective*, in F. Battaglia, N. Mukerji e J. Nida-Rumelin, *Rethinking Responsibility in Science and Technology*, Pisa, Pisa University Press, 2014, pp. 143-166.

[39] P. Kazanzides, S. Martel, R.V. Patel, V.J. Santos, R.H. Taylor, G.-Z. Yang, J. Cambias, K. Cleary, E. Daimler, J. Drake, P.E. Dupont e N. Hata, *Medical Robotics – Regulatory, Ethical, and Legal Considerations for Increasing Levels of Autonomy*, in *Science Robotics*, 2, 2017, pp. 1-2. I vari gradi di autonomia sono stati oggetto di discussione durante la

La proposta formulata nel campo medico appare particolarmente significativa in quanto indica la direttrice lungo la quale il concetto di sicurezza evolve. In sintesi:

Livello 0. No autonomy. Questo livello include robot teleoperanti, o protesi, che rispondono ed eseguono il comando dell'utente.

Livello 1: Robot assistance. Il robot è una guida meccanica che assiste il chirurgo, il quale continua ad avere il pieno controllo del sistema.

Livello 2: Task autonomy. Il robot è autonomo per specifici compiti, solo «avviati» dal chirurgo, il quale mantiene un controllo più moderato (per esempio, nel caso di sutura, il robot potrebbe eseguire materialmente la stessa, mentre il chirurgo si limita a dare il comando iniziale per monitorare e intervenire in caso di necessità).

Livello 3: Conditional autonomy. Un sistema che «genera» strategie chirurgiche, ma lascia al chirurgo la facoltà di selezionarne una.

Livello 4: High autonomy. Il robot assume decisioni mediche ma sotto la supervisione di un medico qualificato.

Livello 5: Full autonomy. In questa ipotesi non c'è bisogno dell'azione umana, si tratta del c.d. «chirurgo robot» in grado di eseguire l'intera operazione chirurgica. È, al momento, solo in fase progettuale.

La grande differenza tra i diversi livelli di autonomia e, quindi, di complessità del sistema di chirurgia robotica permette, dunque, di delineare in che modo può evolvere il concetto stesso di sicurezza. Mentre, infatti, con riferimento ai primi livelli di autonomia, non vi è dubbio che si tratti di sicurezza da prodotto come tradizionalmente intesa, qualche dubbio sorge considerando il c.d. assistente robotico, il quale sarà in grado di eseguire tutta l'operazione chirurgica da sé: il dovere di garantire la sicurezza non è più riferito a un prodotto, ma si sviluppa in più fasi, poiché il robot esegue una prestazione.

roadmap on robotic autonomy, Dipartimento di informatica, Università di Verona, 30-31 ottobre 2017.

L'altra caratteristica che, almeno a una prima analisi, incide sulla valutazione degli elementi della fattispecie di responsabilità civile è da considerare entro i limiti dell'attuale stato dell'arte della ricerca (vedi cap. I, par. 2). L'apprendimento di una macchina deriva anche dall'interazione con l'ambiente esterno: il modo di percepire l'ambiente dipende dalla quantità e dalla qualità dei sensori attraverso i quali la macchina riceve le informazioni dall'ambiente esterno, e seleziona l'azione da compiere senza l'intervento umano[40]. È necessario, tuttavia, fare riferimento a due approcci tecnici seguiti per progettare l'AI: l'algoritmo genetico e la rete neurale. Quest'ultimo emula un sistema neuronale e la macchina basata su tale sistema, in pratica, impara procedendo per prove ed errori. Il giurista, in questo caso, dovrebbe essere consapevole che il *design* è plasmato dalla fase «esperienziale», più che da quella di programmazione. L'algoritmo genetico, invece, è metafora dell'evoluzione biologica. Si tratta di algoritmi che operano su un gruppo di potenziali soluzioni, applicando il principio della sopravvivenza del migliore. L'impossibilità di controllo sul risultato finale comporterebbe l'esclusione della responsabilità del programmatore per l'azione robotica[41].

A giustificare l'applicazione di un regime meno rigoroso di quello della responsabilità del produttore, in caso di danno da artefatto robotico[42], non sono solo le caratteristiche tecniche delineate, qualora considerate nei loro gradi più elevati[43], ma anche una considerazione sugli utilizzi cui sono destinati e sulle funzioni dei robot. Vi è già chi, infatti, ha

[40] La macchina porrebbe in essere «comportamenti emergenti», grazie all'interazione con l'ambiente e con le cose: in una parola, grazie all'esperienza. Cfr. R.C. Arkin, *Behavior-based Robotics*, Cambridge, The Mit Press, 1998.

[41] Il ragionamento è ampiamente spiegato da Bertolini, *Robots and Liability*, cit., p. 156.

[42] In ogni caso, va ricordato che anche per questi altri regimi, occorrerebbe dimostrare la difettosità del prodotto, ed è proprio questo elemento che presenta le sfide maggiori quando il danno deriva dal funzionamento degli algoritmi intelligenti.

[43] A creare tali dubbi sono i gradi più elevati di autonomia e capacità di autoapprendimento.

prospettato tale soluzione, distinguendo l'argomento c.d. ontologico, basato sulle differenti caratteristiche tecniche, da quello c.d. funzionale, basato su considerazioni di policy, e fondate sul rispetto di principi costituzionalmente garantiti[44]. L'esempio è, ancora una volta, quello delle protesi robotiche (*bionics*)[45]. La protesi robotica viene classificata come un dispositivo medico e ciò, quindi, è sufficiente, in linea di principio, ad applicare il regime di responsabilità da prodotto difettoso in caso di danno. Peraltro, per il tipo di interazione con l'apparato muscolo-scheletrico e con il sistema nervoso, la protesi robotica è spesso causa di malfunzionamenti non altrimenti evitabili.

A questo punto non resta che analizzare la vicenda secondo le due argomentazioni. Quella ontologica non giustificherebbe un regime diverso da quello oggettivo della responsabilità del produttore, poiché di per sé i gradi di autonomia e di autoapprendimento delle protesi non sono più elevati di altri dispositivi della stessa classe. Nonostante ciò, pare opportuno chiarire che le caratteristiche tecniche potrebbero, ugualmente, giustificare uno scostamento dai parametri generali: si tratta, infatti, di un oggetto sofisticato, connesso con il sistema nervoso centrale e l'accertamento del nesso di causa potrebbe, quindi, risultare complicato dal difetto nella captazione o nell'interpretazione del segnale nervoso[46].

L'argomento funzionale introduce una prospettiva diversa. Questo tipo di protesi innovative sono un ausilio di estrema utilità, poiché permettono al disabile di non rinun-

[44] M.R. Calo, *Open Robotics*, in *Maryland Law Rev.*, p. 70; Bertolini, *Robots and Liability*, cit., p. 144.

[45] Si tratta di un'ampia categoria, tra queste le protesi che modificano le caratteristiche strutturali e funzionali del sistema scheletrico e muscolare, gli esoscheletri. Non si tratta di apparati volti a sostituire delle parti fisiche mancanti, ma potrebbero dar luogo al fenomeno del c.d. *human enhancement*.

[46] Argomenti nel senso della specialità delle protesi robotiche rispetto alle regole di responsabilità si trovano in A. Bertolini, *Robotic Prostheses as Products Enhancing the Rights of People with Disabilities. Reconsidering the Structure of Liability Rules*, in *International Review of Law Computers & Technology*, 29, 2-3, 2015, pp. 116-136.

ciare alla piena realizzazione della sua vita sociale. In questo contesto, pertanto, un regime di responsabilità meno severo sarebbe giustificato da considerazioni di policy, dovute alle caratteristiche funzionali, e non strutturali, degli artefatti robotici. Si tratta, dunque, di un esempio di accettazione di un livello di rischio più elevato[47], che permette a chi indossa una protesi robotica di guidare[48], pur sapendo che un eventuale malfunzionamento, o errore del dispositivo medico, aumenterebbe le possibilità di causare incidenti.

3.2. *Gli umanoidi: cenni sull'impatto giuridico di antropomorfismo e illusione empatica*

Con lo sviluppo della robotica bioispirata e il conseguente intensificarsi della relazione robot-uomo, altri elementi potrebbero incidere nel determinare la sicurezza dei prodotti e nel configurare eventuali nuove circostanze che potrebbero dar atto a danni. Tali elementi sembrano risiedere nel rapporto che si instaura tra le varie tipologie di intelligenze: artificiale, emotiva e sociale[49].

Pare utile introdurre una preliminare definizione delle c.d. abilità cognitive dei robot, secondo le terminologie correnti diffuse nella comunità che si occupa di robotica[50]. In sintesi:

[47] A ben vedere, la situazione descritta rievoca la riflessione di G. Calabresi, *Il dono dello spirito maligno. Gli ideali, le convinzioni, i modi di pensare nei loro rapporti col diritto*, Milano, Giuffrè, 1996.

[48] Ciò non implica, necessariamente, che sia la vittima dell'incidente a dover sopportare i costi dell'incidente. Un piano di risarcimento *no fault*, per esempio, potrebbe evitare questa conseguenza.

[49] Il rapporto che lega AI ed emozioni umane, e le conseguenti implicazioni sociali, rappresenta un'area di indagine di crescente importanza. Si rinvia a C. Torsi, *Emozioni umane e Affective Computing emozioni umane in relazione all'intelligenza artificiale: 3 studi sperimentali*, Independently published, 2017.

[50] La ricognizione è operata da A. Santosuosso e B. Bottalico, *Autonomous Systems and the Law: Why Intelligence Matters. A European Perspective*, in E. Hilgendorf e U. Seidel (a cura di), *Robotics, Autonomics, and the Law. Legal Issues Arising from the Autonomics for Industry 4.0*

– per *cognitive robot* si intende un robot autonomo che esegue processi analoghi ai processi cognitivi umani sotto i seguenti profili: *i*) ragionamento; *ii*) programmazione; *iii*) apprendimento;

– per *social robots* agenti che fanno parte di un gruppo eterogeneo, e sono in grado di riconoscersi e di interagire;

– gli *evolutionary robots* impiegano un processo informatico evolutivo per adattarsi all'ambiente attraverso un processo analogo a quello dell'evoluzione naturale.

Si tratta, in sintesi, di una macro-categoria che, in considerazione dei sistemi avanzati di AI, potrebbe distinguersi per i seguenti profili: esecuzione di un'azione non prevista; l'effetto dell'antropomorfismo sull'uomo, e l'empatia che si crea tra uomo e robot. Gli umanoidi assomigliano sempre più all'uomo, grazie anche alla c.d. *soft-robotics*, ossia, l'uso di materiali morbidi per simulare le sembianze umane. Gli umanoidi sono al centro degli studi di *human-robot interaction*, e dell'emergente ambito della sociologia dei robot: alcuni studi esplorativi hanno evidenziato la tendenza dell'uomo a percepire i robot sociali in maniera diversa rispetto ad altri oggetti[51]. Più il robot è impiegato nella vita sociale, più è progettato per prendervi parte: questa tendenza ad attribuirgli caratteristiche e abilità simili a quelle umane dà luogo, ancora una volta, a questioni relative al *design* e considerazioni di policy[52]. L'antropomorfismo tende a far percepire i robot come cose viventi: è necessario, allora, capire se si debba regolare anche il comportamento delle persone che si rapportano con un robot. Le interazioni tra

Technology Programme of the German Federal Ministry for Economic Affairs and Energy, Baden-Baden, Nomos, 2017, p. 28, cui si rinvia per maggiori spiegazioni sulla classificazione qui proposta.

[51] H. Knight, *How Humans Respond to Robots: Building Public Policy through Good Design*, Brookings Report 2014; M. Saerbeck e C. Bartneck, *Attribution of Affect to Robot Motion*, in *Proceedings of the 5th Acm/Ieee International Conference on Human-Robot Interaction (Hri2010)*, Osaka, 2-5 marzo 2010, pp. 53-60.

[52] K. Darling, *Extending Legal Protection to Social Robots. The Effects of Anthropomorphism, Empathy, and Violent Behavior towards Robotic Objects*, in M. Froomkin, R. Calo e I. Kerr, *Robot Law*, Cheltenham, Edward Elgar, 2016.

uomo e robot sociale risultano già caratterizzate da molte «proiezioni»: il primo (uomo) tende ad ascrivere al secondo (robot) intenti e sentimenti. Le ricerche psicologiche rilevano che l'attaccamento emotivo al robot può essere sorprendentemente forte[53], per almeno tre motivi: la fisicità; la percezione di movimenti autonomi del robot che non sono tutti prevedibili dall'uomo; e il comportamento sociale. Tutto ciò avviene quando le persone non conoscono come funziona l'umanoide e, pertanto, sono inclini ad assimilare alla natura umana azioni che sono il risultato di algoritmi. E questo incide sul modo di rapportarsi con loro: il modo in cui le tecnologie sono impiegate è aspetto centrale per la sicurezza e per l'allocazione delle responsabilità, in particolar modo quando le parti che interagiscono con i robot sono minori e anziani, cioè soggetti vulnerabili.

Da circa un anno, ad esempio, nel reparto di pediatria dell'Azienda ospedaliera di Padova, un robottino umanoide, Pepper, aiuta i bambini accompagnandoli nei corridoi, o facendo loro compagnia nell'attesa di un intervento o nel corso di una terapia, parlando, giocando, e reagendo alle loro emozioni. Si tratta della *robot-therapy* già utilizzata negli ospedali giapponesi, canadesi, svizzeri, belgi, francesi e introdotta al fine di migliorare l'umore dei giovani pazienti, e di calmare gli stati d'ansia che precedono e accompagnano esami diagnostici e chirurgici invasivi[54]. I responsabili della *robot-therapy* hanno, per esempio, notato che è importante la scelta di un modello di robot che sia, in proporzione, più basso rispetto al bambino di cui si prende cura: con bambini di 3 anni viene, dunque,

[53] S. Turkle, *In Good Company?: On the Threshold of Robotic Companions*, in Y. Wilks (a cura di), *Close Engagements with Artificial Companions: Key Social, Psychological, Ethical and Design Issues*, Philadelphia, John Benjamins, 2010, p. 24.

[54] Vi è chi ha osservato che questo tipo di robot, detti badanti o assistenti artificiali, non sono macchine pronte all'uso ma, al contrario, richiedono un periodo di training per poter imparare a svolgere le funzioni per le quali sono state programmate, proprio come accade per lo stagista che si accinge ad apprendere un nuovo lavoro. Cfr. Pagallo, *Il diritto nell'età dell'informazione*, cit., p. 303.

utilizzato il modello alto 90 cm; mentre con bambini più grandi si utilizza il modello alto 120 cm. Questo perché i bambini si spaventano se si rapportano con un Pepper che supera la loro altezza[55].

L'interazione potrebbe creare le condizioni per «orientare» i comportamenti umani e indurli a compiere determinate azioni giuridicamente rilevanti. In altri termini, attraverso l'illusione empatica che si può instaurare nell'uomo che si rapporta con il robot. Quest'ultimo può influire sulla fiducia di soggetti vulnerabili[56]. Per di più, va considerato che la manipolazione del soggetto avviene attraverso la società che controlla l'hardware o il software del robot e che ha accesso ai dati che permettono di esplorare il tipo di relazione creatasi[57].

Quanto fin qui osservato pone al centro il rapporto tra adempimento dei doveri di informazione e di avvertenza del produttore e la colpa del danneggiato-utilizzatore del prodotto, destinatario, appunto, delle informazioni e avvertenze circa la condotta da tenere per ridurre o evitare i rischi. Com'è già stato ricordato con specifico riferimento al contesto dei prodotti hi-tech «tutti gli approcci [alla responsabilità] dovrebbero tener conto delle azioni della persona che utilizza la tecnologia e dovrebbe identificare in modo più preciso quale debba essere il ruolo degli utilizzatori della

[55] Intervista a Roberto Mancin, responsabile sviluppo di sistemi e tecnologie informatiche innovative presso il Dipartimento di salute della donna e del bambino dell'Università degli Studi di Padova, 12 marzo 2018. Già nel 2016, il robottino umanoide Nao era stato ospite del reparto di Cure palliative e terapia antalgica pediatrica della stessa azienda. Attualmente il modello più evoluto di Pepper è Sanbot.

[56] Una decisione, in risposta a una *class action* del *District Court for the Eastern District of Missouri*, ritenne sussistere gli estremi per il reato di frode nell'impiego di un computer in grado di simulare l'interazione umana. Cfr. *In re Ashley Madison Customer Data Sec. Breach Litig.*, n. 2669 (United States Judicial Panel on Multidistrict Litigation, 12 settembre 2015).

[57] Si pensi, per inciso, anche ai costi elevati di riparazione dei robot che i produttori potrebbero imporre, proprio facendo leva sul legame affettivo che l'uomo instaura con il robot.

medesima tecnologia»[58]. *Ex* art. 122 cod. cons., il risarcimento del danno causato dal prodotto è ridotto o escluso se l'utilizzatore, conoscendo o dovendo conoscere il rischio non lo abbia evitato, adottando le idonee cautele. Nel caso del prodotto umanoide, l'informazione circa le peculiarità, la natura e la sicurezza dello stesso dovrebbe essere tale da non indurre in errore il consumatore e da tutelare il suo diritto di scelta e di autodeterminazione.

Particolare rilievo assume, inoltre, l'informazione nelle strategie di *marketing*: qualora essa faccia leva sui tratti dei robot sociali, senza metterne in luce la reale natura, potrebbe risultarne un'informazione commerciale ingannevole ai fini della configurazione di una pratica commerciale scorretta ai sensi della Direttiva 2005/29/CE[59].

4. *Robot e standard tecnici di sicurezza*

Gli standard tecnici di sicurezza armonizzati sono lo strumento principale al quale i giudici dovrebbero far riferimento per valutare il livello di rischio che i consumatori devono accettare[60]. Il duplice obiettivo degli standard è quello di: contenere la discrezionalità dei giudici, da un

[58] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al comitato delle regioni, *Costruire un'economia dei dati europea*, Com(2017) 9 final.

[59] Migliorare la trasparenza è uno degli obiettivi chiave sottesi all'etica dei sistemi intelligenti e autonomi. Cfr. Anna Spagnolli (professore associato di Psicologia sociale), intervistata da me, il 18 marzo 2018, Università di Padova, centro Hit.

[60] Il tema della normazione tecnica ha occupato prima gli economisti e poi i giuristi. La letteratura giuridica è vastissima. Per norma tecnica si intende quella «approvata da un organismo riconosciuto e abilitato ad emanare atti di normazione la cui osservanza non sia obbligatoria». Per un contributo chiave in materia si rinvia a U. Carnevali, *La norma tecnica da regola di esperienza a norma giuridicamente rilevante. Ricognizione storica e sistemazione teorica. Ruolo dell'Uni e del Cei*, in *Resp. civ. e prev.*, 1997, p. 257; e L. Montanari, *I poteri normativi degli organismi tecnico-scientifici*, in G. Comandé e G. Ponzanelli (a cura di), *Scienza e diritto nel prisma del diritto comparato*, Torino, Giappichelli, 2004, pp. 445 ss.

lato; e bilanciare la protezione degli utilizzatori con la responsabilità del produttore, dall'altro[61].

A partire dalla metà degli anni Ottanta, ovvero dall'esordio sulla scena europea della strategia regolatoria di «nuovo approccio»[62], o «approccio globale»[63], la normazione tecnica ha garantito l'armonizzazione degli standard di sicurezza per i prodotti immessi in commercio. Ha, quindi, assunto un ruolo preminente rispetto ai prodotti ottenuti con le tecniche più innovative, caratterizzati dal mutevole flusso di informazioni circa la natura dei rischi e i relativi metodi di valutazione. Si tratta, infatti, di standard definiti in base alle conoscenze tecniche più avanzate del momento. Essi promuovono un efficiente funzionamento del mercato ed evitano lo squilibrio competitivo tra gli operatori di uno

[61] In merito all'importanza degli standard in robotica si è espressa C. Amato, nella relazione tenutasi durante il Münster Colloquium (Germania), vedi p. 11 nota 10. La relatrice esprime la necessità di includere previsioni di legge sulla *post-market surveillance* in una eventuale riforma della Direttiva *Liability 2.0*. Si rinvia a C. Amato, *Product Liability and Product Security: Present and Future*, in Atti di Münster Colloquium, in corso di pubblicazione.

[62] Quale conseguente azione legislativa alla nota sentenza *Cassis de Dijon* (Corte di giustizia, 20 febbraio 1979, Rewe-Zentral AG/Bundesmonopolverwaltung für Branntwein (120/78, Racc., p. 649)), la tecnica legislativa del «nuovo approccio» è stata approvata dal Consiglio dei ministri il 7 maggio 1985 nella *Risoluzione relativa a una nuova strategia in materia di armonizzazione tecnica e normalizzazione*, in *GU C*, 136, del 4 giugno 1985, p. 1. I principi fondamentali di questa nuova strategia sono stati poi recepiti nel Libro verde per il perfezionamento del mercato unico del 1985. Cfr. A. Cordiano, *Sicurezza dei prodotti e tutela preventiva dei consumatori*, Padova, Cedam, 2005, pp. 12 ss.

[63] Nel 1989 e nel 1990 il Consiglio ha, quindi, adottato una Risoluzione sull'approccio globale e la Decisione 90/683/Cee, contenente gli orientamenti generali e le procedure dettagliate per la valutazione della conformità, aggiornata e sostituita dalla Decisione 93/465/Cee del Consiglio, del 22 luglio 1993, concernente i moduli relativi alle diverse fasi delle procedure di valutazione della conformità e le norme per l'apposizione e l'utilizzazione della marcatura CE di conformità, da utilizzare nelle direttive di armonizzazione tecnica (*GU L*, 220, del 30 agosto 1993, p. 23), a sua volta abrogata e aggiornata dalla Decisione 768/2008/CE, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti (*GU C*, 282, del 25 novembre 2003, p. 3).

spazio economico comune, predisponendo livelli di sicurezza ragionevole e accettati dal mercato internazionale[64].

Gli standard abbattono, dunque, le barriere tecniche e normative alla libera circolazione dei prodotti per assicurare ai consumatori livelli minimi e uniformi di sicurezza e ridurre, per quanto possibile, l'inevitabile scarto tra il dato normativo e una realtà economica e sociale in continua e rapidissima evoluzione[65]. La *Blue Guide on the Implementation of EU Product Rules* del 2014[66] e i lavori per il Partenariato transatlantico per il commercio e gli investimenti hanno, infatti, enfatizzato tale loro ruolo nel mercato globale[67].

L'impiego di dettagliati standard tecnici è alla base della normativa europea, sia quella di settore, che quella orizzontale sulla sicurezza generale dei prodotti[68]: norme

[64] Sul concetto di sicurezza ragionevole si rinvia a E. Al Mureden, *Il danno da «prodotto conforme». Le soluzioni europee e statunitensi nella prospettiva del Transatlantic Trade and Investments Partnership*, in *Contratto e Impr.*, 2, 2015, p. 38.

[65] U. Carnevali, *La norma tecnica da regola di esperienza a norma giuridicamente rilevante. Ricognizione storica e sistemazione teorica del ruolo dell'Uni e del Cei*, in *Resp. civ. prev.*, 1997, p. 257; G. Smorto, *Certificazione di qualità e normazione tecnica*, in *Dig. IV, disc. priv., sez. civ.*, Aggiornamento, I, 2003, pp. 205 ss.; F. Ancona, *Normazione tecnica e certificazione di qualità. Elementi per uno studio*, in *Cons. Stato*, 1994, p. 1563.

[66] European Commission, *The Blue Guide on the Implementation of EU Product Rules*, 2014, p. 14.

[67] Per un esame dello stato dell'arte sulle trattative si rinvia a http://ec.europa.eu/trade/policy/in-focus/ttip/index_it.htm.

[68] L'importanza dell'armonizzazione degli standard di sicurezza dei prodotti è indirettamente testimoniata dai tentativi di concludere il *Transatlantic Trade and Investment Partnership* (Ttip) o Partenariato Transatlantico per il commercio e gli investimenti. A tal proposito è già stato posto in evidenza che «l'analisi comparatistica del sistema della sicurezza dei prodotti e della responsabilità del fabbricante nell'Unione europea e negli Stati Uniti assume una valenza che va ben oltre la finalità di individuare elementi di differenziazione e punti di contatto; essa, nella prospettiva di uniformazione degli *standards* di sicurezza richiesti ai fini dell'immissione in commercio dei prodotti in uno spazio economico comune, appare un imprescindibile presupposto per l'individuazione di questioni già da tempo emerse nell'ordinamento statunitense e non ancora compiutamente delineate nel nostro sistema legislativo e giurisprudenziale. Tra queste, merita particolare attenzione

tecniche, armonizzate e formulate, pertanto, da organismi tecnici e di certificazione, a cui la normativa fa rinvio[69], o direttamente incluse tra gli allegati. Essi definiscono le caratteristiche strutturali che il prodotto deve presentare per poter essere definito sicuro, includendovi anche le definizioni, la scelta dei metodi di valutazione del rischio, le soglie di accettabilità dello stesso.

Le norme tecniche, per lo più espressione di procedimenti di *self-regulation* o *co-regulation*, sono dettate da organismi tecnico-scientifici e si sostituiscono, o affiancano, alle più rigide procedure di controllo preventive. Gli organismi di normazione sono presenti a livello mondiale (Iso), europeo (Cen, Cenelec, Etsi) e nazionale (Uni, Cei).

Come accade in altri settori hi-tech, si pensi a quello digitale[70], anche nell'ambito della robotica, la normazione tecnica è presente da più di trent'anni[71]. Peraltro, un breve *excursus* storico dell'evoluzione della stessa indica, non solo i grandi cambiamenti e sviluppi che hanno caratterizzato il progresso in robotica, ma, soprattutto, i problemi cruciali che hanno contraddistinto il settore, nel passaggio fondamentale dalle applicazioni a uso industriale a quelle di natura sociale e collaborativa.

I pericoli associati ai robot dipendono dal tipo di AI «embedded». Pertanto, la definizione dello standard non è operazione agevole. Le norme designate per robot in determinati contesti, come quelli industriali, possono garantire la

quella della responsabilità del fabbricante per i danni cagionati da un prodotto conforme a *standards* di sicurezza legislativi». Così E. Al Mureden, *La sicurezza dei prodotti e la responsabilità del produttore*, Torino, Giappichelli, 2017, p. 4.

[69] La Comunicazione della Commissione nell'ambito dell'applicazione della Direttiva 2006/42/CE del Parlamento europeo e del Consiglio relativa alle macchine e che modifica la Direttiva 95/16/CE. Si veda anche la Comunicazione 2018/C 092/01 del 9 marzo 2018.

[70] Per un esempio, si pensi all'impiego diffuso degli standard tecnologici in contesti digitali, cfr. G. Pascuzzi, *Il diritto dell'era digitale*, Bologna, Il Mulino, 2016, p. 347.

[71] Per la sicurezza dei robot industriali, il corrispondente organo internazionale è il gruppo di lavoro Iso/TC 299 WG3.

sicurezza solo relativamente a questi contesti[72], mentre, invece, difficilmente la tutelano in altri, si pensi al robot collaborativo e a tutti i profili specifici della *human-robot interaction*.

Nella predisposizione della normativa tecnica, il passaggio dalla diffusione della robotica industriale a quella dei servizi è, dunque, cruciale, tanto che, fino al 2014, l'Iso aveva predisposto solo standard di sicurezza per robot industriali. Poi, le norme Iso 13482:2014, dedicate ai *Robots and robotic devices – Safety requirements for personal care robots* hanno specificato i requisiti per una progettazione sicura, misure di protezione e utilizzo di *personal care robots* (con particolare riguardo ai *personal care robot*, *mobile servant robot*, *physical assistant robot*, *person carrier robot*): questi robot eseguono *tasks* per migliorare la qualità di vita, a prescindere dall'età e dalle capacità degli utenti. In queste ipotesi, pertanto, per ridurre i rischi associati all'uso dei robot entro una soglia accettabile, è necessario considerare l'interazione uomo-macchina. Le modalità collaborative implicano, infatti, l'accesso continuo allo spazio di lavoro e la possibilità di interazione fisica con il sistema robotizzato attraverso contatti volontari o accidentali. L'analisi dei rischi deve avvenire in relazione a tutto il sistema robotizzato, compresi il layout e il comportamento dell'operatore. Il tipo di protezione da adottare nell'uso del robot collaborativo – ad esempio una limitazione di velocità – è molto diverso da quello usato per i robot industriali (es. predisposizione di spazi c.d. *safeguarded*), dove il sistema robotizzato non è operativo in presenza dell'operatore. Tale evoluzione è ancor più marcata dopo la pubblicazione degli Iso/TS 15066:2016 recanti «Raccomandazioni per la valutazione del rischio in accordo con la Direttiva macchine – Progettazione di posti di lavoro

[72] L'*International Organization for Standardization* classifica i pericoli in base alla fonte: pericoli meccanici possono derivare da movimenti inattesi, uso incontrollato di un attrezzo, movimenti rotatori, incastro nelle macchine robotiche di vestiti o capelli ecc., pericoli elettrici, originati, per esempio, da contatto tra cavi elettrici e persona, o l'esposizione alla tensione elettrica; pericoli associati a superfici calde o esposizioni ad alte temperature richieste dallo specifico processo produttivo industriale, radiazioni ecc.

con robot collaborativi (cobots)». Si tratta di una specifica tecnica (Uni EN Iso 10218-2:2011) dedicata ai requisiti di sicurezza relativi alle modalità collaborative, armonizzate dalla Direttiva Macchine 2006/42/EC[73].

L'evoluzione nei contenuti degli standard conferma, dunque, che le nuove opportunità dovute alla stretta interazione tra uomo e robot sono gli aspetti più critici da validare in termini di sicurezza. Questo passaggio ha configurato scenari completamente diversi da quelli esistenti, comportando la necessità di ripensare alle definizioni, alle nuove questioni di sicurezza nella sempre più stretta interazione uomo-robot e al conseguente problema di regolamentare un robot come una macchina, o altro. Con l'evolvere del settore e delle tipologie di artefatti, la stessa interazione uomo-robot è divenuta, quindi, importante al fine di assicurare l'adeguamento dei requisiti di sicurezza[74].

4.1. *Il danno da artefatto robotico conforme agli standard di sicurezza*

Si può presumere che, analogamente a quanto avviene per gli *unavoidable unsafe products*, anche i prodotti robotici potrebbero, frequentemente, configurare l'ipotesi di danno da prodotto conforme agli standard[75].

Gli standard di sicurezza armonizzati sono considerati – nei termini della *Blue Guide on the Implementation of EU Product Rules*[76] – il *trait d'union* tra le norme della

[73] Iso/TS 15066:2016, *Robots and Robotic Devices – Collaborative Robots*.

[74] G.S. Virk, *The Role of Standardisation in the Regulation of Robotic Technologies*, in E. Palmerini e E. Stradella, *Law and Technology. The Challenge of Regulating Technological Development*, Pisa, Pisa University Press, 2013, pp. 311 ss.

[75] Sul tema dei danni da prodotti conformi agli standard si rinvia a E. Al Mureden, *Il danno da prodotto conforme*, Torino, Giappichelli, 2016.

[76] European Commission, *The Blue Guide on the Implementation of EU Product Rules*, cit., p. 12. In particolare si veda il paragrafo «1.2.3 How the system fits together».

responsabilità del produttore e quelle della sicurezza dei prodotti[77]. Ciò presuppone di muovere dalla fondamentale, e ormai ben nota, distinzione tra prodotto difettoso e prodotto dannoso: il primo è un prodotto non conforme alle caratteristiche previste dagli standard, e solo in alcune circostanze può assumere un carattere dannoso; il secondo si riferisce a un prodotto che, nonostante sia pienamente conforme alle caratteristiche tecniche, presenta significativi margini di dannosità (es. farmaci e cosmetici).

In robotica pare difficile, per il fabbricante, valutare le probabilità dell'accadimento dannoso e quando esso sia la risultante di un'azione eseguita dalla macchina, in virtù del processo di autoapprendimento, se già in stato avanzato. Il risultato di un'operazione di calcolo può essere identificato come l'origine del difetto? Non vi è, rispetto a molte applicazioni, precedente *expertise* su tecnologie simili. Lo standard è il mezzo più funzionale per valutare se il *design* è stato realizzato a regola d'arte.

La questione del danno da prodotto conforme ha occupato, varie volte, le aule dei tribunali italiani, spesso come problema sottotraccia di altri. Non vi è un orientamento uniforme. In molte decisioni viene omesso completamente il riferimento agli standard tecnici che sarebbero, invero, disponibili in materia, facendo, invece, ricorso alla presunzione di sicurezza generale[78].

Vi è, poi, un altro gruppo di decisioni giurisprudenziali, che, in luogo della lettura sistematica delle norme indicate, optano per l'applicazione della norma di cui all'art. 2050 c.c.[79].

[77] Al Mureden, *La sicurezza dei prodotti e la responsabilità del produttore*, cit., p. 26. L'autore osserva che l'analisi della casistica giurisprudenziale in materia di danni da prodotto fa emergere proprio la «limitatissima propensione ad operare una lettura sistematica e coordinata delle norme».

[78] Così emerge dalla *Blue Guide on the Implementation of EU Product Rules*, cit., p. 10.

[79] Tra i tanti cfr. Cass., 4 giugno 1998, n. 5484, in *Studium Juris*, 1998, p. 1119 sui danni cagionati dallo scoppio di bombole a gas; o Trib. Salerno 2 ottobre 2007, in *Rass. dir. farmaceutico*, 2008, p. 29 sui danni da farmaco.

Solo un numero esiguo di sentenze interpreta la difettosità del prodotto alla luce degli standard presenti in materia, rifiutando l'equazione «rispetto della soglia = presunzione di non dannosità»[80].

Anche la dottrina si è espressa in modo non unanime[81]. Una parte fa leva sulla possibilità che il produttore, in quanto *best risk avoider*, attui tutte le misure precauzionali, secondo le conoscenze tecnoscientifiche più aggiornate, per evitare il danno. Altra parte ha, invece, evidenziato che tale ruolo del produttore potrebbe essere valido con riferimento a determinati ambiti, come i farmaci, ma non ad altri, come la produzione dei veicoli[82].

Tuttavia, nell'*Affaire Pip* in materia di dispositivi medici difettosi, la Corte di Giustizia europea[83], adita sul «contiguo» aspetto della responsabilità dell'organismo di certificazione, ha affermato la responsabilità di tali organi per il mancato rispetto di un livello di diligenza che vada al di là degli obblighi di legge, per adottare tutte le misure di precauzione che si rendano effettivamente necessarie per prevenire il rischio e assicurare il massimo livello di sicurezza.

Nella prospettiva del produttore, il problema è stabilire se il rispetto degli standard legislativi costituisca un «limite massimo» di sicurezza esigibile, conseguito il quale non può ravvisarsi alcuna responsabilità dello stesso; oppure, se esso rappresenti solamente un «limite minimo», necessariamente richiesto per la commercializzazione del prodotto, ma non

[80] In materia di danni cagionati da prodotti cosmetici v. Cass., 15 marzo 2007, n. 6007, in *Resp. civ. e prev.*, II, 2007, p. 1587, con nota di Gorgoni, *Responsabilità per prodotto difettoso: alla ricerca della (prova della) causa del danno.*

[81] Tutti gli orientamenti sono ricostruiti e proposti da Al Mureden, *Il danno da prodotto conforme*, cit. In tema vedi anche A. Genovese, *Il mercato dei dispositivi medici. Precauzione, sicurezza e responsabilità*, in *Contr. e impr./Europa*, 1, 2010, pp. 319 ss.

[82] Al Mureden, *Il danno da prodotto conforme*, cit.; R. Nader e J.A. Page, *Automobile Design Liability and Compliance with Federal Standards*, in *Geo. Wash. L. Rev.*, 64, 1996, p. 415 e P. Pardolesi, *Profili comparatistici di analisi economica del diritto privato*, Bari, Cacucci, 2015.

[83] Corte giustizia UE, 16 febbraio 2017, causa C-219/15, in *NGCC*, 2017, pp. 1244 ss., con nota di F. Caroccia.

sufficiente a escludere la persistenza di obblighi risarcitori in capo al fabbricante.

Tutte queste diverse interpretazioni giurisprudenziali della medesima questione non si verificano nell'ordinamento americano, grazie all'operatività della clausola della *preemption*, la quale consente un'applicazione più omogenea delle regole operazionali.

5. *Profili di responsabilità civile*

Sullo sfondo delle brevi note di apertura circa il rapporto *torts and innovation*, mi accingo qui a condurre a un passo successivo la riflessione sui profili di responsabilità civile. Ciò al fine di capire se le difficoltà di accertare le responsabilità per le caratteristiche strutturali e funzionali intrinseche alla robotica (par. 3.1), e ai robot collaborativi (par. 3.2), inducano a introdurre nuovi paradigmi, ovvero adattamenti funzionali a riconciliare le molteplici funzioni della responsabilità civile con gli incentivi all'innovazione[84]. Vari contesti applicativi esemplificheranno tale riflessione. Saranno, invece, oggetto di una trattazione specifica i profili di sicurezza e responsabilità del produttore delle *driverless cars* (*infra* par. 7).

Le attenzioni della dottrina si sono concentrate sul c.d. *responsibility gap*. A seconda delle circostanze, e dei sistemi giuridici, diversi regimi giuridici possono essere applicabili. È possibile tracciare una distinzione generale tra i regimi dei settori specifici e quelli a carattere generali. I primi vengono in esame ogni volta in cui IoT e l'AI sono impiegate in un ambito coperto da tali specifici regimi. I secondi concernono la responsabilità da prodotto e la responsabilità per colpa. L'impatto della robotica si manifesta, però, anche in relazione alla configurazione della fattispecie di responsabilità. Ciò che le caratteristiche tecniche e funzionali della robotica sembrano minare è la corrispondenza

[84] J. Morgan, *Torts and Technology*, in R. Brownsword, E. Scotford e K. Yeung, *The Oxford Handbook of Law, Regulation and Technology*, Oxford, Oxford University Press, p. 522.

tra possibilità di controllo, capacità di evitare il danno e relativa imputazione della responsabilità. In estrema sintesi, detto impatto si manifesta sotto i seguenti profili.

a) Valutazione degli elementi costitutivi della fattispecie.

Tradizionalmente, lo sviluppo tecnoscientifico ha comportato un ripensamento di alcune tra le categorie fondanti della fattispecie di responsabilità[85].

L'accertamento della sequenza causale si presenta come uno dei profili più critici in robotica[86], la quale si compone di artefatti ingegnerizzati, software e sistemi di controllo artificiale, arricchendoli di «cognizione» e capacità decisionale. Nella sua forma più debole questa sequenza logica esprime un nesso di causa tra condotta/omissione dell'agente ed evento di danno; nelle ipotesi di responsabilità per colpa mette in luce anche una rimproverabilità soggettiva dell'agente[87]. Si pensi all'individuazione del nesso causale o, in prospettiva futura, alle peculiarità del machine learning[88], e del controllo su macchine che sono programmate per porre in essere azioni autonome.

b) L'onere della prova.

Rappresenta uno dei profili più complessi nei giudizi di responsabilità concernenti la robotica avanzata. La casistica in materia di chirurgia robotica ha, già da tempo, messo in evidenza che la prova del malfunzionamento del robot

[85] R. Montinaro, *Dubbio scientifico e responsabilità civile*, Milano, Giuffrè, 2012, p. 155.

[86] Per uno studio approfondito in materia di nesso eziologico si rinvia a R. Pucella, *La causalità «incerta»*, Torino, Giappichelli, 2007. Si pensi alla difficoltà di individuare la *proximate cause* (causa prossima), la quale indica la vicinanza minima necessaria tra l'atto del danneggiato e l'incidente occorso a giustificazione dell'attribuzione di responsabilità. Si tratta di un giudizio c.d. valoriale non fattuale: «esso è una limitazione intellettuale ed artificiale di un corso di eventi di per sé naturalisticamente più ampio». Così P.G. Monateri, D. Gianti e M. Balestrieri, *Causazione e giustificazione del danno*, Torino, Giappichelli, 2016, p. 30.

[87] E. Palmerini, *Robotica e diritto: suggestioni, intersezioni, sviluppi a margine di una ricerca europea*, in *Resp. civ. e prev.*, 6, 2016, p. 173.

[88] Per un'analisi del problema dell'autonomia, della prevedibilità, della causalità e del controllo si rinvia a M.U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, in *Harvard Journal of Law & Technology*, 29, 2, 2016, pp. 353-400.

chirurgico costituisce una *probatio diabolica*. D'altro canto, casi di danni da dispositivo medico, come per esempio quelli in materia di protesi mammarie difettose[89], manifestano analoghe difficoltà probatorie che danno luogo ai diversi orientamenti giurisprudenziali. È, però, l'algoritmo a rappresentare la principale fonte di criticità sul fronte probatorio (vedi *infra*).

c) La distribuzione delle responsabilità tra i diversi soggetti interdipendenti nella complessa catena di produzione.

Nella messa a punto e nell'impiego degli stessi prodotti robotici intervengono molteplici professionalità e utilizzatori, sia in modo sincronico che diacronico. Ciò rende difficile attribuire con certezza una specifica condotta a un determinato soggetto all'interno di un contesto di gruppo (responsabilità stocastica). Si configurerebbe, così, l'ipotesi del c.d. danno anonimo, il quale priva di risarcimento i danneggiati[90].

Anche la responsabilità d'équipe assume tratti *sui generis*, visto che la prospettiva offerta dal progresso è quella di un ambiente di lavoro sempre più «collaborativo» tra lavoratori e robot. Nel caso di impiego del c.d. deep learning, per esempio, i robot sono in grado di essere proattivi, presentando proposte al team con il quale collaborano[91]. La collaborazione uomo-robot può anche avvenire per mezzo del robot c.d. «indossabile», una sorta di esoscheletro, come ad esempio un guanto meccanico che aiuta l'operaio alleggerendo il peso gravante sulla persona del lavoratore.

[89] Per due diversi orientamenti si vedano: *Foster v. Biosil*, n. 59 (Central London County Court, 19 aprile 2000); *Tesco Stores Ltd v. Pollard*, n. 393 (Court of Appeal, 12 aprile 2006). Per un'analisi puntuale si rinvia ad Amato, *Product Liability and Product Security*, cit.

[90] Sul danno anonimo si rinvia a P.G. Monateri, D. Gianti e M. Balestrieri, *Causalità e giustificazione del danno*, in P.G. Monateri (a cura di), *Trattato sulla responsabilità civile*, Torino, Giappichelli, 2016.

[91] È il caso di Baxter, il robot prodotto da Rethink Robotics, azienda americana – start up nel 2012 – che oggi produce robot collaborativi per il settore industriale. Baxter è stato progettato per operare in team misti di lavoro, lavoratori e robot insieme, e viene definito un modello di *learn by doing* per le modalità di autoapprendimento che attua.

Il *gap*, poi, sembrerebbe configurarsi con riguardo alla figura del programmatore, il cui ruolo evolve[92]: passa dalla programmazione tradizionale di un software ingegneristico, alla costruzione di sistemi autonomi di AI[93]. Il *by design* (vedi *retro* cap. I e *infra* par. 7) serve allora a «codificare» regole di condotta ed etiche sulle modalità di interazione con l'uomo e con l'ambiente. È sovente oggetto di richiami un esempio di «codice» proveniente dal mondo fantascientifico, formulato dallo scrittore e biochimico Asimov settantacinque anni fa: si tratta delle note tre leggi di Asimov[94], spesso punto di partenza per la riflessione roboetica.

d) L'«intersezione» tra sicurezza dei prodotti e sicurezza dei sistemi informatici.

Con l'interoperatività e interconnessione dei robot per mezzo dello sfruttamento delle risorse contenute nel cloud, si delinea sempre più nitida la zona di interazione tra sicurezza dei prodotti e sicurezza informatica[95]. Questo profilo

[92] A. Matthias, *The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata*, in *Ethics and Information Technology*, 6, 2004, pp. 175-183.

[93] Il successo dell'apparato di regole e (più in generale) dell'intero sistema che si trova a fronteggiare la situazione di incertezza rispetto al nuovo rischio, si misura, quindi, nella capacità di superare, nel più breve tempo possibile, la crisi del processo decisionale per elaborare e implementare le misure maggiormente idonee a gestire il rischio. Cfr. Izzo, *La precauzione nella responsabilità civile*, cit. Il ragionamento era riferito al danno da contagio, ma appare estendibile, in generale, al rischio tecnologico.

[94] I. Asimov, *Circolo vizioso*, New York, Street & Smith, 1942. Prima Legge: «Un robot non può recar danno a un essere umano né può permettere che a causa del proprio mancato intervento un essere umano riceva danno». Seconda legge: «Un robot deve obbedire agli ordini impartiti dagli esseri umani purché tali ordini non contravvengano alla prima legge». Terza legge: «Un robot deve proteggere la propria esistenza purché questo non contrasti con la prima e la seconda legge». Successivamente, nel romanzo *Io Robot*, l'autore aggiunse una quarta legge, superiore per importanza a tutte le altre ma valida solo per gli automi più sofisticati, definita legge zero: «Un robot non può recar danno all'umanità e non può permettere che, a causa di un suo mancato intervento, l'umanità riceva danno».

[95] Per una sintesi sulla sicurezza dei sistemi informatici che delinea le molte sfaccettature del tema vedi Pascuzzi, *Il diritto dell'era digitale*, cit., pp. 349 ss.

complica notevolmente l'oggetto d'esame ed è, infatti, tra i temi di studio della Comunicazione della Commissione del 25 aprile 2018.

5.1. *La responsabilità da prodotto: il concetto di difettosità si confronta con le caratteristiche della robotica*

Nella prospettiva della responsabilità da prodotto robotico, il giurista si chiede, preliminarmente, quali rischi potrebbero reificarsi in difetti[96].

Secondo la tradizionale tripartizione dei difetti[97], dal carattere essenziale nell'ordinamento americano[98], e soltanto descrittivo nel contesto europeo[99], si distinguono: *i*) difetti legati a vizi di progettazione/programmazione o design, come le disfunzioni delle componenti meccaniche, degli attuatori del sistema elettronico o dei problemi del software; *ii*) vizi di produzione; *iii*) difetti di informazione, istruzioni e formazione del personale addetto, i quali hanno già, massicciamente, occupato le aule giudiziarie americane nell'ambito specifico della chirurgia robotica[100].

[96] Ragionamento, quest'ultimo, che sembrerebbe estendibile anche ai rischi che si concretizzano nel contesto dell'IoT.

[97] 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, in *OJ L*, 210, 7 agosto 1985, pp. 29-33.

[98] I tre tipi di difetti sono: *failure to warn*, *design defect*, *manufacturing defect*. Cfr. *Restatement (Third) of Torts: Prod. Liab.* (1998).

[99] La disciplina europea prevede una nozione unitaria di difettosità: *ex* art. 6 della Direttiva 85/374/EC, il prodotto «è difettoso quando non offre la sicurezza che ci si può legittimamente attendere tenuto conto di tutte le circostanze».

[100] La casistica in materia di danni provocati da robot chirurgici è molto recente. Tra i tanti, si rinvia a *Mracek v. Bryn Mawr hospital et al.*, Pennsylvania Eastern District Court, 11 marzo 2009 ove il ricorrente era un paziente e i convenuti erano la struttura ospedaliera, il Bryn Mawr Hospital e il produttore, Intuitive Surgical, di un robot chirurgico utilizzato dall'ospedale. Il ricorrente sosteneva sussistesse una responsabilità diretta da prodotto (*strict product liability*), una responsabilità diretta da malfunzionamento (*strict malfunction liability*), negligenza (*negligence*) e

La nozione di «difetto» ha un carattere normativo[101], sebbene il legislatore europeo lasci ampio margine interpretativo[102]. La difettosità del prodotto, infatti, è strettamente connessa al concetto di sicurezza[103], e si configura *ex* art. 117 comma 1, cod. cons., quando il prodotto «non offre la sicurezza che il consumatore può legittimamente attendere». Tale formulazione da cui originano tutte le ambiguità interpretative[104] può avvalersi solo di alcune circostanze che definiscono il contenuto. La valutazione, da compiersi

violazione della garanzia (*breach warranty claims*). Il paziente sosteneva che uno dei robot chirurgici avesse cominciato a non funzionare più correttamente dopo l'inizio dell'operazione e che, conseguentemente al ritardo provocato nello svolgimento dell'operazione e alla necessità per il chirurgo di continuare l'operazione con i metodi tradizionali (laparoscopia), egli avesse sofferto svariati danni permanenti. La corte distrettuale rigettò il ricorso in quanto il ricorrente non era riuscito ad allegare idonee prove del malfunzionamento del robot. Va ricordato, inoltre, che nel caso di specie, ai sensi della legge della Pennsylvania il paziente avrebbe dovuto allegare la testimonianza del produttore, poiché il chirurgo, pur essendo «l'intermediario esperto» non è stato considerato esperto nel campo specifico della chirurgia robotica. Tra gli altri casi famosi si veda anche *Silvestrini v. Intuitive Surgical Inc et al.*, n. 11-2704 (Louisiana Eastern District Court, 6 febbraio 2012); *Taylor v. Intuitive Surgical, Inc.*, n. 45052-6-II (Court of Appeals Cause No. 45052-6-II, 7 luglio 2015). Il numero dei report presentati dai chirurghi americani all'Fda per eventi avversi occorsi durante l'utilizzo del robot è cresciuto talmente tanto da indurre, nel 2013, la stessa *agency* a lanciare una procedura di sorveglianza per verificarne le cause dei malfunzionamenti. Il contezioso in materia, tuttavia, è cresciuto senza interruzione, fino alla proposizione, nel 2015, della prima *class action* nello Stato del Missouri, si rinvia a http://surgicalwatch.com/davinci-robot/lawsuit/ (ultima consultazione 15 marzo 2018).

[101] La giurisprudenza europea si è pronunciata sul concetto di difetto e della sua prova con Corte giustizia UE, 5 marzo 2015, cause riunite C-503/13 e C-504/13, in *Danno e resp.*, 5, 2016, con nota di Bittetto; in *Resp. civ. e prev.*, 2015, p. 751, con nota di Nobile de Santis.

[102] Vedi *amplius* A. Fusaro, *Responsabilità del produttore: la difficile prova del difetto*, in *La nuova giur. civ.*, 6, 2017, p. 896.

[103] *Ex* art. 103 cod. cons. si deduce che la sicurezza del prodotto è definita come la generale assenza di rischi, pur tollerando rischi minimi considerati accettabili dall'ordinamento giuridico comunitario.

[104] E. Rajneri, *L'ambigua nozione di prodotto difettoso al vaglio della Corte di Cassazione italiana e delle altre Corti europee*, in *Riv. dir. civ.*, 2008, p. 623.

caso per caso, andrà effettuata tenendo conto delle seguenti circostanze: «il modo in cui il prodotto è stato messo in circolazione, la sua presentazione, le sue caratteristiche palesi, le istruzioni e le avvertenze fornite; l'uso al quale il prodotto può essere ragionevolmente destinato e i comportamenti che, in relazione a esso, si possono ragionevolmente prevedere; il tempo in cui il prodotto è stato messo in circolazione».

La giurisprudenza più recente ha chiarito che tale concetto va analizzato non tanto con riferimento alle ragionevoli aspettative del consumatore[105], quanto, piuttosto, adottando un approccio olistico che tenga conto sia delle limitazioni d'uso, che delle controindicazioni prescritte dal fabbricante (cosicché si può parlare di difetto solo quando esso si esplica nelle esatte modalità d'uso); e inoltre, del corretto rapporto costi/benefici.

Le applicazioni robotiche che presentano un elevato grado di autonomia (ad esempio le *self-driving cars* di III e IV livello) aumentano, drasticamente, le difficoltà legate alla valutazione della difettosità[106].

Molte ipotesi di danno saranno provocate da mancato o inadeguato design[107], che si va delineando quale difetto-tipo in robotica: esso mette in discussione i criteri di valutazione

[105] *Wilkes v. DePuy International Limited*, n. HQ15P02664 (High Court of Justice Queen's Bench Division, 12 dicembre 2016). Di notevole interesse la decisione del 6 dicembre 2016 dell'Alta Corte del Queens (Londra), in un caso di *product liability* conseguente al malfunzionamento di una protesi all'anca. Non era in discussione che la protesi fosse progettata secondo gli standard tecnici previsti dalla normativa tecnica; tuttavia, l'attore lamentava la difettosità del prodotto per il cedimento di questa e la delusione delle aspettative riposte nel prodotto.

[106] In base all'art. 7 della Direttiva 85/374/Cee, la responsabilità è esclusa «se lo stato delle conoscenze scientifiche e tecniche, al momento in cui il produttore ha messo in circolazione il prodotto, non permetteva ancora di considerare il prodotto come difettoso». Nel nostro ordinamento, la disposizione è stata recepita nell'art. 118 lett. *e*) del Codice del Consumo. Per un'analisi sul punto si rinvia, tra i tanti, a D. Cerini, *Responsabilità del produttore e rischio di sviluppo: oltre la lettera della direttiva 85/374/Cee*, Milano, Giuffrè, I, 1996, p. 57.

[107] Si concorda con A. Bertolini, *Robot as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules*, in *Law, Innovation and Technology*, 5, 2013, pp. 214-247, spec. p. 239.

applicati sia in Europa che oltreoceano. L'ordinamento americano valuta la scelta del progettista attraverso il confronto con il design alternativo (c.d. *reasonable alternative design* o Rad)[108] idoneo a evitare il danno[109]. In pratica, in base a tale criterio si stabilisce se il prodotto è difettoso qualora risulti che il malfunzionamento sarebbe stato evitato, progettando diversamente il prodotto. Spetta al danneggiato provare tale non conformità a un progetto alternativo. Secondo Owen, il *risk-utility test* del *Third Restatement* sottende un bilanciamento di interessi delle parti che si traduce nella verifica comparativa tra «risk utility of chosen design, on the one side, against the risks and benefits of the proposed alternative design, on the other». La valutazione comparativa si basa sull'utilizzo di numerosi criteri: la probabilità che l'evento dannoso si verifichi, la gravità del danno, le informazioni e le avvertenze offerte, la natura del prodotto, le conoscenze generali del prodotto, i costi per realizzare il prodotto alternativo, la sicurezza dei due prodotti; la possibilità di accesso dei consumatori a tale prodotto alternativo. Misurando i vantaggi del prodotto alternativo, si finisce per valutare il costo delle precauzioni che il fabbricante avrebbe dovuto adottare al fine di evitare il danno[110].

Anche il concetto di prevedibilità (*foreseeability*) rimane inestricabilmente collegato al criterio del Rad: il *Terzo Restatement* indica, infatti, che l'identificazione del Rad stesso dipende dallo stato della conoscenza tecnica e, dunque, dai

[108] In base al *Restatement Third*, par. 2, comment *f)* del 1998: «product is defective in design if the reasonable risks of harm could have been reduced by a reasonable alternative design».

[109] Si noti che la materia della responsabilità da prodotto rientra nelle materie di competenza statale, ma tutte sono orientate dai lineamenti di disciplina generali tracciati dal *Terzo Restatement*.

[110] Cfr. D.G. Owen, *Risk-utility Balancing in Design Defect Cases*, University of South Carolina, 1997. L'autore osserva che, focalizzandosi sul costo delle precauzioni, si perviene a formulazioni del tipo: «a product is defective in design if the safety benefits from altering the design as proposed by plantiff were foreseeably greater than the resulting cost». Si tratta della «reasonable safety» che delinea un modello di prodotto alternativo che: *a*) può essere realizzato a costi accessibili; *b*) presenta una pericolosità minore rispetto a quella del prodotto considerato.

rischi prevedibili e dalle tecniche di *risk-avoidance* in uso al momento della distribuzione[111].

Nell'ordinamento europeo, invece, si procede con logiche diverse. La Direttiva non impiega il criterio del Rad per definire il difetto di concezione[112]. La difettosità non si può inferire al semplice fatto che nel mercato circoli un prodotto più perfezionato, riferendosi in generale a tutti i tipi di difetti potenzialmente configurabili, o evitabili, attraverso l'adozione del modello avanzato[113].

Il diritto europeo utilizza, invece, criteri generali come il *risk-utility test*, l'analisi costi-benefici[114], e il criterio delle ragionevoli aspettative.

Anche con riferimento specifico all'algoritmo, il difetto più verosimile è quello della progettazione: la maggior parte dei difetti di design dell'algoritmo dà luogo al malfunzionamento del computer. Il software di guida automatizzato, per esempio, potrebbe causare un'accelerazione maggiore

[111] Per un'analisi analitica del rischio di danno prevedibile si rinvia a A.S. Chellappa, *Strict Products Liability after Bustos v. Hyundai: UJI 13-1407 and the Requirement to Show Reasonable Alternative Designs in Automobile Crash Cases*, in *N.M. L. Rev.*, 44, 2014, p. 207. Sulla conoscibilità del rischio si veda anche S.P. Kennedy, *Who Knew – Refining the Knowability Standard for the Future of Potentially Hazardous Technologies*, in *Wash. J.L. Tech. & Arts*, 9, 2014, p. 267.

[112] Così si legge alla nota 37 del Libro Verde sulla responsabilità da prodotto del 28 luglio 1999.

[113] Sul punto cfr. F. Galgano, *Diritto civile e commerciale*, II, 2, Padova, Cedam, 1999, pp. 404-405; e G. Ponzanelli, *Commento al d.p.r. 24 maggio 1988, n. 224*, in *Corr. giur.*, 1988, pp. 796 ss.

[114] Il progettista è, infatti, il soggetto in grado di porre in essere le misure precauzionali richieste per soddisfare la c.d. *Learned Hand formula*. Sulla *Learned Hand formula*, e su vari altri criteri utilizzati per valutare la difettosità (es. *consumer expectation test*, *risk-utility test*) si rinvia, in generale, a G. Ponzanelli, *La responsabilità civile. Profili di diritto comparato*, Bologna, Il Mulino, 1992, p. 188; R. Cooter, U. Mattei, P.G. Monateri, R. Pardolesi e T. Ulen, *Il mercato delle regole. Analisi economica del diritto civile*, I, *Fondamenti*, Bologna, Il Mulino, 2006, p. 225, che fanno riferimento alla redazione di regolamenti e leggi per specificare uno standard normativo equivalente al livello efficiente di prevenzione. Cfr. P. Pardolesi, *Profili comparatistici di analisi economica del diritto privato*, Bari, Cacucci, 2015, p. 132.

rispetto a quella normale, o il veicolo potrebbe non fermarsi con il semaforo rosso.

In questi casi, l'attore avrebbe bisogno di un esperto altamente specializzato per capire come l'algoritmo alternativo avrebbe dovuto essere «scritto» (programmato), in modo maggiormente sicuro, e pertanto idoneo a prevenire l'incidente. E in ogni caso, per la complessità della procedura, i costi e le difficoltà di trovare tale esperto, questo tipo di operazione è difficilmente proponibile.

In realtà, il criterio del Rad si palesa come criterio sempre più indeterminato nel contesto delle tecnologie innovative[115].

In termini più concreti: il riferimento alla «ragionevolezza» non pare più adeguato. Sembrerebbe più idoneo valutare, su base statistica, l'opzione di scelta scaturita dall'esecuzione di algoritmi, e dalla quale potrebbe derivare un danno, nonostante il design sia conforme ad un modello alternativo. L'argomento è approfondito qui di seguito e nei paragrafi dedicati alle questioni giuridiche delle *self-driving cars*.

5.2. *Il «malfunzionamento» dell'algoritmo*

La Direttiva 85/374/CE può essere applicata in caso di malfunzionamento dell'algoritmo?

I pochi pareri in materia sono ancora discordanti. Tuttavia, se si considera il razionale della Direttiva, la risposta sembra essere (almeno per ora) affermativa[116].

[115] Cfr. S. Chopra e L.F. White, *A Legal Theory for Autonomous Artificial Agents*, Michigan, Michigan University Press, 2011, p. 139; e A. Davola, *A Model for Tort Liability in a World of Driverless Cars: Establishing a Framework for the Upcoming Technology*, 1° febbraio 2018, consultabile all'indirzzo https://ssrn.com/abstract=3120679 or http://dx.doi.org/10.2139/ssrn.3120679.

[116] Così anche J.S. Borghetti, *Is Defectiveness an Appropriate Notion to Deal with Damage Associated with the IoT or Artificial Intelligence?*, relazione presentata al *Münster Colloquia on EU Law and Digital Economy. Liability for Robotics and in the Internet of Things*, presso Westfalische Wilhelms, Universitat Münster, Germany, 12-13 aprile 2018 e in corso di stampa per gli atti del convegno. Si rinvia anche a J.S. Borghetti, *La responsabilité du fait des produits. Etude de droit comparé*, in *LGDJ*,

Da decadi gli algoritmi sono stati una componente integrante di ogni programma informatico. Oggi, le «decisioni» algoritmiche dominano molti aspetti della nostra vita: al di là dell'esecuzione di complesse operazioni computazionali, esse, molto spesso, sostituiscono la discrezionalità della scelta umana. Sul punto fa già scuola il caso *State of Wisconsin v. Eric L. Loomis* del 2016, nel quale la Supreme Court of Wisconsin si pronunciò, per la prima volta, sulla costituzionalità dell'uso degli algoritmi nel processo di decisione giudiziale, ai fini di valutare (su basi logiche e statistiche) il rischio insito nella condotta umana. La Corte non ravvisò alcuna violazione della *due process clause* per il mancato accesso del convenuto a una spiegazione adeguata circa le operazioni di calcolo che portavano a tale decisione[117].

Molti prodotti e servizi, inclusi i filtri anti-spam, i dispositivi medici, i prodotti di marketing, le macchine *self-driving* dipendono dal funzionamento degli algoritmi, dalla velocità e dalla capacità di previsione. Sarà sempre più ricorrente, pertanto, la questione dell'affidabilità delle opzioni di scelta generate dall'algoritmo.

Una questione interessante appare l'individuazione dell'oggetto su cui focalizzare l'attenzione: se sia opportuno considerare, quale oggetto di imputazione del malfunzionamento, il robot nella sua fisicità, ovvero gli algoritmi che

495, 2004, e *L'accident généré par une intelligence artificielle autonome. Le droit civil à lère du numérique*, Actes du colloque du Master 2 Droit privé gènèral et du Laboratoire de droit civil, Paris II, 21 aprile 2017, consultabile all'indirizzo http://web.lexisnexis.fr/fb/droit_civil_a_l_ere_numerique_112017/index.html#23.

[117] *State of Wisconsin v. Eric L. Loomis*, n. 16-6387 (Supreme Court of Wisconsin, 13 luglio 2016). La Corte decise che l'accuratezza degli strumenti e la capacità dei giudici di capire i possibili malfunzionamenti erano sufficienti ad assicurare i diritti fondamentali del convenuto. Tuttavia, criticando la decisione, vi è chi sottolinea la necessità di usare software *open source* nel sistema di giustizia. Cfr. I. De Miguel Beriain, *Does the Use of Risk Assessments in Sentences Respect the Right to Due Process? A Critical Analysis of the Wisconsin v. Loomis ruling*, in *Law, Probability and Risk*, 17, 1, 2018, pp. 45-53.

generano la decisione da cui discende l'azione materiale del robot[118].

Tradizionalmente, gli algoritmi sono stati considerati alla stregua di meri strumenti nelle mani degli uomini. La disciplina della responsabilità applicabile è stata pertanto significativamente differente da quella applicabile alle azioni umane. Se, solo per ipotesi, si configurasse una responsabilità per colpa del robot, bisognerebbe indagare più a fondo, come suggeriscono alcune ricerche giuridiche americane, l'applicabilità del criterio di ragionevolezza all'algoritmo: si parla di *reasonable algorithm*, il quale richiama lo standard del ragionevole uomo o professionista ragionevole. La ragionevolezza specifica dell'algoritmo può essere molto diversa da quella della persona ragionevole o del professionista, sulla base del quale misurarlo. Stabilire il contenuto del c.d. *reasonable algorithm standard*, e ciò che lo differenzia da quello applicato all'azione umana, è oggetto di interessanti dibattiti.

Intuitivamente, le elevate potenzialità degli algoritmi condurrebbero a identificare, quale parametro di riferimento per la valutazione del funzionamento, quello della ragionevolezza «qualificata». Ma, in ogni caso, assoggettare l'algoritmo a un'analisi del comportamento o delle scelte sembra improprio, poiché si «personificherebbe» la macchina. Un robot negligente è, in ultima analisi, un robot difettoso[119].

Gli algoritmi non sono persone, sebbene nella c.d. società dell'algoritmo i dispositivi *software-driven* stiano rimpiazzando alcuni «compiti» tipici dei professionisti. È stato, allora, osservato che l'oggetto da regolamentare non è l'algoritmo ma la condotta umana della persona che lo programma, o lo connette al database, la quale decide per quali scopi utilizzarlo[120]. Il produttore di un dispositivo

[118] K. Chagal-Feferkorn, *The Reasonable Algorithm*, in *Journal of Law, Technology and Policy*, 1, 2018, pp. 113 ss. L'autore pone tale preliminare complessa questione.

[119] Così Borghetti, *Is Defectiveness an Appropriate Notion to Deal with Damage Associate with the IoT or Artificial Intelligence?*, cit.

[120] J.M. Balkin e S. Austin, *Distinguished Lecture on Big Data Law and Policy: The Three Laws of Robotics in the Age of Big Data*, in *Ohio*

medico diagnostico dovrebbe essere valutato secondo lo stesso standard di riferimento adottato per disciplinare la condotta del medico che il dispositivo «sostituisce» per quella specifica operazione. Ciò implicherebbe il monitoraggio di quello che produttori e programmatori stanno codificando. Non è un'operazione semplice, poiché, come osserva Frank Pasquale – in *The Black Box Society* – molte architetture dei sistemi digitali sono velate da segretezza assoluta: è impossibile capire che cosa succeda nella scatola nera dell'algoritmo[121]. Per garantire il monitoraggio, i legislatori dovrebbero allora stabilire delle regole e delle linee-guida per la programmazione e le loro interazioni[122].

Altra proposta deriva da chi studia la casistica dei c.d. *computer-generated torts*: quando i computer, i robot o la macchina diventano più sicuri dei professionisti o dell'uomo, il produttore non dovrebbe più essere valutato secondo lo standard della responsabilità oggettiva, quanto piuttosto secondo lo standard di negligenza[123].

Questo ragionamento è sinergico all'iniziativa riguardante la progettazione di «comportamenti responsabili» nella macchina, la quale non interagisce con l'intento e la volontà umana: si tratta della *responsibility-by-design*, complementare al *security-by-design*, e alla *privacy-by-design*[124].

St. L.J., 78, 2017, p. 1217. Secondo l'autore gli algoritmi «(a) construct identity and reputation through (b) classification and risk assessment, creating the opportunity for (c) discrimination, normalization, and manipulation, without (d) adequate transparency, accountability, monitoring, or due process».

[121] F. Pasquale, *The Black Box Society*, Cambridge, Harvard University Press, 2015.

[122] Id., *Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society*, in *Ohio St. L.J.*, 78, 2017, p. 1243.

[123] R. Abbott, *The Reasonable Computer: Disrupting the Paradigm of Tort Liability*, in *George Washington Law Review*, 86, 1, 2018, consultabile all'indirizzo https://ssrn.com/abstract=2877380 or http://dx.doi.org/10.2139/ssrn.2877380.

[124] Balkin e Austin, *Distinguished Lecture on Big Data Law and Policy*, cit.

In sintesi, emerge una prima considerazione: a prescindere dal regime di responsabilità applicabile, la base per la valutazione dell'algoritmo sarà, in ogni caso, la difettosità. Il problema consiste nell'individuare il criterio per valutare il difetto da progettazione dell'algoritmo che sembra avvalorare il passaggio dal parametro della ragionevolezza a quello statistico.

5.3. *Questioni di responsabilità e ripensamenti intorno alla capacità giuridica del robot*

I problemi emersi fin qui comportano un ripensamento intorno alla capacità giuridica attribuita e attribuibile ai robot. Come anticipato nel capitolo I, par. 2.2, pur adottando, in questa sede, un'ampia definizione di robot, tale da assimilarlo a una macchina e, quindi, a un prodotto, è necessario dar conto delle molteplici ipotesi avanzate, sul piano operativo, da dottrina e istituzioni pubbliche[125].

Robot come prodotti. Abbiamo già detto di questa ipotesi, trattandosi di una premessa del lavoro.

Robot come animali[126]. La capacità di locomozione e la capacità di reagire alle condizioni ambientali, indipendentemente dal controllo dell'uomo[127], hanno indotto alcuni

[125] Per una ricostruzione delle proposte avanzate si rinvia a A. Bertolini, *Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules*, in *Law, Innovation and Technology*, 5, 2013, pp. 214-247; e C. Boscarato, *Who Is Responsible for a Robot's Actions? An Initial Examination of Italian Law within a European Perspective*, in B. van de Berg e L. Klaming (a cura di), *Technologies on the Stand: Legal and Ethical Questions in Neurosciences and Robotics*, Nijmegen, Wolf Legal Publishers, 2011, p. 393, consultabile all'indirizzo https://pure.uvt.nl/portal/files/1328301/Berg_Technologies_on_the_stand_110509_publishers_embargo_1_y.pdf. L'autore si chiede se sia ragionevole considerare il robot come un artefatto, piuttosto che come entità capace di agire.

[126] Il numero di robot dalle sembianze animali è aumentato: negli anni più recenti sono stati sperimentati in molti campi, da quello militare a quello domestico-ludico.

[127] E. Schaerer, R. Kelley e M. Nicolescu, *Robots as Animals: A Framework for Liability and Responsibility in Human-Robot Interactions*, paper presentato al *18th Iee International Symposium on Robot and*

studiosi ad assimilare i robot agli animali, per configurare un'ipotesi di applicabilità della disciplina *ex* art. 2052 c.c. In questo modo, il proprietario e l'utilizzatore sono soggetti responsabili per i danni causati dal robot, in virtù dell'obbligo di custodia[128]. La similitudine robot-animale diventa più enigmatica quando a essere paragonato all'animale vero è un robot elettrodomestico (es. Roomba), il quale uscito dalle mura domestiche sfugge al controllo del custode/proprietario[129]. Secondo questa ricostruzione, la locomozione è caratteristica, di per se stessa sufficiente a dar luogo a situazioni imprevedibili[130]. Alcuni mettono in dubbio la similitudine in esame dal momento che ciò che suscita la reazione in un animale vero è l'istinto e la sua indole caratteriale, e non il «discostamento» dell'azione rispetto al programma preimpostato[131]. Laddove invece, al

Human Interactive Communication, Toyoma, Japan, 27 settmbre-2 ottobre 2009, consultabile all'indirizzo http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2271466, p. 72.

[128] Sul tema si rinvia anche a U. Ruffolo, *Per i fondamenti di un diritto della robotica self-learning; dalla machinery produttiva all'auto driverless: verso una «responsabilità da algoritmo»?*, in U. Ruffolo (a cura di), *Intelligenza artificiale e responsabilità*, Milano, Giuffrè, 2017, p. 24.

[129] Roomba 174 rappresenta la prima generazione di puliscipavimenti domestici. Consiste, sostanzialmente, in un disco che si muove intorno alla casa e, girando continuamente su se stesso aspira la polvere. La seconda generazione di questo tipo di robot, chiamata Scooba, può anche lavare i pavimenti. Per conoscere questo tipo di tecnologia si rinvia a: http://www.irobot.com/.

[130] La similitudine tra animale e Roomba è proposta da Boscarato, *Who Is Responsible for a Robot's Actions*, cit.

[131] Bertolini, *Robots as Products*, cit., p. 289. Si legge: «One area of particular interest within this field is the study of those capacities by virtue of which men and women qualify as moral agents, beings who are responsible for their actions. This study is especially important to the theory of duty since that theory, in modern philosophy, characteristically assumes a strong doctrine of individual responsibility. That is, it assumes principles of culpability for wrongdoing that require, as conditions of justified blame, that the act of wrongdoing be one's own and that it not be done innocently. Only moral agents are capable of meeting these conditions. And the presumption is that normal, adult human beings qualify as moral agents whereas small children and nonhuman animals do not. The study then focuses on those capacities that distinguish the

contrario, si consideri che i robot agiscono sulla base di una razionalità primitiva, che esclude la possibilità di controllo (così come l'impulso istintivo dell'animale) ma non la responsabilità del proprietario, ciò potrebbe avvalorare la similitudine con i robot.

Robot come agenti e «oggetti animati». La riflessione filosofica compara i robot dotati di un'autonomia forte agli agenti morali, in grado di agire secondo principi etici, come se fossero agenti responsabili delle loro azioni[132]. In questo modo essi potrebbero essere considerati centro di imputazione di responsabilità.

Pare interessante dar conto di un profilo fiscale connesso all'attribuzione della capacità giuridica, delineatosi nell'ordinamento statunitense entro il contesto dei prodotti giocattolo. La dottrina americana si è chiesta se il robot rappresenti una cosa «animata» ai fini della tassazione: a partire dagli anni Cinquanta, infatti, il problema è emerso sovente nel *case law*, laddove, per ragioni storiche, la tassazione sulle bambole, prevista dal *Tariff Act* del 1930, è diversa da quella imposta su altri giocattoli, sul presupposto che le prime rappresentino una c.d. *animate life*[133]. Caso emblematico appare *Louis Marx & Co. and Gebrig Hoban & C., Inc. v. United States*[134], in cui un ufficio doganale è stato chiamato a decidere se un robot importato (nella specie un modello dotato della funzione di locomozione) dovesse essere tassato come un oggetto animato, e quindi con l'applicazione del regime tariffario al 35% del valore, in luogo del 50% del regime ordinario. Secondo quanto emerse dai verbali di causa, a cui diede luogo la vicenda, il giudice chiese all'importatore se il robot giocattolo in questione fosse un'imitazione di un oggetto animato, e l'importatore replicò: «Yes, a robot. It is as a synthetic man. It is something imitating men. That is

former from the latter as responsible beings. The main issue is whether the power of reason alone accounts for these capacities».

[132] Cfr. R. Audi (a cura di), *Cambridge Dictionary of Philosophy*, Cambridge, Cambridge University Press, 1999, p. 326.

[133] Cfr. *United States Tariff Act of 1930* (noto come *Hawley-Smoot Tariff Act*), US legislation, 17 giugno 1930.

[134] *Louis Marx & Co. v. United States*, (Custom Court, 1958).

the animate object that this particular toy represents. Also, the common meaning of robot supports our contention»[135]. Queste spiegazioni non convinsero, però, la corte.

Robot dotati di «personalità elettronica». La Risoluzione del Parlamento europeo ipotizza l'attribuzione ai robot autonomi, e anche agli agenti software[136], della «personalità elettronica», registrandoli e munendoli di un codice identificativo. Si tratterebbe di una personalità giuridica simile a quella attribuita alle società: i robot diventerebbero centro di imputazione autonomo delle responsabilità. Tuttavia, questa ipotesi sembra inappropriata, a prescindere dal modello giuridico prescelto: non può coincidere con quello attribuibile alla persona fisica, poiché il robot non può essere titolare di diritti umani, quali il diritto alla dignità, all'integrità, alla remunerazione, alla cittadinanza. Si determinerebbe, infatti, una situazione in contraddizione con quanto stabilito dalla Carta dei diritti umani dell'Unione europea e dalla Convenzione per la protezione dei diritti umani e delle libertà fondamentali. *Robots cannot be sued* affermò una famosa sentenza del terzo circuito della Corte d'Appello degli Stati Uniti[137]. Si noti, però, che la decisione fu presa nel lontano 1984, quando i robot non erano certo così «intelligenti» come quelli odierni.

La «personalità elettronica» dei robot non può, però, nemmeno ispirarsi al modello della persona giuridica, dal momento che ciò implicherebbe l'esistenza di una persona

[135] Il caso è riportato anche in R. Calo, *Robots in American Law*, in Hilgendorf e Seidel (a cura di), *Robotics, Autonomics, and the Law*, cit.

[136] Gli agenti software, detti anche agenti digitali, elettronici o informatici, sono, in sintesi, programmi informatici capaci di azione autonoma in ambienti complessi. Si tratta di software ancora di limitata diffusione, ma già all'attenzione degli studiosi d'informatica, degli sviluppatori di software e degli operatori di internet. La dottrina giuridica si è, da tempo, cimentata nell'analizzare la natura giuridica del software quale strumento in grado di giocare un ruolo attivo nel rapporto con il proprio ambiente e con possibili controparti (umane o automatiche). Cfr. G. Sartor, *Gli agenti software: nuovi soggetti del cyberdiritto*, in *Contratto e impresa*, 2, 2002, p. 465.

[137] *United States v. Athlone Indus.*, Inc., n. 83-5822 (United States Court of Appeals, 23 ottobre 1984).

fisica rappresentata dalla persona giuridica, per conto della quale quest'ultima agisce. E questo non è il caso del robot[138].

In merito alle difficoltà emerse appare interessante quanto afferma il prof. Burkhard Schafer nella sua presentazione al Ministro federale dell'economia e della tecnologia a Berlino nel 2012. Nel Regno Unito la qualifica giuridica di un robot appare meno centrale rispetto a quanto rappresenti nel nostro ordinamento. La mentalità inglese – conclude il professor Schafer – non si focalizza sulle specifiche capacità del robot e sulla sua essenza ontologica per poi attribuirgli quella normativa, quanto piuttosto nel modo in cui le persone percepiscano certi artefatti e si relazionino con essi[139].

6. *Gli schemi alternativi alle comuni regole di responsabilità*

In questa sede è possibile esporre solo alcune considerazioni generali. Il Parlamento europeo manifesta chiara preoccupazione in merito alle difficoltà di compensare i danni da prodotti robotici e allocare le responsabilità senza causare effetti di *overdeterrence* o, al contrario, *underdeterrence*: condizioni queste non ottimali per uno sviluppo dell'industria robotica che sia in armonia con l'agenda di Rri.

Nella Comunicazione dedicata alla costruzione di un'economia dei dati[140], la Commissione europea ha vagliato

[138] La capacità giuridica del robot non può essere ispirata al modello anglosassone del *Trust* o a quello tedesco di *Fiducie* or *Treuhand*. Si tratta, infatti, di costruzioni giuridiche molto complesse che richiedono competenze specialistiche. Entrambe, peraltro, non risolverebbero il problema dell'imputazione della responsabilità, poiché presuppongono l'esistenza di un essere umano – il *trustee* o fiduciario – responsabile della gestione del robot.

[139] L'opinione è espressa nel Report *Suggestion for a Green Paper on Legal Issues in Robotics. Contribution to Deliverable D3.2.1 on Elsi Issues in Robotics* (euRobotics The European Robotics Coordination Action Grant Agreement Number: 248552), consultabile all'indirizzo https://www.unipv-lawtech.eu/files/euRobotics-legal-issues-in-robotics-DRAFT_6j6ryjyp.pdf.

[140] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Costruire un'economia dei dati europea*, cit.

diversi approcci, al fine di creare le condizioni più favorevoli all'innovazione. In particolare, vengono elencati:

a) l'*approccio della creazione e della gestione del rischio* con il quale si indica che la responsabilità potrebbe essere assegnata all'operatore del mercato che crea un rischio sostanziale ad altri, oppure all'operatore del mercato che si trova nella posizione migliore per ridurre al minimo o evitare il verificarsi di tale rischio. Il modello di analisi del rischio utilizzato dal Regolamento UE 2016/679 in materia di *Data Protection* è un esempio;

b) *regimi di assicurazione volontari e obbligatori* per risarcire le parti che hanno subito il danno. Questo approccio dovrebbe fornire una tutela giuridica agli investimenti delle imprese, rassicurando, al contempo, le vittime sull'equità del risarcimento o sull'esistenza di un'assicurazione in caso di danni.

Queste iniziative riecheggiano anche nella Risoluzione. Innanzitutto, la (criticata) proposta di attribuire personalità elettronica ai robot per poter imputare loro l'obbligo risarcitorio per gli eventuali danni diverrebbe funzionale alla creazione di un fondo generale per tutti i robot autonomi intelligenti, o di un fondo individuale per ogni categoria di robot. Così, alle «persone elettroniche» si assocerebbe un numero d'immatricolazione individuale, iscritto in un registro specifico dell'Unione «onde consentire a chiunque interagisce con il robot di essere informato sulla natura del fondo, sui limiti della responsabilità in caso di danni alle cose, sui nomi e sulle funzioni dei contributori e su tutte le altre informazioni pertinenti» (Risoluzione, art. 59).

Anche lo strumento assicurativo diventa di centrale importanza, poiché la Risoluzione propone una soluzione analoga a quella applicata ai veicoli a motore, prospettando il *favor* per l'integrazione di tale regime assicurativo con un fondo.

In caso di assenza di copertura assicurativa[141], le soluzioni

[141] Sul contratto assicurativo, tra i tanti, si rinvia al recente contributo di D. Cerini, *Regolare la complessità. L'assicurazione tra sentimenti, valori, regole tecniche*, in M. Graziadei e M. Serio (a cura di), *Regolare*

che si profilano sono varie e dovranno essere opportunamente considerate dalle imprese assicurative, onde evitare situazioni di *impasse* che ritarderebbero adeguate risposte di indennizzo ai consumatori/utenti. La Risoluzione propone di introdurre un regime assicurativo obbligatorio necessario per categorie specifiche di robot. Come avviene già, per esempio, nel settore automobilistico[142].

Altra proposta, al momento attuale solo di natura dottrinale, consiste nel dotare produttori e progettisti di un c.d. *safe harbor*, ossia di un'immunità operante qualora le circostanze confermino che il robot, causa di danni, abbia agito sotto il controllo del consumatore, o dell'operatore che controllava il software[143]. Vi sono, poi, altre proposte per ambiti specifici, come per il settore automobilistico (vedi *infra* par. 7).

7. *Un esempio: il contesto delle «driverless cars»*

La diffusione dei mezzi elettronici per il supporto alla guida è, secondo le stime delle società internazionali di

la complessità. Giornate in onore di Antonio Gambaro, Atti del V Convegno nazionale Sird, Trapani, 24-25 giugno 2016, Torino, Giappichelli, 2016, pp. 100-111.

[142] Secondo l'art. 58 della Risoluzione «la possibilità per il produttore, il programmatore, il proprietario o l'utente di beneficiare di una responsabilità limitata qualora costituiscano un fondo di risarcimento nonché qualora sottoscrivano congiuntamente un'assicurazione che garantisca un risarcimento in caso di danni arrecati da un robot».

[143] La dottrina americana ha proposto di adottare una c.d. «immunità selettiva» per i produttori di piattaforme robotiche aperte («open robots»): «What would immunity for personal robotics manufacturers look like? One option is blanket immunity for all robot manufacturers. […] The problem with blanket immunity in the context of robotics is that it would remove not only the legal disincentive to the production of open robots but also an incentive to make them safe. […] I am thus arguing for a compromise position: A presumption against suit unless the plaintiff can show the problem was clearly related to the platform's design». R. Calo, *Open Robotics*, in *Maryland Law Review*, 70, 2011, pp. 571-613.

consulenza direzionale[144], il principale fattore di diminuzione degli incidenti stradali: essi sono, infatti, un indiscutibile strumento per l'aumento della sicurezza stradale. Tali sistemi, in pratica, consistono nel rilevamento delle condizioni spazio-temporali, entro le quali il veicolo si muove, nonché nel monitoraggio dei parametri del veicolo stesso per poi assistere il conducente nel controllo, fino a «sostituirlo» completamente[145]. Questi ultimi sono, attualmente, solo in fase di sperimentazione.

I vantaggi sono indiscutibili. L'utilità sociale di tali veicoli, una logica conseguenza[146]. Ad aumentare la domanda di sistemi completamente automatizzati alla guida concorre la diffusione del *car sharing*, fenomeno che, nei principali aggregati urbani, realizza la *sharing economy*[147].

La diffusione dei veicoli autonomi è accompagnata dal dibattito sul c.d. *control dilemma*: mentre i progressi

[144] McKinsey Global Institute, *Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy*, 2013, consultabile all'indirizzo www.mckinsey.com. Secondo le stime si potrebbero evitare ogni anno dalle 30.000 alle 150.000 vittime della strada.

[145] Vedi M.C. Gaeta, *Automazione e responsabilità civile automobilistica*, in *Resp. civ. prev.*, 2016, pp. 1718-1750.

[146] Per un'analisi sulla misurazione del benessere sociale costruita a partire dalle utilità degli individui, si rinvia a S. Shavell, *Analisi economica del diritto*, Torino, Giappichelli, 2007, p. 103.

[147] Sul fenomeno della *sharing economy* si rinvia a E. Mostacci e A. Somma, *Il caso Uber. La sharing economy nel confronto tra common law e civil law*, Milano, Egea, 2016. Vedi anche V. Zeno Zencovich, *Uber: modello economico e implicazioni giuridiche*, in *Medial Law*, 1, 2018, pp. 140-143. Peraltro, gli indubbi benefici, in termini di diminuzione dell'inquinamento atmosferico e di gestione del traffico stradale hanno motivato le pubbliche amministrazioni ad assumere un ruolo attivo nella logica dell'economia della condivisione, partecipando direttamente alla fornitura dei servizi e alla messa a disposizione dei veicoli. Questo profilo, nell'ottica della diffusione delle macchine a guida automatizzata, ha rilevanti conseguenze: in prima battuta, verrebbe meno il nesso tra proprietario del veicolo e responsabilità per danni causati dal veicolo stesso richiesto *ex* art. 2054 c.c., con il trasferimento dei costi degli incidenti sulle pubbliche amministrazioni, anche in caso di guida automatizzata. Così notano anche A. Davola e R. Pardolesi, *In viaggio col robot: verso nuovi orizzonti della r.c. auto («driverless»)?*, in *Danno e resp.*, 5, 2017, pp. 616-629, spec. p. 620.

della tecnologia nel campo automobilistico permettono ai conducenti di affidarsi, sempre di più, alle informazioni rilevate dal monitor e dai sistemi di controllo automatici, dal punto di vista giuridico il conducente è (ancora) obbligato a mantenere il controllo del veicolo. Questo paradosso non solo riduce l'attrattività delle nuove macchine a guida autonoma, ma costringe i conducenti a un eccesso di attenzione, nonostante i test psico-fisici abbiano già dimostrato l'impossibilità di mantenere vigile l'attenzione in assenza di una sufficiente stimolazione[148].

Il profilo della responsabilità del conducente, però, esula dal presente ambito di studio. L'analisi è nella prospettiva della sicurezza del veicolo e responsabilità del produttore: quando un software di guida autonoma non esegue adeguatamente il complesso compito di guidare la macchina attraverso il traffico, è verosimile che si configuri un'ipotesi di responsabilità del produttore dell'auto e/o del sistema di controllo. La figura del produttore si candida, infatti, come la più idonea a rispondere di tali disfunzioni dei veicoli:

> la casa automobilistica funge da garante dell'affidabilità dei propri prodotti, sia quando è impegnata direttamente nel loro sviluppo, sia qualora, in qualità di assemblatore, selezioni i partner più adeguati per curarne specifici aspetti di marcata criticità (quale, appunto, la sicurezza del software per la guida automatica); è, inoltre, l'unico soggetto in grado di svolgere un'attività di monitoraggio sistematico del funzionamento dei propri prodotti, come pure quello meglio posizionato per intervenire, ove essi rivelino imperfezioni o malfunzionamenti, al fine di migliorarne la qualità e l'affidabilità[149].

[148] E. Hilgendorf, *Automatisiertes Fahren und Recht*, in *Veroffentlichung der auf dem*, 53, Koln, 2015, p. 67. J.L. Mashaw e D.L. Harfst, *From Comman and Control to Collaboration and Deference: The Transformation of Auto Safety Regulation*, in *Yale Journal on Regulation*, 34, 1, 2017, pp. 167-278.

[149] Davola e Pardolesi, *In viaggio col robot*, cit., p. 627. Gli autori propongono l'introduzione di un regime di responsabilità oggettiva limitata al fine di individuare il fabbricante come soggetto responsabile dei danni causati da veicoli automatizzati, evitare che la configurazione di una responsabilità da rischio da sviluppo penalizzi gli investimenti

Le soluzioni giuridiche sono ancora incerte, con conseguenti ricadute sulle scelte produttive: i produttori stanno, infatti, offrendo un numero ancora limitato di sistemi *self-driving*, nonostante i loro indubbi vantaggi.

La trattazione che segue esemplifica, dal punto di vista funzionale, il carattere multiforme della questione sicurezza (per la variegata tipologia di rischi)[150], e dal punto di vista giuridico, il funzionamento del software di guida automatica mette in luce le difficoltà di predisporre adeguati standard.

7.1. *Le peculiarità tecnologiche nelle recenti iniziative legislative sulla sicurezza dei veicoli*

È preliminarmente utile fornire i necessari chiarimenti terminologici. Mentre nel linguaggio dei media, i termini *robot-car* e *driverless car* risultano essere i più diffusi, nella letteratura ingegneristica si preferiscono le espressioni *assisted driving*, *autonomous driving*, *partially autonomous driving*[151], o secondo il linguaggio principalmente usato dagli *scholars* americani, *Highly Automated Vehicles* (Hav).

Le distinzioni sono state recepite nei primi documenti di *self regulations* in materia. Il *German Federal Highway Research Institute* (Bast) utilizza l'espressione guida automatizzata, suggerendo di differenziare i vari livelli di autonomia

in termini di R&D ed evitare che l'aumento dei costi da sviluppo si traduca in una traslazione dei costi in capo al consumatore, ostacolando la diffusione del prodotto e riducendo il beneficio sociale.

[150] Utilissime esemplificazioni mi sono state proposte dai professori Luca Bascetta (professore associato di Robotica e Automatica industriale) e Matteo Matteucci (professore associato di Sistemi di elaborazione delle informazioni), intervistati dall'autore, Politecnico di Milano, Milano, Italia, 7 giugno 2018. Tra le misure di sicurezza da garantire, ad esempio, è possibile adottare quelle tipiche dei cosiddetti sistemi «safety critical» per quel che riguarda la parte di sistemi embedded (hardware e software integrato).

[151] G. Meyer e S. Beiker, *Road Vehicle Automation*, Basel, Springer International Publishing, 2014.

come segue[152]: solo conducente; assistita; semi-assistita; e completamente autonoma[153].

Una più dettagliata classificazione dei livelli di autonomia è proposta dalla *Society of Automotive Engineers* (Sae)[154], la quale ha introdotto una scala per livelli – o gradi – di autonomia del veicolo che va da zero a cinque e permette di capire se un veicolo è autonomo, ovvero se abbia dei meri ausili alla guida tradizionale. Si tratta, in sintesi, dei seguenti sei livelli:

Livello 0 – *No Automation*. Questo tipo di vettura necessita dell'attenzione costante del guidatore poiché esegue materialmente tutte le manovre di guida. Il sistema avverte soltanto il conducente di eventuali malfunzionamenti o situazioni di pericolo.

Livello 1 – *Driver Assistance*. L'automobile prende alcune iniziative: imprime accelerazioni laterali (sterzando) o longitudinali (frenando/accelerando); il guidatore deve comunque prestare costantemente attenzione.

Livello 2 – *Partial Automation*. L'automobile è in grado di azionare, in alcune circostanze, sia lo sterzo sia l'acceleratore e il freno. Il guidatore deve, comunque, essere pronto a intervenire.

Livello 3 – *Conditional Automation*. L'automobile è in grado di azionare sia lo sterzo sia l'acceleratore e il freno. L'automobile monitora l'ambiente circostante ma il conducente deve comunque essere pronto a intervenire.

Livello 4 – *High Automation*. Il guidatore può delegare totalmente al veicolo la guida in situazioni definite. La presenza del guidatore è sempre richiesta ma è più di controllo in caso di emergenza.

[152] *54th German Traffic Court Conference*, Goslar, 25-27 febbraio 2016.

[153] Sulle obiezioni mosse alle definizioni offerte dal documento tedesco si rinvia a E. Hilgendorf, *Automated Driving and the Law*, in Hilgendorf e Seidel (a cura di), *Robotics, Autonomics, and the Law*, cit., p. 172.

[154] Sae International, *Taxonomy and Definitions for Terms Related to On-road Motor Vehicle Automated Driving Systems*, 30 settembre 2016. Consultabile all'indirizzo http://standards.sae.org/j3016_201609/; e su https://autoalliance.org/wp-content/uploads/2017/07/Automated-Vehicles-Levels-of-Automation.pdf.

Livello 5 – *Full Automation*. L'automobile riesce a controllare longitudinalmente e lateralmente gli spostamenti del veicolo. Non è richiesta la presenza del guidatore.

Sul mercato sono già presenti veicoli di livello 4, mentre sono in fase di sperimentazione i veicoli di livello 5. Un esperimento in tal senso è stato realizzato nel 2010 in Italia dove, grazie al progetto Vislab dell'Università di Parma, due furgoni senza conducente hanno percorso il suolo pubblico, lungo un tragitto di 8.000 miglia, da Roma a Shanghai. Più di recente, in California, il Google project ha sperimentato la *Google self-driving car*[155].

Per legittimare la circolazione stradale di queste autovetture sono state necessarie alcune revisioni alla normativa, a partire dall'art. 8 della Convenzione di Vienna del 1968 sul traffico stradale che escludeva la circolazione di veicoli senza conducente[156]. La formulazione della stessa disposizione, peraltro, era tale da non poter essere oggetto di interpretazione evolutiva[157]. La modifica della disposizione è avvenuta nel 2016, a opera del *Working Party on Road Traffic Safety* che ha autorizzato i sistemi di guida automatica, alla condizione essenziale che essi possano essere disattivati

[155] Nel febbraio del 2016, sulle strade di Mountain View (California) una macchina *self-driving* di Google tentò di sorpassare un autobus urbano. L'autobus non si mosse come previsto dalla macchina, la quale andò a collidere contro lo stesso autobus. Data la velocità contenuta dei veicoli non ci furono feriti, ma Google constatò che la causa dell'incidente dipese dall'errore del software e si impegnò a porvi rimedio.

[156] Convenzione sulla circolazione stradale, conclusa a Vienna, 8 novembre 1968, approvata dall'Assemblea federale il 15 dicembre 1978, strumento di ratificazione, depositato dalla Svizzera l'11 dicembre 1991, entrata in vigore per la Svizzera l'11 dicembre 1992.

[157] Secondo la Risoluzione le attuali norme generali di diritto internazionale privato sugli incidenti stradali applicabili all'interno dell'Unione «non hanno bisogno urgente di essere modificate in modo sostanziale per adattarsi allo sviluppo di veicoli autonomi, tuttavia la semplificazione dell'attuale duplice sistema per definire la legge applicabile (basato sul Regolamento (CE) 864/2007 del Parlamento europeo e del Consiglio e sulla convenzione dell'Aia del 4 maggio 1971 sulla legge applicabile in materia di incidenti della circolazione stradale) migliorerebbe la certezza del diritto e limiterebbe le possibilità di scelta opportunistica del foro».

dal conducente, sempre presente, per intervenire in caso di necessità, assumendo il controllo del veicolo[158].

Questo adattamento giuridico in risposta alle peculiarità tecnologiche è stato recepito in tutte le leggi in materia, per esempio: la legge tedesca sul traffico stradale (*Straßenverkehrgesetz*, StVG), approvata dal Bundestag, il 12 maggio 2017, ha introdotto nel codice della strada una disciplina per le auto a guida autonoma, confermando l'obbligo del sistema c.d. di *hand-over*, in base al quale il veicolo dev'essere dotato di un sistema per l'attivazione e la disattivazione manuale del sistema di guida automatizzata da parte del conducente[159]. Anche il *Vehicle Technology and Aviation Bill* inglese, introdotto il 22 febbraio 2017[160], al fine di assicurare un più efficiente sistema di indennizzo, prevede che nel caso di incidente provocato dal veicolo, in modalità guida automatizzata, rimanga responsabile il proprietario, laddove il veicolo non sia coperto da assicurazione[161]. Il funzionamento di tale sistema è uno degli aspetti che presenta più criticità in ottica *ex post* (vedi *infra*).

Oltre alle leggi tedesche e inglesi in materia, nell'arco del 2017, anche altri ordinamenti, come Danimarca, Finlandia, Polonia, e poi Francia e Spagna hanno introdotto provvedimenti aventi come principale obiettivo quello di testare le auto senza conducente su strade pubbliche e verificare la coesistenza con le regole del traffico tradizionale[162]. L'ordinamento italiano, con il recentissimo

[158] Working Party on Road Traffic Safety, *Report of the Sixty-eigth Session*, Ginevra, 24-26 marzo 2014, in sede Unece.

[159] Per i dettagli si veda il comunicato stampa all'indirizzo https://www.bundesregierung.de/Content/DE/Artikel/2017/01/2017-01-25-automatisiertes-fahren.html. Il progetto di legge è stato tradotto da M.G. Losano, *Il progetto di legge sull'auto a guida automatizzata*, in *Dir. Informazione e informatica*, 2017, p. 1.

[160] Il testo è consultabile all'indirizzo https://services.parliament.uk/bills/2016-17/vehicletechnologyandaviation.html.

[161] Anche questa soluzione è stata criticata dalla dottrina, cfr. Davola e Pardolesi, *In viaggio col robot*, cit., p. 621.

[162] Per una panoramica sulle leggi dei vari Stati europei, e per un approfondimento dei temi qui trattati, si rinvia a Davola e Pardolesi, *In viaggio col robot*, cit., pp. 616 ss.

decreto 28 febbraio 2018 concernente «Modalità attuative e strumenti operativi della sperimentazione su strada delle soluzioni Smart Roads e di guida connessa e automatica» (c.d. decreto Smart Roads)[163], prevede la sperimentazione di soluzioni tecnologiche per adeguare la rete infrastrutturale ai nuovi servizi smart. Alcune città italiane hanno già avviato tale sperimentazione[164]. Lo stesso decreto prospetta l'importanza delle soluzioni assicurative per promuovere l'adeguamento tecnologico e digitale della rete stradale e per introdurre una specifica copertura assicurativa al fine di garantire i rischi conseguenti a tale speciale segmento di circolazione stradale[165].

La stessa condizione di *hand-over* e la necessità di ripensare, o adattare, il regime di responsabilità per rispondere ai nuovi tipi di rischi, pur in presenza di una diminuzione di quelli tradizionali e l'utilizzo del suolo pubblico sono tutti aspetti al centro del ricco e vario panorama regolatorio americano. Nel rapporto *Driven to Safety: Robot cars and the Future of Liability* dell'*American Association for Justice* del 2017[166], del Dipartimento dei Trasporti Usa (Dot-Department of Transportation's – National Highway Traffic Safety Administration, Nhtsa) il Governo federale ha

[163] Decreto 28 febbraio 2018, «Modalità attuative e strumenti operativi della sperimentazione su strada delle soluzioni di Smart Roads e di guida connessa e automatica», in *GU* 18 aprile 2018.

[164] Il 30 marzo 2018 è stato siglato un Protocollo d'intesa tra la Città di Torino e 14 partner industriali e di ricerca per testare le auto autonome di livello 3.

[165] In materia si rinvia a D. Cerini, *Dal decreto Smart Roads in avanti: ridisegnare responsabilità e soluzioni assicurative*, in *Danno e resp.*, 4, 2018, pp. 401-409.

[166] Il testo è consultabile all'indirizzo https://www.justice.org/sites/default/files/Driven%20to%20Safety%202017%20Online.pdf. La normativa contiene previsioni relative alla «scatola nera» e alla registrazione dei relativi dati (con termine di memorizzazione di sei mesi, a meno che il veicolo non sia coinvolto in un sinistro). L'obbligatorietà della scatola nera mira proprio a rendere possibile la ricostruzione delle rispettive responsabilità in caso di incidente. Il testo della nuova normativa e gli emendamenti discussi sono reperibili sul sito del *Bundestag* tedesco: https://www.bundestag.de/dokumente/textarchiv/2017/kw13-de-automatisiertes-fahren/499928.

tentato di garantire uniformità anche attraverso strumenti di *soft law* più flessibili a rispondere al rapido sviluppo tecnologico[167]. Tali indicazioni sono state recepite da più di 21 Stati federali americani attraverso una legislazione specifica, mentre altri hanno emanato degli ordini esecutivi (*executive orders*) in materia[168].

Il processo di adattamento che si innesca interessa anche i caratteri tipici del sistema di assicurazione r.c. auto: per tutelarsi dal rischio di risarcimenti per malfunzionamento dei propri autoveicoli, la prospettiva più verosimile è quella di una trasformazione dei servizi assicurativi verso forme di polizze più simili a quelle per responsabilità da prodotto[169].

7.2. *Gli standard tecnici nel settore automobilistico…*

Come anticipato nel capitolo I, par. 3.1, nel settore automobilistico il rispetto degli standard di sicurezza legali è requisito essenziale per ottenere l'omologazione del veicolo, poiché è presunzione di non difettosità. Tuttavia, risultano di cruciale importanza gli standard volontari (es. quelli dell'EuroNcap), e una loro lettura sistematica con le regole di responsabilità, sulla scia del modello americano[170]. Ciò

[167] Tale profilo è stato duramente contestato, come emerge dalle *notice-and-comments* al documento. American Association for Justice, *Driven to Safety: Robot cars and the Future of Liability*, 2017, p. 8 del documento. Nhtsa è responsabile per lo sviluppo, l'implementazione e l'enforcement degli standard di sicurezza per veicoli (Fmvsss) e la regolamentazione dei motori e della strumentazione dei veicoli.

[168] I 21 Stati sono: Alabama, Arkansas, California, Colorado, Connecticut, Florida, Georgia, Illinois, Louisiana, Michigan, New York, Nevada, North Carolina, North Dakota, Pennsylvania, South Carolina, Tennessee, Texas, Utah, Virginia, Vermont e Washington DC. I 6 Stati federali che hanno invece optato per l'*exective order* sono: Arizona, Delaware, Hawaii, Massachusetts, Washington and Wisconsin. http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx#Enacted Autonomous Vehicle Legislation.

[169] Davola, *A Model for Tort Liability in a World of Driverless Cars*, cit.

[170] E. Al Mureden, *Sicurezza «ragionevole» degli autoveicoli e responsabilità del produttore nell'ordinamento italiano e negli Stati Uniti*, in *Contratto e impresa*, 28, 2012, pp. 1505-1525, osserva come nessuna

anche al fine di circoscrivere le ipotesi di responsabilità da sviluppo, quando in concreto fosse disponibile una soluzione tecnica più adeguata a costi di realizzazione accessibili per il progettista/costruttore[171]. Ciò significa comparare i software di guida di queste vetture (o dei sistemi autonomi). Essi sono programmati per risolvere problemi, raffrontando la realtà che «vedono» attraverso una telecamera, con i modelli (*pattern*) presenti nelle loro memorie, e ricercando una corrispondenza tra i due elementi con metodi statistici: in tali metodi sono insite percentuali di errori ineliminabili.

Con modesto anticipo rispetto al quadro europeo previamente delineato, gli Stati Uniti diedero avvio al processo di disciplina della sicurezza dei veicoli con l'emanazione dell'*Highway Safety Act* del 1966, poi trasposto nell'*United States Code*, Title 49, chapter 301 *Motor Vehicle Safety*. Il Title 49 è noto anche come *crashworthiness doctrine* e sancisce l'obbligo di immettere sul mercato veicoli che garantiscano un livello di sicurezza ragionevole in caso di incidente. I requisiti tecnici che concretizzano tale parametro di riferimento sono quelli previsti dal *Federal Motor Vehicle Safety Standards* (Fmvss) aggiornati dalla *National Highway Traffic Safety Agency*[172].

Per quanto concerne l'applicazione giurisprudenziale di tali standard, diversamente da quanto accade alle nostre latitudini, i giudici americani fanno ricorso agli standard in modo più rigoroso, proprio in virtù dell'operatività della *preemption clause*[173]. Tuttavia, è necessario sottolineare che

delle sentenze italiane in materia evidenzi il collegamento tra la responsabilità del produttore e la sicurezza delle automobili, e rileva che «tali norme non vengono considerate ai fini di verificare se l'esemplare che si assume difettoso presenti in concreto caratteristiche difformi rispetto a quelle previste dagli standards tecnici» (p. 1505).

[171] In fondo questa prospettiva è stata messa in evidenza anche da U. Carnevali, *Il difetto di progettazione negli autoveicoli*, in *Resp. civ. prev.*, 2011, p. 2108.

[172] Per dettagliate informazioni in materia di guida automatizzata, si rinvia a https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety.

[173] Molti casi sono riportati da J.T. O'Reilly, *Federal Preemption of State and Local Law*, Chicago, American Bar Association, 2006, cui si

gli standard federali Fmvss sono da intendersi, *ex* art. 49 Usc par. 30102(a)(9), come disposizioni che garantiscono i livelli minimi, il cui rispetto è condizione per ottenere l'omologazione. Nella prospettiva della responsabilità civile, però, tale requisito non è sufficiente a escludere la responsabilità del costruttore per difetti di progettazione o di informazione: gli standard previsti dal Fmvss rappresentano la soglia di sicurezza minima richiesta, mentre, invece, il livello di sicurezza ragionevole è configurabile attraverso il raffronto tra il *design* utilizzato e il Rad[174]. Nonostante ciò, il rispetto di ulteriori standard non è obbligatorio, ma volontario: essi garantiscono un livello di *optimal-not perfect-safety*[175].

La guida automatizzata porrà, ancora di più, l'accento sulla funzione degli standard volontari e aggiuntivi, e il ruolo assunto dagli stessi in sede di giudizio, al fine di soddisfare il livello ragionevole di sicurezza. Per contribuire alla funzione della Nhtsa di monitorare tali sistemi, l'Agency ha pubblicato nel 2016 la *Vehicle Performance Guidance for Automated Vehicles* (d'ora in poi: *Guidance*)[176] con la quale ha indicato quali standard e crash test, basati sulle più recenti conoscenze tecniche, potrebbero assurgere a tecnologie salvavita. La *Guidance* fornisce istruzioni e suggerimenti ai costruttori di sistemi automatizzati, da considerare quando progettano, testano e sviluppano tali sistemi. Sebbene si tratti di misure volontarie, l'*Agency* ha già prospettato che in futuro la Nhtsa potrebbe rendere vincolanti alcune di esse. Inoltre, per garantire la sicurezza, lo stesso documento incentiva i produttori ad adottare, in aggiunta, *best practices*,

rinvia. Tra i tanti, a titolo di esempio: *Anderson v. General Motors Corps*, n. BC116926 (L.A. Cty Super. Ct., 15 luglio 1999).

[174] Sul problema si rinvia a Pasquale, *The Black Box Society*, cit.

[175] Vedi *amplius* Al Mureden, *Sicurezza «ragionevole» degli autoveicoli e responsabilità del produttore nell'ordinamento italiano e negli Stati Uniti*, cit., p. 1505. Si veda, inoltre, G. Owen, *Product Liability Law*, St. Paul, Minn., Thomson-West, 2005, p. 1134.

[176] US Department, Nhtsa, *Federal Automated Vehicles Policy, Accelerating the Next Revolution in Roadaway Safety*, 2016, consultabile all'indirizzo https://www.transportation.gov/AV.

linee guida di progettazione e standard predisposti dall'Iso[177] e dalla Sae, standard messi a disposizione da autorità per l'aviazione, lo spazio e l'esercito, come ad esempio le *standard practices on system safety* messe a disposizione dell'US Department of Defense, nella misura in cui siano rilevanti e applicabili.

Tra gli standard più recenti spiccano quelli dedicati al design[178]. Si tratta di un design complesso, poiché le automobili sono un «ibrido» tra veicoli e computer: esse, infatti, sono gestite da un sistema informatico, costituito da telecamere, *signal processing*, e da software Gps, oltreché da una serie di altre tecnologie[179].

Conviene notare che il divario tra il livello di sicurezza imposto dagli standard per l'omologazione e quello scaturente dagli standard volontari, per il tipo di veicoli in esame, potrebbe essere notevole e richiedere, pertanto, modelli di «sicurezza ragionevole» molto diversi, con tutte le difficoltà poste dalle tecnologie emergenti all'impiego del criterio della ragionevolezza, di cui si è già detto.

7.3. *… e per le autovetture autonome: sicurezza preventiva e «machine ethics»*

Quando l'analisi della sicurezza preventiva concerne una *self-driving car*, e quindi, in ultima analisi, un software di guida autonoma, il ragionamento sull'adeguatezza degli standard deve rispondere a esigenze che vanno ben al di

[177] Cfr. Iso 26262, Road Vehicles – Functional Safety.

[178] «The process should place significant emphasis on software development, verification and validation. The software development process should be well-planned, well-controlled, and well-documented to detect and correct unexpected results from software development and changes. Through and measurable software testing should complement a structured and documented software development process» (così la *Guidance*).

[179] La sicurezza informatica interessa veicoli, aeromobili e navi, ma anche la loro infrastruttura di sostegno, gestione e controllo. Con l'emergere di crescenti preoccupazioni in materia di sicurezza informatica, questo sarà uno degli elementi essenziali della sicurezza dei trasporti.

là della necessità di arginare le classiche tipologie di rischi tecnologici, o dei metodi di analisi dei rischi utilizzati: l'azione risultante dall'esecuzione della sequenza algoritmica, in special modo quella relativa alla possibilità di evitare ostacoli, potrebbe implicare una scelta etica[180].

Si profila, così, un dibattito al crocevia tra etica, morale e diritto che, per tale natura, necessita di un dialogo interdisciplinare. Pertanto, qui può essere solo introdotto, al fine di ricondurlo entro la prospettiva d'esame, per delineare quali nuove questioni dovranno essere considerate in sede di predisposizione degli standard di sicurezza.

Tutto ha origine da ciò che, in filosofia etica, è noto come «dilemma del carrello» che si concretizza nelle scelte compiute dal software di guida autonoma[181]: le macchine dovranno decidere chi salvare o proteggere in caso di collisione. Quali istruzioni dovrà ricevere il sistema per scegliere quale ostacolo, tra due potenziali, colpire? La scelta deve basarsi sulla comparazione dell'entità del danno, o dovrebbe tener in considerazione altri criteri? E nel caso il sistema dovesse optare tra ferire più persone, o colpirne sola una fatalmente?

Tutte le considerazioni etiche sono, imprescindibilmente, legate al problema della responsabilità giuridica: seguire la via più scontata, e imputarla al produttore in quanto soggetto responsabile del prodotto finale, significherebbe attribuirgli le responsabilità per la decisione etica che, convenzionalmente, sarebbe stata presa dal conducente trovatosi nella medesima circostanza. Quali criteri avrebbe, dunque, dovuto seguire il produttore nella progettazione del software? In questa prospettiva diverrebbe necessaria la predisposizione

[180] Sul concetto di comportamento morale dell'auto a guida autonoma e la proposta di modelli di studio *ad hoc* si rinvia a N.J. Goodall, *Machine Ethics and Automated Vehicles*, in G. Meyer e S. Beiker (a cura di), *Road Vehicle Automation. Lecture Notes in Mobility*, Cham, Springer, 2014, pp. 93-102.

[181] J.J. Thomson, *The Trolley Problem*, in *Yale L.J.*, 94, 1985, pp. 1395-1396.

di una gerarchia di criteri per coordinare principi etici e azioni giuridiche[182].

È importante, dunque, stabilire se questa parte del design, o codice, della macchina debba essere oggetto, ed entro che limiti, della standardizzazione. La risposta sembra essere affermativa qualora si consideri la *ratio* dell'armonizzazione degli standard tecnici: un parametro fondamentale per la valutazione obiettiva del prodotto, per di più frutto del dialogo tra istituzioni europee e organismi privati che può contribuire ad affrontare questioni etiche al fine di far entrare in commercio solo la tecnologia più sicura. In questa prospettiva diverrebbe necessaria la predisposizione di una gerarchia di criteri per coordinare principi etici e azioni giuridiche[183].

A una visione più generale, i problemi appena delineati confermano la necessità di favorire l'approccio della *governance-by-design* che, come anticipato nel capitolo I, sta diventando un modello di *policy making* importante[184].

7.4. *La responsabilità del produttore e i criteri di valutazione della sicurezza*

Non vi è, ancora, un approccio sistemico in materia di responsabilità per danni da *self-driving cars*, se non qualche isolata proposta dottrinale[185]. Alcune proposte sono imperniate sulla valutazione dell'applicabilità del corrente

[182] Tutto questo viene trattato da E. Hilgendorf, *Automated Driving and the Law*, in Hilgendorf e Seidel (a cura di), *Robotics, Autonomics, and the Law*, cit., p. 189.

[183] Questa è una delle ragioni per cui l'uso degli standard tecnici rappresentano una soluzione ottimale per regolare AI e prodotti nell'IoT: così osserva Amato, *Product Liability and Product Security*, cit.

[184] D.K. Mulligan e K.A. Bamberger, *Saving Governance-by-design*, in *Calif. L. Rev.*, 106, 2018, p. 697.

[185] U. Ruffolo, *Self-driving car, auto driverless e responsabilità*, in U. Ruffolo (a cura di), *Intelligenza artificiale e responsabilità (Convegno del 29 novembre 2017)*, Milano, Giuffrè, 2017, pp. 36 ss.; Davola, *A Model for Tort Liability in a World of Driverless Cars*, cit. L'autore dà conto delle più attuali proposte.

regime di responsabilità da prodotto, mentre altre studiano quali nuovi modelli di responsabilità potrebbero meglio disciplinare lo scenario radicalmente nuovo degli incidenti provocati dalla guida autonoma[186]. Entro il primo ambito, una preliminare distinzione dovrebbe essere tracciata tra il difetto del software e dell'algoritmo, e il difetto materiale nel prodotto che è governato o animato dall'algoritmo (es. i sensori). Sono, poi, intuitive le difficoltà probatorie relative al «difetto-tipo», quello di progettazione, specialmente con riguardo all'operatività del comando di sostituzione della guida umana: una misura di sicurezza centrale nella *litigation* della responsabilità da prodotto. Pensando alla corrente diffusione delle auto di livello 3 di autonomia, si potrebbero configurare due distinti scenari di responsabilità da prodotto: 1) il sistema di *hand-over* potrebbe non funzionare correttamente, in base al modo in cui è stato progettato; 2) gli algoritmi potrebbero non riuscire ad anticipare la necessità di azionare il sistema di sostituibilità in particolari circostanze[187]. Quest'ultimo scenario risulterebbe ancor più complicato dalle difficoltà probatorie: il danneggiato dovrebbe provare il difetto del software di guida autonoma, nonché il fatto che quel difetto specifico è stato la causa dell'incidente.

Ma i problemi originano anche dalle sofisticate parti che compongono un'autovettura del tipo di quelle in esame. A titolo di esempio, si pensi a tutti i fattori che incidono sul

[186] K.S. Abram e R.L. Rabin, *Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era*, in *Virginia Law Review*, 105, 2019, in corso di pubblicazione. Gli autori propongono un modello di responsabilità definito *Manufacturer Enterprise Responsability* costruito a partire da considerazioni di contesto: *in primis*, l'importanza dell'incidenza della *safety technology*. Essi osservano: «the needless cost and anachronistic quality of design defect litigation will consequently call into question not only how responsibility for these accidents should be allocated, but also how compensation should be measured and awarded. In this regard, a reformulation of responsibility standards for Hav-related accidents would highlight for reconsideration the case-by-case "make whole" approach to tort compensation as well».

[187] Cfr. Abram e Rabin, *Automated Vehicles and Manufacturer Responsibility for Accidents*, cit.

malfunzionamento dei sensori. Inoltre, anche altre circostanze contribuiscono a complicare la scena: si pensi al fatto che più persone nella macchina possano fungere da conducente, con conseguente difficoltà di individuare quale possa essere un parametro di riferimento quando si considera che l'auto dev'essere *as safe as a human driver*[188].

Anche il contesto delle *self-driving car* mette in primo piano il problema della scelta del criterio per la valutazione della sicurezza.

Lo standard della sicurezza che la persona può legittimamente attendersi diventa un requisito generale che necessita di contenuti più precisi: è difficile individuare il rischio «socialmente accettabile», date le variabili che incidono nell'uso delle *self-driving cars*.

Quanto è sicuro chi è nell'abitacolo della vettura o chi circola nel traffico? Dal punto di vista statistico, la vettura autonoma dovrebbe essere più sicura di quella tradizionale, o almeno tanto quanto la stessa. Ma anche tale standard appare molto astratto. Solo il dato statistico, considerato su larga scala, può essere significativo. Altro metodo potrebbe basarsi sulla valutazione comparativa di un'ipotetica condotta del conducente mediamente avveduto ed esperto. Tuttavia, un software di guida autonoma non può essere paragonato a una condotta umana, poiché l'errore della macchina avviene per cause diverse da quelle che caratterizzano l'errore umano.

La casistica è ancora molto limitata per poter disporre di criteri valutativi. Nell'ordinamento americano, oltre al recentissimo caso della Volvo di Uber, descritto in apertura al volume, vanno, infatti, ricordati solo pochi altri incidenti provocati da Tesla: in uno, il conducente della Tesla Model S, dotata di un sistema a guida assistita (non autonoma) perse la vita in uno schianto autostradale contro un camion. Il camion, completamente bianco, aveva occupato la carreggiata dell'auto Tesla, la telecamera non era riuscita a interpretare questa situazione imprevista, poiché lo sfondo chiaro del cielo

[188] Così M. Schellekens, *Self-driving Cars and the Chilling Effect of Liability Law*, in *Computer Law & Security Review*, 31, 2015, pp. 506-517.

aveva formato una sorta di schermo bianco[189]. Lo scontro, avvenuto con un tir, provocò la morte dell'autista e – secondo il rapporto preliminare della *National transport safety board* – non vi era stato alcun malfunzionamento del sistema, ma solo il mancato intervento del conducente; nell'altro, una Model X si schiantò contro un *guard-rail* di legno, mentre il veicolo viaggiava con la stessa modalità *Autopilot*[190]. Anche la casa automobilistica Toyota è stata citata in più distretti per un difetto relativo al software incorporato in un suo modello di vettura, il quale provocava un'accelerazione del veicolo nonostante la frenata del conducente[191].

Tuttavia, il problema dell'individuazione del regime di responsabilità applicabile in caso di incidenti causati da veicoli a guida autonoma non è del tutto nuovo. Nel *case law* americano si annovera un modesto numero di questi casi. In *Ferguson v. Bombardier Service Corp.*[192], per esempio, la corte rigettò l'azione di responsabilità per difetto di costruzione esperita contro il produttore di un sistema di pilotaggio automatico di un aereo cargo militare, ritenendo che il carico fosse improprio e l'incidente fosse stato provocato dal fattore atmosferico (vento). Anche i casi più risalenti nel

[189] Tra gli Stati americani che per primi hanno approvato il transito di vetture a guida autonoma su strada si annovera: il Nevada con il Bill 69 del 2016 e la Florida con il Bill 7027 del 2018. Inoltre, il *California Department of Motor Vehicles* (Dmv) ha, da poco, annunciato l'entrata in vigore dal 2 aprile 2018 di una regolamentazione che elimina l'obbligo della presenza a bordo di una persona al posto del conducente per prendere il comando del mezzo in caso di emergenza, si rinvia al sito https://www.dmv.ca.gov/portal/dmv. Altri diciannove Stati stanno discutendo simili progetti di legge cfr. J.S. Brodsky, *Autonomous Vehicle Regulation: How an Uncertain Legal Landscape May Hit the Brakes on Self-Driving Cars*, in *Berkeley Tech. L.J.*, 31, 2016, p. 851.

[190] Si rinvia al post: *Road death puts the brakes on self-driving cars as flaws are exposed*, in www.lse.ac.uk, 2016.

[191] *In re Toyota Motor Corp. Unintended Acceleration Mktg*, n. 1100-01 (Central District of California, 27 dicembre 2013). La Corte aveva negato alla Toyota il *summary judgement* richiesto sulla base della mancanza, da parte attrice, della prova del difetto di design. L'attrice, aveva fatto ricorso alla regola dell'*inference*.

[192] *Ferguson v. Bombardier Service Corp.*, n. 05-14781 (US Court of Appeals, 26 luglio 2007).

tempo presentano analoghi problemi. In *Nelson v. American Airlines, Inc.*[193], la Corte fece ricorso al criterio della *res ipsa loquitur* per identificare un comportamento negligente in capo all'American Airlines per i danni causati dai suoi aerei che viaggiavano in modalità pilota automatico. L'American Airlines avrebbe dovuto allegare, quale prova liberatoria, fatti relativi alla causa sopravvenuta e imprevedibile.

Il malfunzionamento dell'auto dovrebbe essere ricondotto in una delle categorie classiche dei difetti, ma la gamma delle potenziali cause degli stessi si amplia, in virtù della complessità ricordata, si pensi a virus, guasti di rete ed errori dei dispositivi informatici[194].

Le circostanze introducono, pertanto, una questione da sempre collegata, relativa all'individuazione dei soggetti in grado di sopportare i costi per riparare i danni. La soluzione attuata nelle sentenze americane ricordate si basa sulla *inference doctrine*[195], corollario della regola della *res*

[193] *Nelson v. American Airline*s, Inc., n. 24240 (Court of Appeal California, 9 luglio 1968).

[194] Il *computer code* non è stato considerato unanimemente un prodotto. In alcuni casi, i giudici l'hanno qualificato alla stregua di un servizio. Vedi, per esempio, *Motorola Mobility, Inc. v. Myriad France SAS*, n. 11 C7373 (United States District Court, 2 febbraio 2012), laddove allegando il difetto del software l'attore agisce per violazione delle condizioni di garanzia contrattuale e non per responsabilità da difetto. Attualmente sono già state esperite, contro varie aziende automobilistiche presenti sul mercato, diverse *class action* che sarebbero destinate ad aumentare in modo considerevole nel caso di incidenti provocati da veicoli a guida automatizzata. Si pensi alla *class action* per frode contro l'azienda automobilistica Toyota nella quale si affermava che la Toyota avesse nascosto per anni i problemi di accelerazione delle sue autovetture Lexus e Scion. L'inchiesta del governo americano è stata aperta contro la stessa azienda automobilistica per un problema al sistema frenante Abs dell'ultimo modello della *Prius*. In tal senso *Toyota, accordo in class action Usa con esborso 1,1 mlddlr*, 2012, in www.reuters.com; e *Toyota, scatta la class action per frode*, 2010, in www.corriere.it.

[195] Le considerazioni circa l'attribuzione delle «porzioni» di responsabilità (*apportioning responsibility*) sulle parti che hanno partecipato alla costruzione e al mantenimento del sistema di guida automatizzata sono state svolte, talvolta, nella variante della c.d. responsabilità per la *common enterprise*. Ciò avviene soprattutto nel campo della protezione del consumatore a opera della *Federal Trade Commission* per affrontare

ipsa loquitur: l'incidente occorso sarebbe, di per sé stesso la prova di un difetto[196]. Con questa premessa, non resterebbe che ripartire le responsabilità tra progettisti, costruttori e programmatori[197].

Secondo alcuni, sebbene i programmi di AI siano più «adattabili» e basati sulla capacità di apprendere dalle circostanze ambientali[198], non vi sarebbe alcuna ragione per introdurre una differenziazione rispetto ad altri veicoli, ma solo, eventualmente, la necessità in Europa di vincolare in maniera più incisiva i costruttori a più elevati standard di sicurezza[199]. Sta proprio qui la difficoltà. L'autonomia elevata e le potenzialità del machine learning delle macchine più evolute introducono elementi di criticità, dal momento che esiste un certo margine di imprevisto e sta alla progettazione, al testing e alla certificazione definire quale sia l'entità di tale margine. I veicoli autonomi, infatti, percepiscono l'ambiente con sensori, ne interpretano le misure e, in base a tale interpretazione, l'algoritmo di controllo effettua opzioni di scelta. La prevedibilità dell'interpretazione del dato sensoriale è correlata alla prevedibilità di ciò che il veicolo si troverà davanti[200].

Il problema più complesso riguarda, allora, la valutazione del malfunzionamento dell'algoritmo, poiché ciò implica l'analisi delle regole impiegate nei programmi dei

il problema della concorrenza delle imprese nel porre in essere pratiche commerciali fraudolente. Cfr. *FTC v. Network Servs. Depot*, Inc., n. 09-15684 (Court of Appeals, 16 agosto 2010).

196 I convenuti dovrebbero, quindi, argomentare che la *doctrine* non dovrebbe essere applicata quando non sia possibile ravvisare il nesso di causa tra il danno e il design difettoso. Cfr. *Restatement (Third) of Torts: Prod. Liab*., par. 3 (1998). La guida autonoma provoca continui interrogativi di questo tipo.

197 Vedi *supra* nota 114.

198 Sulla responsabilità per le azioni dell'agente si rinvia ai par. 7.03, par. 7.07 del *Restatement (Third) of Agency* (2006).

199 Vladeck, *Machines without Principals*, cit., p. 127.

200 Prof. Luca Bascetta (professore associato di Robotica e Automatica industriale) e Matteo Matteucci (professore associato di Sistemi di elaborazione delle informazioni), intervistati dall'autore, Politecnico di Milano, Milano, Italia, 7 giugno 2018.

computer per prevenire gli incidenti e minimizzare le perdite. Sul tema si richiamano tutte le considerazioni relative alla *machine ethics*.

Si tratta di nuovi elementi che modellano l'architettura della sicurezza nella progettazione e comprendono aspetti tecnici che riguardano i sensori, gli attuatori, la segnalazione del difetto, le previsioni dei potenziali errori nel software, il controllo delle azioni non programmate, e della collisione con oggetti e pedoni che condividono lo spazio in cui si muove il veicolo, la stabilità e il calcolo delle traiettorie. Ma il design riguarda anche la c.d. *human machine interface* (Hmi)[201], e la deviazione rispetto alle pratiche di guida. L'interazione tra veicolo e conducente ha un ruolo importante nel design di veicoli a guida autonoma. Le complessità sono, infatti, in parte dovute alle sofisticate funzioni del veicolo che convertono i segnali provenienti dall'interazione con l'ambiente e quelli relativi al suo funzionamento in accurate informazioni per il conducente.

8. *Considerazioni di sintesi e finali*

Il capitolo ha affrontato le questioni poste dagli artefatti robotici sul versante della responsabilità civile, prendendo le mosse dal rapporto intercorrente tra le regole che disciplinano il sistema sicurezza-responsabilità e l'innovazione.

L'osservazione *bottom up* dei diversi prodotti robotici ha prospettato quali elementi costituiscono nuove tipologie e fonti di rischio, segnandone la differenza rispetto ai prodotti inevitabilmente pericolosi (cap. II, par. 8.3).

La sicurezza dei robot si può raffigurare come un'immagine complessa, dove appare fondamentale la capacità e l'esperienza di chi usa e interagisce con gli stessi. Com'è

[201] Si noti che ciò è particolarmente rilevante per le auto dotate del livello Sae 3 nel quale il conducente deve monitorare ed essere pronto ad assumere il controllo del mezzo, ma tale capacità potrebbe essere osteggiata dai limiti che caratterizzano la capacità umana di essere vigili quando, di fatto, non si è alla guida del veicolo.

stato osservato all'inizio del paragrafo 4, il potenziamento degli standard tecnici armonizzati è strumento idoneo a garantire l'immissione in commercio della miglior, e più sicura, tecnologia disponibile. Gli standard, inoltre, si candidano a essere strumento funzionale a disciplinare quella parte del codice che determina il «comportamento» della *machine ethics*. Tuttavia, in molte occasioni, uno sguardo alle promettenti caratteristiche della robotica avanzata, rappresentate *in primis* dalle ricerche sull'autoapprendimento, ha permesso di delineare quali ostacoli potrebbero porsi, di fatto, nella predisposizione dell'intervento regolatorio preventivo. Il *case-study* delle macchine a guida autonoma ha fornito un chiaro esempio di tutto ciò.

Se, a una visione d'insieme, il sistema sicurezza-responsabilità appare già sufficientemente elastico per rispondere alle questioni poste dalle tecnologie emergenti, ciò non toglie che sia auspicabile, anche in Europa, una lettura più sistematica dello stesso, secondo il modello delle *courts* americane.

A una lettura di dettaglio, invece, le caratteristiche della robotica avanzata inducono a ripensare la fattispecie di responsabilità del produttore sotto molteplici profili, come descritto nel paragrafo 5. La tradizionale tassonomia dei difetti, ad esempio, è messa alla prova dai tratti *sui generis* del malfunzionamento originato dall'esecuzione della sequenza algoritmica. Altro problema, centrale in materia, è posto dalla valutazione del difetto del design del robot: l'articolato dibattito in merito all'identificazione dei criteri di riferimento, ha fatto emergere, in particolare, quali elementi potrebbero incentivare il passaggio dal parametro della ragionevolezza a quello statistico.

Non sono solo le caratteristiche strutturali della tecnologia robotica a richiedere un adattamento delle regole giuridiche, ma anche ragioni di policy. Per esempio, a propiziare eventuali adattamenti dei regimi assicurativi o di forme di indennizzo speciali, ovvero immunità parziali sarebbe non solo, o non sempre, il grado di autonomia elevata, o le promettenti ricerche su adattabilità e percezione, ma anche ragioni di carattere funzionale alla tutela di valori garantiti costituzionalmente. Le protesi robotiche e l'utilità

sociale dei robot da compagnia hanno esemplificato questo profilo (par. 7.3).

In prospettiva futura, alcune applicazioni biomedicali, come l'assistente robotico, sembrerebbero delineare un passaggio evolutivo in materia di sicurezza: la sicurezza del prodotto potrebbe coincidere con la sicurezza della prestazione, con ciò implicando tutti i mutamenti dovuti al diverso regime di responsabilità previsto. Sono, però, casi relativi ad applicazioni ancora, per lo più, in fase progettuale. In fondo, questo spunto che si aggiunge al già variegato panorama suggerisce di procedere *sector by sector*.

In conclusione. Fin dalle prime pagine, l'interazione uomo-robot e robot-ambiente, così come le questioni di compatibilità etica e di desiderabilità sociale del progresso hanno indotto a ripensare ciò che incide sul livello di sicurezza ragionevole e sulle ragioni che potrebbero minare la certezza del diritto in tale contesto. L'incertezza non riguarda solo i rischi, ma anche il modo stesso in cui la tecnologia evolve: nel nuovo ecosistema dell'IoT aumenta il numero delle variabili che incidono sulla sicurezza dei robot «connessi».

Infine, ha trovato riscontro l'obiettivo sottotraccia: l'apporto di diversi saperi è condizione essenziale della ricerca giuridica riguardante un cambiamento tecnologico. Queste pagine forniscono solo alcune prime indicazioni, poiché sono molti gli esperimenti che il giurista dovrà ancora compiere per poter sfruttare, a pieno, le potenzialità di tale lavoro e approdare, così, a una ricerca autenticamente interdisciplinare.

Ormai pare un passaggio imprescindibile: gli adattamenti giuridici necessari ad accogliere il cambiamento tecnologico, garantendo ai consumatori un elevato livello di sicurezza degli artefatti, si svelano anche a partire dal lavoro su questo fronte.