
Notre Dame Journal of International & Comparative Law

Volume 11 | Issue 2 Article 4

6-24-2021

Liability and Emerging Digital Technologies: An EU Perspective

Maria L. Montagnani

Mirta Cavallo

LIABILITY AND EMERGING DIGITAL TECHNOLOGIES: AN EU PERSPECTIVE

MARIA LILLÀ MONTAGNANI AND MIRTA CAVALLO*

---

* This work reflects the work carried out by one of the authors – Maria Lillà Montagnani – within the EU expert group on product liability – new digital technologies formation. Opinions herein expressed are however the author's personal ones. Maria Lillà Montagnani is an Associate Professor of Commercial Law, Bocconi University of Milan (Italy) and a Transatlantic Technology Law Forum Fellow, Stanford Law School. The work was written while she was a NYU Global Houser Research Fellow 2019-2020 (NYU Law School, NY) and the author is grateful to the participants to the NYU Global Fellows Forum for the insightful comments to a first draft of the paper, in particular to Gráinne de Búrca, Florian Möslein, Dhanay Cadillo Chandler and Amandine Léonard. Mirta Cavallo is a graduate of Bocconi University Law School. In 2018 she also completed the LLM in Law of Internet Technology of Bocconi University. The views expressed in the article present the authors' own opinion.
This article was lastly updated in Spring 2020.

INTRODUCTION

Emerging digital technologies (EDTs),[1] (e.g. Internet of Things and of Services (IoT/IoS),[2] Artificial Intelligence (AI),[3] advanced robotics,[4] and autonomous vehicles (AV)[5]) can lead to fundamental discoveries, opening up new possibilities, and significantly improving the lives of many, particularly, by bringing major benefits to our society and economy through better healthcare, more efficient public administration, stronger democratic processes, safer transport, a more competitive industry, and sustainable farming. Machine-learning,[6] for example, can be used to make more accurate and faster medical diagnoses and surgeries,[7] carry out dangerous and repetitive tasks, and free up valuable time. The Internet of Bodies, that is, the merger of IoT and AI with the

1 The category of emerging digital technologies is not fully defined and exhaustively identified in European documents on the topic, where they are indicated with the exemplificative list of "Internet of Things (IoT), Artificial Intelligence, advanced robotics and autonomous systems". In this work, the wording of the EU institutions is adopted.

2 IoT is "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies." (Recommendation ITU-T Y.2060, June 2012, https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060, p. 1). An overview of the IoT as "the next major economic and societal innovation wave enabled by the Internet.", together with an account of technologies and phenomena like personal wearables, smart homes, smart cities, smart manufacturing, smart energy, smart farming, and circular economy, are provided in Staff Working Document, *Advancing the Internet of Things in Europe*, 19.4.2016, SWD(2016) 110 final, http://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:52016SC0110, accompanying the Communication of the European Commission, *Digitising European Industry - Reaping the full benefits of a Digital Single Market*, COM (2016) 180, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016DC0180&from=EN.

3 According to the definition endorsed at European level, "[a]rtificial intelligence (AI) refers to systems that display intelligent behavior by analyzing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)." High-Level Expert Group on Artificial Intelligence, *A definition of AI: Main capabilities and scientific disciplines* 1 (2019), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341.

4 Robotics is interestingly defined as "AI in action in the physical world." Not surprisingly, it is also referred to as embodied AI." For an overview of relevant initiatives of the European Union, *see* https://ec.europa.eu/digital-single-market/en/robotics.

5 An account of the initiatives of the European Union in relation to Connected and Automated Mobility (CAM) is available at https://ec.europa.eu/digital-single-market/en/connected-and-automated-mobility-europe. *See also* Katie Atkinson, *Autonomous Cars: A Driving Force for Change in Motor Liability and Insurance*, 17 SCRIPTED A J. L., TECH. & SOC'Y 125 (2020); Francesco Paolo Patti, *The European Road to Autonomous Vehicles*, 43 FORDHAM INT'L L.J.125 (2019).

6 Machine learning – either supervised, unsupervised or reinforcement learning – is only one of the several learning techniques used to train AI, along with, for instance, neural networks, deep learning, and decision trees. The goal is to engineer a general intelligence characterized by autonomy, self-reflection, self-improvement, and commonsense, in the ambitious attempt to replicate, or even outdo, human intelligence. *See* PETER VOSS , ARTIFICIAL GENERAL INTELLIGENCE (Springer 2007).

7 For instance, neurodegenerative disorders, such as Parkinson's and Alzheimer's disease, could be diagnosed on the basis of mouse flickers registered by an AI application. Ryan W. White, P. Murali Doraiswamy, E ric Horvitz, *Detecting Neurodegenerative Disorders from Web Search Signals*, NPJ DIGITAL MED. 1 (2018), https://www.nature.com/articles/s41746-018-0016-6). Characteristics and issues of healthcare AI applications are analyzed in Drew Simshaw, Nicolas Terry, Kris Hauser, M.L. Cummings, *Regulating Healthcare Robots: Maximizing Opportunities While Minimizing Risks*, 22 RICH. J. L. & TECH 1 (2016).

human body, can allow athletes to track their performance with a watch, truck companies to check the alertness of their drivers, and patients to be reminded if they forgot to ingest their medication on the basis of a sensor implanted in their stomach.[8] In more general terms, such technologies have the potential to transform products, services, activities, procedures, and practices in several economic sectors and in relation to many aspects of society, promising increased productivity and efficiency gains. At the same time, EDTs can even play a key role with regard to climate and environmental-related challenges, as enablers for advancing the 2030 Agenda and attaining the Sustainable Development Goals of the Green Deal.[9] Moreover, quantum computing is expected to be a game-changer, thus leading EDTs beyond anything currently envisaged.[10]

However, as smart machines develop in a way that makes them pursue their tasks with diverse degrees of autonomy,[11] their new and enhanced potential brings in risks – or increase the existing ones – for both those who offer them and those who use them. Indeed, such technologies may have unintended effects or be used for malicious purposes. The list of new possible "algorithmic damages" is as long and various as the list of new ways to inflict old harms. Algorithms trained with biased data may lead to biased decisions to the detriment of minorities when screening job candidates, assessing creditworthiness for loans, or predicting criminal behaviour.[12] Not surprisingly, even a chatbot may turn out to be racist[13]. Autocomplete functions of search engines may cause defamation, reputational damage, or trademark violations.[14] Robo-advisors may lead to wrong investments,[15] while errors in automated diagnoses and surgeries may ruin a person's life. Cybersecurity vulnerabilities in smartwatches for children may be exploited to obtain access to the child,[16] while a flaw in the radio of a vehicle could expose the risk of unauthorised access by a third party maliciously intending to take over the control system of the self-

8 Andrea M. Matwyshyn, *The Internet of Bodies,* 61(1) WM. & MARY L. REV. 77 (2019).

9 *Communication of the European Commission*, *The European Green Deal*, COM (2019) 640 final (Dec. 11, 2019), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52019DC0640&from=EN. For an overview of Sustainable Development Goals, *see* resources available at https://ec.europa.eu/eurostat/web/sdi and https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm.

10 Commission Staff Working Document, *Quantum Technologies*, 19.4.16, SWD(2016) 107, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15270, accompanying the *Communication of the European Commission Parliament the Council, the Europe Economic and Social Committee of the Regions*, *European Cloud Initiative - Building a competitive data and knowledge economy in Europe*, COM (2016) 178 final (Apr. 19, 2016) , https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15266.

11 On the concept of autonomy, see *infra* para 2.

12 James Manyika, Jake Silberg, and Brittany Presten, *What Do We Do About the Biases in AI?*, HARV. BUS. REV. (2019), https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai.

13 This occurred with Tay, the chatbot developed by Microsoft to self-learn conversational skills and autonomously interact with users via Twitter. It was shut down in 2016. Sarah Perez, *Microsoft silences its new A.I. bot Tay, after Twitter users teach it racism*, TECHCRUNCH (2016), https://techcrunch.com/2016/03/24/microsoft-silences-its-new-a-i-bot-tay-after-twitter-users-teach-it-racism/.

14 Stavroula Karapapa, Maurizio Borghi, *Search Engine Liability for Autocomplete Suggestions: Personality, Privacy and the Power of the Algorithm*, 23(3) INT'L J. L. AND INFO. TECH. 261 (2015).

15 Dominic Litz, *Risk, Reward, Robo-Advisers: Are Automated Investment Platforms Acting in Your Best Interest*, 18(2) J. HIGH T. L. 367 (2018).

16 On a similar case, see the RAPEX notification from Iceland published in the EU Safety Gate's website (A12/0157/19).

driving car.[17] In fact, although autonomous vehicles promise a reduction of accidents caused by human errors, flaws in object recognition technologies embedded in self-driving cars could still cause accidents, and thus injuries and material damage. Similarly, cyberattacks on the control systems of driverless metro, autonomous weapons, industrial plants, or critical infrastructures may cause enormous damage as well.

This scenario certainly raises challenges for regulators and policymakers that, in the context of an overall strategy for "responsible innovation,"[18] have to face the ontological difficulty of foreseeing and possibly controlling the impact of EDTs on economy and society, to make sure that they are human-centric, ethical, explainable, sustainable and respectful of fundamental rights and values.[19] An ecosystem where both citizens and businesses can trust the technology they interact with is, in fact, fundamental to both unlocking the potential of the above-mentioned new technologies and enabling them to ameliorate people's lives. An environment of trust and accountability around the development and use of AI-powered devices and autonomous self-learning systems includes, therefore, the design of legal rules on civil liability[20] – or the adaptation of existing ones – to the risks generated by their use.

The adequacy and completeness of liability regimes in the face of technological challenges are indeed crucial for society. If the system is inadequate or flawed or has shortcomings in dealing with the damages caused by EDTs, victims may end up partially compensated. On the other hand, an overprotective liability regime risks to stifle the development and use of EDTs – and in the last instance, innovation – by introducing systems that overcompensate for harm generated during the operation of such technologies.

In this context, many are the questions that arise and are in need of an answer. Does the current legislative framework in the EU address all the possible damages that can derive from the use of EDTs, or encompass a general clause suitable to cover all of them? What – if any – gaps do the current legal framework reveal? What possible amendments are currently being studied and proposed? Given the features of emerging digital technologies, would a one-size-fits-all solution be preferable, or should a technology-specific oriented solution be adopted? Does it make sense to recognize autonomous systems as legal entities that may be held liable in damages? Should specific obligations be

17 On a similar case, see the RAPEX notification from Germany published in the EU Safety Gate website (A12/1671/15).

18 This concept, intended to emphasize the role of responsibility in shaping and promoting innovation, is gaining increasing attention among scholars and policy makers. On this, *see* B.J. KOOPS, I. OOSTERLAKEN, H. ROMIJN, T. SWIERSTRA, J. VAN DEN HOVEN (EDS), RESPONSIBLE INNOVATION 2. CONCEPTS, APPROACHES, AND APPLICATIONS (Springer 2015).

19 There is a lively discourse around ethical issues raised by new technologies, as analyzed in M.D. DUBBER, F. PASQUALE, S. DAS (EDS), THE OXFORD HANDBOOK OF ETHICS OF AI (Oxford U. Press 2020);M. COECKELBERGH, AI ETHICS (The MIT Press 2020). With specific regard to algorithmic transparency and the need to shift from a black-box society to an intelligent one, *see* F. PASQUALE, THE BLACK BOX SOCIETY 218 (Harvard University Press 2015)("Rather than contort ourselves to fit 'an impersonal economy lacking a truly human purpose,' we might ask how institutions could be re-shaped to meet higher ends than shareholder value . . . Black box services are often wondrous to behold, but our black box society has become dangerously unstable, unfair, and unproductive. Neither New York quants nor California engineers can deliver a sound economy or a secure society. Those are the tasks of a citizenry, which can perform its job only as well as it understands the stakes").

20 This work focuses on civil liability, to be distinguished from criminal. Later in this work, the term liability is used by the court to refer to civil liability.

imposed on providers of EDTs as to the design of the technology (i.e., "safety by design")? Should safe harbours aim at enabling a data-driven economy be adopted? Where to strike a balance between the need to compensate victims and encouraging innovation?

To answer the above questions, one should identify the normative foundations on which a liability regime for new technologies may be built on.[21] While it is often maintained that the objective of the liability system is to compensate victims, this cannot be the only goal of regulators, but it should go hand-in-hand with promoting innovation by providing incentives towards those actors who are best situated to take precautions against harm. To do this, it is crucial to understand whether the existing rules present gaps in considering the possible damages that occur in the context of the use of IoT, AI, advanced robotics and autonomous systems, and to identify possible solutions that would build trust in these technologies. All this can take place only by striking a balance between the need to compensate possible victims and the desire to incentivize innovation. The adequacy and completeness of liability regimes in the face of technological challenges are indeed crucially important for society. If the system is inadequate or flawed or has shortcomings in dealing with damages caused by emerging digital technologies, victims may end up totally or partially uncompensated, even though an overall equitable analysis may make the case for indemnifying them. The social impact of a potential inadequacy in the existing legal regimes to address new risks created by emerging digital technologies might compromise the expected benefits. In addition, certain factors, such as the ever-increasing presence of emerging digital technologies in all aspects of social life and the multiplying effect of automation, can also exacerbate the damage these technologies cause. Damages can easily become viral and rapidly propagate in a densely interconnected society. For these reasons, answering the question as to whether the current liability regime is fit to encompass the damages that might derive from the use of EDTs is urgent and crucial to their own development. The envisaging of possible solutions is also crucial were the current liability regime not completely fit to address the changes brought about by the EDTs.

In the following paragraphs, we seek to ascertain whether the current liability regimes are fit for the new digital environment and to envisage possible measures to face the new reality. To this end, Section 1 preliminary reconstructs the current liability framework, which at the European level is quite fragmented and only partially harmonised. Section 2 analyses the feature of EDTs to illustrate how they challenge the current legal landscape, to the point of questioning traditional liability notions – as explained in Section 3. Section 4 surveys the EU institutions' position on these challenges and Section 5 focuses on the findings of the Report on Liability for AI and emerging digital technologies,[22] as it provides a valid starting point for discussing any adjustments that may be needed. Finally, Section 6 highlights the need for a

21 Rolf H. Weber & Dominic N. Staiger, *New Liability Patterns in the Digital Era*, EU INTERNET L. 197 (2017).

22 Report of the Expert Group on Liability and New Technologies - New Technologies Formation, *Liability for Artificial Intelligence and other Emerging Digital Technologies* (2019), https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608.

multi-faced approach to tackle the ever-changing issues raised by EDTs through an overview of the most viable options to complement liability rules, also from an ex-ante perspective.

I. THE CURRENT LEGAL LIABILITY FRAMEWORK WITHIN THE EU

To understand how the development and use of EDTs impact the current liability notions is necessary to preliminary reconstruct the current liability framework, which at the European level is only partially harmonised.[23] The existing EU tort law rules are, in fact, limited product liability law under Directive 85/374/EC ("PLD"),[24] liability for infringing data protection law (Article 82 of the GDPR),[25] and liability for infringing competition law (Directive 2014/104/EU).[26] There is also a well-established regime governing liability insurance with regard to damage caused by the use of motor vehicles (Directive 2009/103/EC),[27] which though does not touch upon liability for accidents itself. Similarly, not dealing directly with liability but with product safety is the regime introduced under Directive 2001/95/EC on general product safety,[28] which requires that products (with the exceptions of pharmaceuticals, medical devices, and food) meet all statutory safety requirements provided by EU and national laws or comply with national standards.

Similarly, at a national level, there are no Member States' liability provisions that contain liability rules specifically applicable to damage resulting from the use of EDTs, with the exception of those jurisdictions that have regulated the use of AVs, where they also provide for coverage of any damages caused, by insurance or by reference to the general rules.[29] At the moment,

23 Ken Oliphant, *Cultures of Tort Law in Europe*, 3 J. EUR.TORT L. 147 (2012); Mauro Bussani & Marta Infantino, *Tort Law and Legal Cultures*, 63 AM. J. COMP. L. 77 (2015).

24 Council Directive 85/374/EEC of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products (1985) O.J. (L 210) ["hereinafter" PLD]. A thorough account of the PLD is provided in D. Fairgrieve, G. Howells, P. Møgelvang-Hansen, G. Straetmans, D. Verhoeven, P. Machnikowski, A. Janssen, R. Schulze, *Product Liability Directive*, EUROPEAN PRODUCT LIABILITY: AN ANALYSIS OF THE STATE OF THE ART IN THE ERA OF NEW TECHNOLOGIES 17 (Cambridge U. Press 2016). *See also* Micheal G. Faure, *Economic Analysis of Product Liability*, EUROPEAN PRODUCT LIABILITY: AN ANALYSIS OF THE STATE OF THE ART IN THE ERA OF NEW TECHNOLOGIES 619 (Intersentia 2016).

25 Commission Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119). *See also Proposal for Regulation on Privacy and Electronic Communications*, Art. 22, COM (2017) 10 final.

26 Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on Certain Rules Governing Actions for Damages under National Law for Infringements of the Competition Law Provisions of the Member States and of the European Union Text with EEA relevance, 2014 O.J. (L 349).

27 Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 Relating to Insurance Against Civil Liability in Respect of the Use of Motor Vehicles, and the Enforcement of the Obligation to Insure Against Such Liability ,2009 O.J. (L 263).

28 Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on General Product Safety, 2002 O.J. (L 11).

29 *See*, among many, Rustin Diehl & Matthew I. Thue, *Autonomous Vehicle Testing Legislation: A Review of Best Practices from States on the Cutting Edge*, 21 J. TECH. L. & POL'Y 197 (2016); and, in the US: Mark A. Geistfeld, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, 105 CAL. L. REV. 1611 (2017).

therefore, harmful damages that arise during the use of EDTs are likely to be compensated under existing rules in tort and contract law.

In general, domestic tort laws include a rule introducing fault-based liability with a broad scope of application, accompanied by several more specific rules which either modify the premises of fault-liability (especially in the distribution of the burden of proof) or establish liability independently from fault (strict or risk-based liability). Most liability regimes also encompass the notion of liability for others (indirect or vicarious liability), which can, in turn, be – depending on the case or the country – fault- or risk-based.

While this is not the place to engage in a comparative analysis of each Member State's liability framework, it is worth pointing out that they all share some common principles. A general rule of liability for fault is, in fact, part of the legal systems of all EU members, and it is also central to the principles restating the common core of European private law.[30] In a nutshell, when an actor fails to take due care, and this negligence causes harm to another – or she causes such harm intentionally – this actor is liable to compensate the victim. Usually, what triggers liability is harm to the fundamental interests of a person, such as life, health, bodily integrity, freedom of movement, private property, and in some countries also purely economic losses and harm to human dignity. In addition, all Member States' legal systems encompass product liability as a result of the PLD implementation. On this base, a damage claim for harm generated by a defective product does not require a finding of fault on the part of the manufacturer, as, in principle, this should be a strict – not fault-based – liability.[31] However, the regime that the PLD introduces resembles more a watered-down version of negligence liability than a strict liability regime since a claimant must, in any case, prove the defect and that such defect generates the harm that she suffered.[32] Moreover, limits to the compensation may be imposed, depending on the national implementation of the directive, and manufacturers may show that the defect was not linked to their activity (alleging, for example, the risk development defence).[33] In sum, for as much as product liability could be of any use, it only covers damages generated by defective products, leaving outside the provision of services, for which then the default negligence-based regime revives.

As a result, the current EU scenario is quite fragmented. In the first place, even though fault-based liability is a common ground, negligence and fault can be given different interpretations across Member States. In the second place, although the PLD should in principle introduce a harmonized strict liability regime for defective products, in practice, its implementation has not been consistent in all Member States and, in any case, it does not seem to encompass many of the instances generated by the use of EDTs.[34] In the third place, the hypotheses of strict and vicarious liability heavily depend on the traditions of

30 EUROPEAN GROUP ON TORT LAW (ED), PRINCIPLES OF EUROPEAN TORT LAW, Art. 1.101 (1)-(2) http://civil.udg.edu/php/biblioteca/items/283/PETL.pdf. For a comment, *see* F.D. BUSNELLI ET AL., PRINCIPLES OF EUROPEAN TORT LAW: TEXT AND COMMENTARY (Springer 2005).

31 *Id*., Recital 2, "liability without fault".

32 PLD, *supra* note 24, at art. 4.

33 See *infra* para. 4.

34 For a survey of the issues as to the application of the Product Liability Directive to the EDTs, *see* Charlotte de Meeus, *The Product Liability Directive at the Age of the Digital Industrial Revolution: Fit for Innovation?*, 8 J. OF EUROPEAN CONSUMER AND MARKET L. 149 (2019).

each national legal framework, and therefore, they cover a set of not uniform cases. Overall, disparities in Member States' legislation and case-law concerning liability may produce distortions of competition and impair the smooth functioning of the single digital market,[35] while the moderate pace with which the European legislator usually proceeds with legislative harmonization may no longer be adequate to keep up with the rapid changes brought by EDTs.[36]

II. NEW TECHNOLOGIES, NEW FEATURES

Against the background of the current liability regime(s) in Europe, the question arises as to whether they are fit for the new digital era comes from the fact that EDTs present features that are unknown to the previous generation of technologies. Namely: complexity, opacity, autonomy, predictability, openness, data-drivenness, and vulnerability.[37] Even though these features are gradual in nature, their combination may, however, seriously challenge the traditional liability notions.

On the one hand, EDTs demonstrate a high degree of complexity due to the interdependency between the different components and layers, ranging from tangible parts and devices (e.g. sensors, actuators, hardware), to software components, data, and connectivity features. The presence of numerous interdependencies in the value chain increases the variety of players involved, which in turn amplifies the overall complication. In addition, the more complex EDTs become, the less those exposed to them can comprehend the processes that may have caused harm to themselves or to others.

The opacity of these systems may only increase when self-learning features are in place, as algorithms no longer come as readable code but amount to black boxes that are almost impossible to understand.

It is this same self-learning capability that makes EDTs autonomous, i.e. capable of performing tasks and interact with the surrounding environment with less, or entirely without, human control or supervision. Many of the operations provided through and by EDTs can be almost fully autonomous, as IoT-devices, advanced robots and all systems empowered by AI are developing increased capabilities to interpret the environment (via sensing, actuating, cognitive vision, machine learning, etc.), to interact with humans, to cooperate with other actors, to learn new behaviours, and execute actions autonomously without human

35 Awareness of this can be found in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), 2000 O.J. (L 178) 40.

36 Jorge Morais Carvalho & Kristin Nemeth, *Time for a Change? Product Liability in the Digital Era*, J. OF EUROPEAN CONSUMER AND MARKET L. 160 (2019).

37 With specific regard to AI, an additional feature has been flagged as riskful: AI intrinsic monomaniacality towards its objectives, which is especially dangerous when AI autonomously makes decisions and interacts with third parties. The main AI goals are in fact: (i) preserving itself in order to maximize the satisfaction of its final objectives, (ii) preserving the content of its final objectives; (iii) improving its rationality, intelligence and decision-making process, to maximize the satisfaction of the final objectives; (iv) acquiring as many resources as possible for the satisfaction of the final objectives of the AI. All this could lead to unexpected risks and make traditional liability rules unsuitable. *See*, Giovanni Comandè, *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, 1 ANALISI GIURIDICA DELL'ECONOMIA 169, 179 (2019).

intervention. However, the more autonomous systems are, the less they depend on other players (i.e. manufacturers, owners, users, etc.), the greater their impact on their environment and on third parties is.[38]

From the ability to operate autonomously by virtue of their interaction with the environment derives EDTs' unpredictability. Many systems are in fact designed to not only respond to pre-defined stimuli, but to identify and classify new ones and link them to self-chosen corresponding reactions that have not been pre-programmed as such. To do this they rely on the data they have been trained with, as well as the data that they keep collecting while interacting with the surrounding environment, which in turn alters the initial algorithms. As a result, the more external data systems are capable of processing, the more difficult it becomes to foresee the precise impact that they will have once in operation.

On the other hand, in order to operate and self-develop, EDTs depend on external information that is not pre-installed but generated by built-in sensors or communicated from the outside by data sources, in other words they are data-driven. This exposes these new technologies to issues whenever the data is flawed or missing, due to an error in communication or in relation to the external or internal source. Strictly linked to the data-driveness is the feature of openness. In order to operate EDTs need not only to interact with data sources but also with other systems. They are in fact not completed once put into circulation, rather, for their nature, they depend upon subsequent inputs, such as updates and upgrades. For these reasons, EDTs are deemed to be "open by design," so to permit external input either via some hardware plugin or through some wireless connection. However, this constant interaction with outside information is what also makes these new technologies vulnerable to cybersecurity breaches, which can cause the systems to malfunction and/or modify its features in a way likely to cause harm.

All the above-mentioned features, combined with the lack of clear legal requirements for EDTs, make more difficult for enforcement authorities to check compliance with applicable legislation and assess liability. In particular, individuals and legal entities having suffered harm from EDTs products may lack the means to verify possible breaches of laws, thus prejudicing their effective access to justice. At the same time, market surveillance and enforcement authorities may lack adequate technical capabilities for inspecting EDT systems. In some instances, they may not be empowered to act or even be uncertain on whether they do have such powers. For instance, the PLD establishes liability of the manufacturer for damage caused by a defective product. However, it is not easy at all to prove a defect in an autonomous vehicle or retrace its decision-making process leading to a car accident, with the consequence of making more difficult to meet the burden of proof and obtain compensation under the current EU and national liability legislation. To this

38 Autonomous capabilities and intelligence ungoverned by human directions or supervision could lead to unexpected outcomes, as shown by the story of Alice and Bob, i.e., two chatbots developed to learn autonomous bargaining skills that started to interact using their own code, indecipherable for humans. Andrew Griffin, *Facebook's artificial intelligence robots shut down after they start talking to each other in their own language*, THE INDEPENDENT (2017), https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-artificial-intelligence-ai-chatbot-new-language-research-openai-google-a7869706.html.

regard, transparency and explainability of algorithms embedded in EDTs should be legally required to help courts to analyse the functioning process of algorithms, identify any flaw and, accordingly, assign appropriate responsibility for failures in decision-making.[39]

III. NEW TECHNOLOGIES AND TRADITIONAL LIABILITY NOTIONS

Because of their features, EDTs raise several open questions as to the capacity of the known liability regimes to encompass the harm generated by their use. Indeed, besides the well-known issues of lack of accountability[40] and transparency,[41] EDTs do challenge traditional liability concepts such as damages, causal link, and duty of care.

As for the notion of damages, in addition to traditional damages (harm to persons and properties), there are also those connected with the transfer of data, privacy, and confidential information security. Interconnected devices may also constitute targets of cyber-attacks: in the case of smart homes, for example, poor security measures at design, manufacturing or operation stage may allow cyber-attackers to take control of a device and modify its functioning or the functioning of other smart devices in the same ecosystem. Now, while injuries to a person or to a physical property can trigger liability, compensation of pure economic loss is not universally accepted, nor is the case of destruction of data as property loss. Similarly, in the scenario in which personality rights are adversely affected, such as the case in which data is released in violation of the right to privacy, differences exist among jurisdictions.

The most controversial element of the liability regime is, however, the causal link between the victim's harm and the defendant's sphere. In principle, in tort law the victim should show that the damage originated by some conduct or risk attributable to the defendant. However, in the case of EDTs such a proof can become quite difficult. Interconnected devices, for example, such as smart homes or AVs, are the result of a combination of hardware, software, connectivity and data, which may make it impossible to identify the real source of the damage. Providing evidence of causation is even harder when dealing with self-learning AI systems fueled by machine learning and deep learning techniques and based on multiple external data collection. Advanced robots and all products empowered by AI may in fact act in ways that were not envisaged at the time that the system was first put into operation, and these behaviours may be so autonomous to interrupt the causal link. In a strict liability regime, such a proof could be less problematic as it would be enough to be to prove that the risk triggering the strict liability materialised; however, strict liability only applies in very limited cases.

As liability is mainly fault-based, the other fundamental element that the use of EDTs challenges is the definition of the duty of care that the perpetrator should have discharged; behaviour that caused then the damage. While statutory

39 Miriam C. Buiten, *Towards Intelligent Regulation of Artificial Intelligence*, 10(1) EUR. J. OF RISK REG. 41, 55 (2019).

40 Mayaan Perel & Niva Elkin-Koren, *Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement*, 69 FLORIDA L. REV., 181 (2017).

41 FRANK PASQUALE, THE BLACK BOX SOCIETY, *supra* note 19.

language may in certain cases define such duties, in many others they are reconstructed by the court based on social beliefs about the prudent and reasonable course of action in the circumstances at stake. In the case of EDTs, a lack of well-established models of proper functioning of these technologies and the fact that they develop as a result of learning without direct human control makes it difficult to apply fault-based liability rules. While the processes running AI systems cannot all be measured according to duties of care designed for human conduct, an accepted standard of care for the creation and operation of autonomous systems has not emerged yet.

Moreover, in some instances it may be hard even to identify the person obliged to meet such duty of care. In fact, it could be unfair or inefficient to assign liability for any damage caused by an AI product always to the designer of the algorithm. Liability should be allocated also to owners and/or users, depending on the circumstances, but the features of EDTs products make such allocation of liability not self-evident at all.[42] However, according to national liability regimes, tracing a damage back to a specific person is still a fundamental prerequisite for any fault-based claim.[43] Such difficulties have prompted some scholars to suggest alternative options that would revolutionize traditional liability notions. In particular, some scholars urge for joint and several liability of all subjects involved in the design, programming and deployment of an AI application.[44] However, while this would represent a much appreciated simplification for users claiming compensation for damage, it might be ineffective in properly allocating costs and, consequently, setting optimally prevention incentives for all relevant players.[45]

Others argue that if AI is an intelligence even able to supersede humans in a number of areas, such intelligence could be at fault sometimes and, accordingly, it should be held directly liable. This would require to reconceptualize intelligent and autonomous machines as entities with the status of a "person" under the law. With such legal fiction, machines could bear liability in case of wrongdoing in a way similar to that of legal entities such as corporations.[46] However, this may open up more problems than it solves,

---

42 For instance, with regard to autonomous weapons: "somehow human responsibility and accountability for the actions taken by the machine evaporate and disappear. The soldier in the field cannot be expected to understand in any serious way the programming of the machine; the designers and programmers operate on a completely different legal standard; the operational planners could not know exactly how the machine would perform in the fog of war; and finally, there might be no human actors left standing to hold accountable". Kenneth Anderson, Matthew C. Waxman, *Debating Autonomous Weapon Systems, their Ethics, and their Regulation under International Law*, in R. BROWNSWORD, E. SCOTFORD, K. YEUNG (EDS), THE OXFORD HANDBOOK OF LAW, REGULATION AND TECHNOLOGY 1097, 1110 (Oxford University Press 2017).

43 European Commission, *On Artificial Intelligence - A European approach to excellence and trust*, 19.02.20, COM (2020) 65 final, https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

44 David C. Vladeck, *Machines Without Principals: Liability Rules and Artificial Intelligence*, 89 WASH. L. REV. 117, 149 (2014).

45 Giovanni Comandé, *Multilayered (Accountable) Liability for Artificial Intelligence*, in SEBASTIAN LOHSSE, REINER SCHULZE & DIRK STAUDENMAYER (EDS), LIABILITY FOR ARTIFICIAL INTELLIGENCE AND THE INTERNET OF THINGS 165, 175 (Hart Publishing Nomos 2019).

46 *See generally*, Jaap Hage, *Theoretical foundations for the responsibility of autonomous agents*, 25 ARTIFICIAL INTELLIGENCE L. 255 (2017); Brandon W. Jackson, *Artificial Intelligence and the Fog of Innovation: A Deep-Dive on Governance and the Liability of Autonomous Systems*, 35(4) SANTA

particularly as to the definition of selection criteria and equity requirements, as well as to the allocation of costs among all parties involved in the development and use of AI applications.[47] In any case, today at least, legislators and courts seem far from revolutionizing the traditional notions of liability to introduce some sort of robot's fault.

Rather than resorting to conceptually new theories, another – maybe more viable – option that has been proposed is that of introducing a predetermined, detailed and acceptable level of care (or quasi-safe-harbor) for designers, manufacturers, owners and users of EDTs: if the level of care is unmet, a presumption of negligence and, therefore, liability would be triggered; if met, the defendant would enjoy a quasi-safe harbor, while the claimant would bear the burden of proving actual negligence.[48]

IV. THE EU POLICY ON LIABILITY IN THE CONTEXT OF EDTS

The debate on whether the current liability regime is fit for accommodating the issues described above is quite lively within the European Union,[49] in particular as to what extent the existing liability schemes are adapted to the emerging market realities that follow the development of new technologies such as AI, advanced robotics, IoT, and the like. In this regard, the EU institutions have adopted a series of documents that in part tackle to topic, in part highlight the need for further analysis.

For example, in February 2017, the European Parliament adopted a Resolution on Civil Law Rules on Robotics with recommendation to the Commission,[50] which proposed a whole range of legislative and non-legislative initiatives in the field of robotics and AI. In particular, it asked the Commission to submit a proposal for a legislative instrument providing civil law rules on the liability of robots and AI, an initiative so far disregarded. In February 2018, the European Parliamentary Research Service (EPRS) published a study on "[a] common EU approach to liability rules and insurance for connected and autonomous vehicles,"[51] as an added value assessment accompanying the Resolution on Civil Law Rules. On April 25, 2018, the Commission published

---

CLARA HIGH TECH. L. J. 35 (2019). This debate has a long history, as shown by Lawrence B. Solum, *Legal Personhood for Artificial Intelligences*, 70(4) NORTH CAROLINA L. REV. 1231 (1992). A case against treating robots like humans is made by Horst Eidenmüller, *The Rise of Robots and the Law of Humans*, J. OF EUR. CONSUMER AND MKT. L., 765 (2017).

47 Giovanni Comandè, *Intelligenza artificiale e responsabilità*, *supra* note 37, at 180.

48 Omri Rachum-Twaig, *Whose Robot Is It Anyway?: Liability for Artificial-Intelligence-Based Robots*, U. OF ILLINOIS L. REV. 1141, 1172-73 (2020).

49 For an analysis of the extent to which tort law may provide remedies to subjects injured by new technologies in the common law (Anglo-American) tradition *see* Jonathan Morgan, *Torts and Technology*, in ROGER BROWNSWORD, ET AL., (EDS), THE OXFORD HANDBOOK OF LAW, REGULATION AND TECHNOLOGY 522 (Oxford University Press 2017).

50 Resolution on Civil Law Rules on Robotics, EUR. PARL. DOC. 2015/2103(INL) (2017), http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html. *See also*, an analysis in Laura Coppini, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, 4 POLITICA DEL DIRITTO 713 (2018).

51 Tatjana Evas, *A common EU approach to liability rules and insurance for connected and autonomous vehicles*, European Added Value Assessment Accompanying the European Parliament's Legislative Own-initiative Report, European Parliamentary Research Service, PE 615.635 (2018).

a "Staff Working Document on Liability for Emerging Digital Technologies,"[52] accompanying the Commission's Communication on Artificial Intelligence for Europe,[53] which provides the starting point of the discussions on liability and EDTs.

All these documents, as well as the following Sibiu Communication of May 2019,[54] stress that a robust regulatory framework should address the ethical and legal questions surrounding AI, including those related to liability. In its 2018 AI Communication, the Commission also announced the adoption of a report assessing the implications of emerging digital technologies on existing safety and liability frameworks by mid-2019. In its 2019 Work Programme, it confirmed it would "continue work on the emerging challenge of Artificial Intelligence by enabling coordinated action across the European Union."[55] Accordingly, on April 2019, the high-level Expert Group on Artificial Intelligence set up by the European Commission listed liability frameworks among the non-technical methods for securing and maintaining a lawful and trustworthy AI,[56] on the assumption that an environment of trust is crucial for fully reaping the benefits of innovation.[57]

In order to provide an answer, in March 2018, the Commission set up an Expert Group on Liability and New Technologies,[58] operating in two different formations: the Product Liability Directive formation and the New Technologies formation. This second formation was in particular asked to assess "whether and to what extent existing liability schemes are adapted to the emerging market realities following the development of the new technologies such as Artificial Intelligence, advanced robotics, the IoT and cybersecurity issues."[59] The experts were requested to examine whether the current liability regimes are still "adequate to facilitate the uptake of . . . new technologies by fostering investment stability and users' trust."[60] In case of shortcomings, the expert group

52 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, SWD/2018/137 final (2018).

53 Communication of the European Commission, *Artificial Intelligence for Europe*, COM (2018) 237 final (Apr. 25, 2018), .https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018SC0137.

54 European Commission, *Preparing for a more united, stronger and more democratic Union in an increasingly uncertain world*, contribution to the informal EU27 leaders' meeting in Sibiu (Romania), (May 9, 2019), .https://ec.europa.eu/commission/sites/beta-political/files/euco_sibiu_communication_en.pdf.

55 Communication of the European Commission, *Commission Work Programme 2019: delivering what we promised and preparing for the future*, COM (2018) 800 final, (Oct. 23, 2018), https://ec.europa.eu/info/sites/info/files/cwp_2019_en.pdf.

56 High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, at 6, 22, (Apr. 8, 2019), https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines.

57 Communication of the European Commission, *Building Trust in Human-Centric Artificial Intelligence*, COM (2019) 168 final (Apr. 8, 2019), https://ec.europa.eu/jrc/communities/sites/jrccties/files/ec_ai_ethics_communication_8_april_2019.pdf.

58 *See* European Commission Expert Groups, *Expert Group on liability and new technologies*, (Mar. 9, 2018), https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592.

59 *See* European Commission Expert Groups, *Call for Applications for the Selection of Members of the Expert Group on Liability and New Technologies*, (E03592) (Mar. 9, 2018), https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592.

60 *Id.*

was invited to make recommendations for amendments, without being limited to existing national and EU legal instruments. However, recommendations were to be limited to matters of extracontractual liability, leaving aside in particular corresponding (and complementary) rules on safety and other technical standards. As a result of the expert group's activity in November 2019 the Report "Liability for Artificial Intelligence and other Emerging Digital Technologies"[61] was published. This undertakes an assessment of existing liability regimes in the wake of emerging technologies and it concludes that the current ones in force in the Member States ensure at least basic protection of victims whose damage is caused by the operation of such new technologies, while also hinting to the adjustments that might be needed.[62]

The need for some adjustments is confirmed by the recently adopted White Paper on artificial intelligence to foster excellence and trust[63] and by the Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics.[64] Both documents stress the ultimate goal being to ensure remediation of damage caused by emerging digital technologies and overall reliability, while promoting investment stability and, more generally, innovation. In this context, efficient liability rules are indeed paramount for trustworthiness, which in turn is a prerequisite for the uptake of emerging digital technologies. Pursuing such a strategy is also deemed a crucial step to strengthen European technology sovereignty and affirms the role of the European Union on the international stage as "the most attractive, secure and dynamic data-agile economy in the world,"[65] despite a fierce global competition.[66]

For the purpose of achieving these goals, the European Commission suggests a regulatory and investment-oriented approach, entailing, among other things, adjustments to current European and national liability regimes. Indeed, a fragmented legal landscape sprinkled of different national initiatives could lead to the fragmentation of the single market and, consequently, endanger not just legal certainty, but also the emergence of a dynamic and flourishing European industry. For this reason, the European Commission stresses the importance of aligning the efforts at European, national, and regional level,[67] while promoting

61 Report, *supra* note 22.

62 *See infra* para. 5.

63 White Paper, *supra* note 43.

64 Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, COM (2020) 64 final (Feb. 19, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A64%3AFIN.

65 White Paper, *supra* note 43, at 3.

66 The European Union is closely involved in EDTs-related work which is ingoing in multilateral fora, including the Council of Europe, the United Nations (UN) the United Nations Educational Scientific and Cultural Organization (UNESCO), the Organisation for Economic Co-operation and Development's (OECD), the World Trade Organisation (WTO) and the International Telecommunications Union (ITU). For instance, the European Union has contributed to development of the OECD's ethical principles for AI, subsequently endorsed by the G20 in its June 2019 Ministerial Statement on Trade and Digital Economy, *see generally* Organisation for Economic Co-operation and Development, *OECD Principles on Artificial Intelligence*, https://www.oecd.org/going-digital/ai/principles/.

67 Stronger coordination is encouraged in Communication of the European Commission, *see Coordinated Plan on Artificial Intelligence*, COM (2018) 795 final (Dec. 7, 2018), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56018, regarding a plan among the

partnership between the private and the public sector towards an "ecosystem of excellence" with proper incentives to research, innovation and deployment,[68] an "ecosystem of trust" duly protecting fundamental rights and consumers' rights[69] such as privacy and non-discrimination,[70] and through liability rules.

In line with the Report from the expert group, the European Commission's analysis of the current legal frameworks concludes for the adaptations of current norms and the adoption of new specific legislation, pursuing a targeted, risk-based approach, and ensuring effective enforcement. In order to address both current and anticipated technological, societal and commercial developments, such revised regulatory framework should effectively balance protection and innovation, while not being excessively prescriptive and burdensome for businesses.

In addition, establishing a European governance structure with specific regard to EDTs could foster a fruitful cooperation of national competent authorities for a number of tasks, including identification of emerging trends, exchange of information and best practice, advise on standards and certifications, stakeholders' participation, audits and assessments.[71]

V. THE REPORT ON LIABILITY FOR AI AND EMERGING DIGITAL TECHNOLOGIES: A CALL FOR ADJUSTMENTS?

Among the several communications and documents issued by European institutions, the Report on Liability for Artificial Intelligence and other emerging digital technologies ("Report") that has been recently adopted by the Expert

European Commission, Member States, Norway, and Switzerland for some 70 joint actions in the following key areas: (i) increasing investment, (ii) making more data available, (iii) fostering talent, and (iv) ensuring trust. The plan will run until 2027, with regular monitoring and update. As mentioned in the White Paper, a revision of the Coordinated Plan is expected by end 2020, taking into account also the results of the public consultation on the White Paper, *see supra* note 43, at 5.

68 To foster investments, the European Commission has proposed a number of measures under the Digital Europe Programme, Horizon Europe and the Multiannual Financial Framework for 2021 to 2027. On this, *see* European Commission, *Info session Horizon 2020: Artificial intelligence for manufacturing*, (Nov. 18, 2019), .https://ec.europa.eu/digital-single-market/en/news/info-session-horizon-2020-artificial-intelligence-manufacturing. A key role is recognized to Digital Innovation Hubs, *see* European Commission, *Digital Innovation Hubs: helping companies across the economy make the most of digital opportunities*, (Jan. 12, 2021), https://ec.europe.eu/digital-single-market/en/news/digital-innovation-hubs-helping-companies-across-economy-make-most- digital-opportunities. According to the European Commission, making the European Union a lighthouse centre of research requires also upskilling the workforce, offering world-leading masters programmes, and attracting the best professors and scientists, *see* White Paper, *supra* note 43, at 7.

69 The Unfair Commercial Practices Directive 2005/29, 2005 O.J. (L 149/22) (EC); and the Consumer Rights Directive 2011/83, 2011 O.J. (L 304/64) (EC).

70 The EU legislative framework protecting against discrimination encompasses the Race Equality Directive 2000/43/EC, the Directive on equal treatment in employment and occupation 2000/78/EC, the Directives on equal treatment between men and women in relation to employment and access to goods and services 2004/113/EC and 2006/54/EC. In addition, as from 2025, the Directive (EU) 2019/882 on the accessibility requirements for products and services will apply. It is noteworthy that the Commission's Advisory Committee on Equal Opportunities for Women and Men is expected to publish by the end of the year an 'Opinion on Artificial Intelligence' analysing, among other things, the impact of AI on gender equality. In fact, AI risks intensifying gender inequalities, as stated in the Communication of the European Commission, *A Union of Equality: Gender Equality Strategy 2020-2025*, COM (2020) 152 final (Mar. 5, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0152&from=EN.

71 *Id.* at 24.

Group appointed by the European Commission[72] represents detailed and insightful indications on the way in which the EU intend addressing the issue of EDTs and liability. Interestingly enough, in its assessment of existing liability regimes in the wake of emerging digital technologies, the expert group concludes that the rules in force in the Member States ensure at least *basic protection* of victims for damages generated in the use of EDTs. However, the specific characteristics of these technologies and their applications make it more difficult to offer these victims a claim for compensation in all cases where this seems justified. It may also be the case that the allocation of liability is unfair or inefficient. To rectify this, it is likely that some adjustments need to be made to EU and national liability regimes. By saying this, the Report confirms the issue-oriented approach that the EU institutions have adopted within the Single Market Strategy.[73]

Being therefore aware that a size-fits-all solution is not possible, the Report identifies four main categories where adjustments may be needed: (*i*) cases where a (reinterpreted) product liability can still be applied; (*ii*) cases in which strict liability should be extended also to other entities; (*iii*) cases in which there is the need to further develop the notion of duty of care; and (*iv*) cases that can be addresses though vicarious liability, by equalling the device to a human auxiliary.

A. *TOWARD A (REINTERPRETED) PRODUCT LIABILITY*

As a starter, product liability remains a very useful tool to address the damages that may occur in the use of EDTs, as long as a defect can be identified.[74] However, to use product liability, there are some adjustments that the current regime introduced by the PLD needs to undertake. After all, the PLD was adopted in a completely different context from the current one, more than thirty years old in the pre-digital age.[75]

In the first place, the PLD should be interpreted in a way that it encompasses also digital content and services (for example, health, financial, and transport services based on stand-alone software leveraging AI technology) and not just tangible products. Such extensions to stand-alone algorithms could be justified by the rationale of the PLD itself, adopted exactly to address the issues posed by the mass distribution of standardised products available to the general public.[76] While once digital content might not have been commonly used, nowadays, it fulfils many of the functions that tangible movable items used to when the PLD was drafted and adopted. For this reason, damages caused by defective digital content should trigger the producer's liability, in particular in the case in which defective digital elements are linked to other products, some of which come separately from the tangible item (for example, an application to be downloaded into the user's house assistant), or in the case of updates taking place after a

72 Report, *supra* note 22.
73 *Id.* at 15-16.
74 *Id.* at 27-28.
75 K. Nemeth & Carvalho, *supra* note 36; Meeus, *supra* note 34.
76 Jean-Sebastien Borghetti, *Civil Liability for Artificial Intelligence: What Should its Basis Be?*, 17 LA REVUE DES JURISTES DE SCIENCES PO 95, 96 (2019).

product has entered the market.[77] In the second place, it is likely that if the digital content is defective, it will be extremely hard for the claimant to identify the causal link between the harm and the defect. In these cases, therefore, an inversion of the burden of proof might be needed, or at least the burden of proof should be alleviated with regard to the causal relationship between a defect and the damage. Lastly, the possibility for the producers to invoke the unpredictability of the defect should be eliminated in those cases in which it was foreseeable that the technology would develop unpredictably. In other words, the risk development defence, which allows the producer to avoid liability for unforeseeable defects, should not be available in cases where it was predictable that unforeseen developments might occur.[78]

In addition to the recommendations of the Report, it could be argued that existing legislation focuses on the safety risks present at the time that a product is placed on the market. However, proper attention should be given to changing functionalities of EDTs systems, in light of the fact that the frequency of software updates and the ever-evolving features of machine learning may entail important product changes during their lifecycle, thus posing risks unexpected at the time of placing on the market. This is especially true in the event that AI software is integrated into a product when the latter is already on the market. In these circumstances, it should be mandatory to conduct new risks assessments and implement adequate measures, including the obligation to maintain transparency, human oversight and quality of data throughout the product lifecycle.[79]

Also, it could be argued that the scope of application should be extended. On the one hand, while the PLD regulates liability of manufacturers, it is still up to Member States to govern liability of others in the supply chain. It would be advisable to properly allocate responsibilities among different economic operators at the European level, and to require cooperation among economic operators in the supply chain, and with users as well. On the other hand, the concept of safety itself is subject to changes, along with the constant evolution of the threat landscape and the possible categories of damage. For instance, risks deriving from loss of connectivity are not yet explicitly addressed in current legislation, nor more apparently futuristic risks such as mental ones resulting from user collaboration with humanoid robots. Accordingly, the notion of safety should be clarified and broadened.[80]

Another notion which may no longer be adequate, especially in light of the widespread use of software, is that of defect.[81] In fact, the mere fact that a

77 This is also in line with what was provided in two recently published directives: Directive (EU) 2019/771 on the sale of goods provided that a seller is also liable for such digital elements being in conformity with the contract, including for updates provided for as long a period as the consumer may reasonably expect, and Directive (EU) 2019/770 established a similar regime for digital content and digital services. Council Directive 2019/770, 2019 O.J. (L. 136), 1 (EU); Council Directive 2019/771, 2019 O.J. (L. 136), 28 (EU).

78 *See* Council Directive 2019/771, *supra* note 77.

79 White Paper, *supra* note 43, at 14–15.

80 *Id.* at 15.

81 Art. 6(1) of the PLD, *supra* note 24, provides as follows: "A product is defective when it does not provide the safety which a person is entitled to expect, taking all circumstances into account, including: (a) the presentation of the product; (b) the use to which it could reasonably be expected that the product

product with an embedded algorithm causes harm does not make it defective. All the methods traditionally adopted by courts to establish a defect may not be always suitable for algorithms—in particular, (i) proof of malfunctioning may not be obvious in the event of a wrong medical diagnosis delivered by an AI system, as it may not necessarily derive from defective design; (ii) proof of the breach of safety standards may not be a viable path if they are not updated as quickly as technology develops; (iii) comparing risks and benefits associated to the use of a product may not be straightforward when they are of different nature, except, for instance, for pharmaceutical products where risks and benefits have the same nature; (iv) comparing two competing products would be hard when it comes to algorithms, because the overall outcomes should be taken into account, rather than the result of each algorithm in a single set of circumstances. In any case, the fact that an algorithm is less good than another one does not necessarily make the former defective. Otherwise, the market would have only one non-defective algorithm at time—the best one; and (v) a comparison with what a reasonable person would have done in the same circumstances would be tricky when AI is involved, especially considering that recourse to AI is usually justified by the assumption that it performs better than humans.[82]

The difficulties surrounding the notions of fault and defect in relation to EDTs could encourage a shift from fault-based liability to strict liability.

B. *STRICT LIABILITY*

In relation to strict liability, the Report states that this could be appropriate only when the risks generated by the EDTs concretize in a public space. If this is the case, the person who is in control of the risk connected with the operation of the EDT and who benefits from its operation should be held liable.[83] In practice, this is the regime that already applies in some Member States to autonomous vehicles and in some cases that applies also to drones. However, the situation varies significantly among jurisdictions, for example in relation to the coverage of economic loss, which is provided only in few countries. Instead, EDTs that move in public spaces (namely vehicles, drones and the like) are likely to require a general rule of strict liability within the whole single digital market for the significant harm to third parties that they can cause.

Interestingly enough, the Report also points out that, in particular in the context of autonomous cars, the concept of operators is preferable to that of "owner", "user" or "keeper" of the technology.[84] While, in the past, the vast majority of accidents used to be caused by human error, in the future most accidents will be caused by the malfunctioning of technology, though not necessarily of the autonomous vehicle itself. The term "operator" refers to the person who is in control of the risk connected with the operation of EDTs and who benefits from such operation. For example, in the case of a fleet of

would be put; (c) the time when the product was put into circulation." In other words, a product can be considered defective when it is unreasonably or abnormally dangerous. To this regard, *see* Joined Cases C-503/13 and C-504/13, *Boston Scientific Medizintechnik GmbH v. AOK Sachsen-Anhalt – Die Gesundheitskasse and Betriebskrankenkasse RWE*, 2015 ECR-148.

82 Borghetti, *supra* note 76, at 97–98.

83 Report, *supra* note 22, at 39.

84 *Id.* at 40–41.

autonomous vehicles, the operator is likely to be the entity that organizes, maintains and offers the services and it is on the operator that a strict liability regime should be imposed on, without the exclusion of product liability on the side of the producer in case of a defective element.

While it may not be desirable to apply a strict liability regime to any damage caused by EDTs, it may be sensible to do so with regard to specific sectors, such as autonomous vehicles, domestic robots and medicine.[85]

C. *THE NOTION OF DUTY OF CARE*

In the opinion of the experts the issue which is likely to require further attention is the identification of a duty of care, whereby in the use of EDTs, the acting person should apply ordinary prudence as applied by the *pater familias* (a Roman law concept) under similar circumstances, in view of an objective business rationale and the features of EDTs' environment. While it is known that, in the case of more traditional technologies, operators have to discharge a range of duties of care that span from the choice of technology—in particular in light of the tasks to be performed and the operator's own skills and abilities—to the organisational framework—in particular with regard to proper training and monitoring—and to maintenance, the real contours of a duty of care in the use of EDTs is still to be established.[86] In order to refine the concept of duty of care in the context of EDTs, Enterprise Risk Management (ERM) and, accordingly, liability mitigation strategies could point the way.[87]

In addition, the Report also highlights the need to consider that producers have to share part of this enhanced duty of care by designing, describing and marketing products in a way effectively enabling operators to comply with their duties; and by adequately monitoring the product after putting it into circulation.[88] This is because the more advanced technologies become, the more difficult it is for operators to develop the right skills and discharge all duties. While the risk of insufficient skills should still be borne by the operators, it would be unfair to leave producers entirely out of the equation.

D. *VICARIOUS LIABILITY*

One option proposed for addressing the risks of emerging digital technology is the potential expansion of the notion of vicarious liability, which could be applied to situations where autonomous technologies are used in place of human auxiliaries.[89] In other words, when harm is caused by an autonomous technology used in a way functionally equivalent to the employment of a human auxiliary, the operator's liability for making use of the technology should correspond to the existing vicarious liability regime of a principal for its own auxiliaries. This equivalent application encounters however two main issues. Firstly, vicarious liability regimes are modelled primarily on human behaviours, while in the case

85 Borghetti, *supra* note 76, at 100.
86 Report, *supra* note 22, at 44.
87 *See* Rolf H. Weber, *Liability in the Internet of Things*, 6 JOURNAL OF EUROPEAN CONSUMER AND MARKET. LAW 207 (2017).
88 Report, *supra* note 22, at 45.
89 *Id.* at 45–46.

of a technological auxiliary there is not a human behaviour to assess. Secondly, vicarious liability regimes are highly different across Member States and the recourse to them runs the risk to incremental increase in the degree of fragmentation. Now, the first obstacle may be overcome by deciding that when an autonomous technology outperforms a human auxiliary, the duty of care should be determined by the performance of a comparable available technology which the operator could be expected to use.[90] The fragmentation issue however cannot be overcome without intervening on the Member States' national regimes.

E. *LOGGING BY DESIGN, COMMERCIAL OR TECHNOLOGICAL UNITS*

Beside the adjustment so far mentioned, the Report introduces two main novelties that ought to be carefully considered as they are likely to significantly contribute to govern the issue of EDTs and liability in the near future. These amount to the requirement of logging by design[91] and to the notion of commercial or technological units.[92]

As to the former, EDTs offer unprecedented possibilities of reliable and detailed documentation of events that may enable the identification of what has caused an accident. This can usually be done using log files, which is why the expert group suggests to impose, under certain circumstances, a duty to provide for appropriate logging and to disclose the data to the victim in a readable format. The real innovation though is about the effects of a lack of compliance with the logging obligations, which would trigger a rebuttable presumption that the condition of liability to be proven by the missing information is fulfilled.[93] In other words, the absence of logged information—or the failure to give the victim reasonable access to it—would reverse the burden of proof and significantly ease the life of a claimant.

As to the latter—the notion of commercial or technological unit—it refers to the digital ecosystem that two or more persons cooperate to create on a contractual or similar basis. A commercial or technological unit is a notion that becomes very useful in complex contexts such as the Internet of the Things, where it becomes almost impossible for the claimant to identify a specific tortfeasor.[94] In such a case all the entities that are part of the unit—for example all the diverse producers or operators of the various devices that contribute to the creation of a smart house—are to be considered part of the same unit and—in the expert group's opinion—to be deemed jointly and severally liable.[95] The reason why such a notion ought to be adopted is that it would avoid the risk to undercompensate victims of damages derived from complex technologies as compared with those that are damaged by technologies that are manufactured or operated by just one clearly identifiable producer. In determining, finally, what counts as a commercial and technological unit the Report pinpoints several elements, among which a joint or coordinated marketing activity for the different

90 *Id.* at 46.
91 *See id.* at 47–49.
92 *See id.* at 55–57.
93 *Id.* at 48.
94 *See* Weber, *supra* note 87, at 207–212.
95 Report, *supra* note 22, at 56.

elements of the complex EDT at issue; the degree of their technical interdependency and interoperation; and lastly the degree of specificity or exclusivity of their combination.[96]

VI. COMPLEMENTING LIABILITY: SOFT LAW, ACCOUNTABILITY AND USERS' EMPOWERMENT, COMPENSATION FUNDS AND INSURANCE SCHEMES

The question of remedying damage deriving from the use of EDTs ignites the debate between those who would favor the free development of the market and those who invoke the expansion of the rules of liability, as well as between those who believe in the adequacy of the current legal framework and those who instead emphasize the need to introduce ad hoc instruments to keep up with technological advancements.[97]

In any case, any initiative focusing just on written rules, rather than aiming to affect the practices and incentives of industry participants would expose to the risk of stifling innovation or missing the goal of compensating victims.[98] It could be argued that the right balance between innovation and protection could hardly be found by industry participants alone, especially if left in an uncertain legal landscape as the current one, or, worse, in a regulatory vacuum. On the contrary, the right balance should be actively pursued by public regulators, following the adoption of a risk-based approach and on the basis of a continuous exchange of information with researchers and professionals,[99] on the assumption that EDTs are too diverse a category – in terms of purposes, capabilities, and so on—to allow a one-size-fits-all approach of dealing with related liability issues.[100]

Even after liability rules are amended according to the adjustments proposed in the previous sections so to properly tackle the ever-changing issues of the algorithmic society, the resulting liability framework would still offer remedies to the victims of wrongdoing *after* the damage occurs and a court rules in favor of the claimant. Instead, it would be sensible to complement such *ex post* mechanism with "soft" guidelines, codes of conduct, standards, best practices and human impact statements[101] aimed at guiding *ex ante* the conduct of designer, developers, owners and users of EDTs, to prevent damage from occurring at all. In other words, soft law could play a crucial role as an

96 *Id.*

97Marta Infantino, *La responsabilità per danni algoritmici: propsettive europeo-continentali*, 5 RESPONSABILITÀ CIVILE E PREVIDENZA 1762 (2019).

98 *Id.* at 1801.

99 Regulatory issues connected to AI, with a focus on the role of public and private actors, are analyzed in Michael Guihot, Anne F. Matthew, & Nicolas P. Suzor, *Nudging Robots: Innovative Solutions to Regulate Artificial Intelligence*, 20 VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW 385 (2017).

100 *See* Ioannis Revolidis, A & Alan Dahi, *The Peculiar Case of the Mushroom Picking Robot: Extra-contractual Liability*, *in Robotics*, in MARCELO CORRALES, MARK FENWICK & NIKOLAUS FORGÓ (EDS), ROBOTICS, AI AND THE FUTURE OF LAW, PERSPECTIVES IN LAW, BUSINESS AND INNOVATION 57 (Spring 2018).

101 With specific regard to AI, *see* Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 107–116 (2019), according to whom "in the absence of oversight, a mixture of industry self-regulation and whistleblower engagement offers us one path forward in the future direction of civil rights law to address the issues raised by AI," especially for issues of lack of transparency and bias. *Id.* at 140.

instrument of early regulation, rather than subsequent reaction.[102] Further advantages could stem from the fact that self-regulation is by definition developed by private actors—such as professional associations and committees of experts—who are far more knowledgeable with the technical complexities of EDTs than public regulators. Moreover, they could update soft law rules much faster than any public regulator—and this is critical to keeping up with the ever-evolving technological landscape.

Guidelines, standards, codes of conduct and best practices can become legally relevant by establishing the principle of accountability at the legislative level. The principle of accountability requires professionals and businesses to take responsibility for their initiatives and activities, by taking measures adequate to the level of risks and by being able to demonstrate compliance with law and best practices. In particular, borrowing the approach successfully adopted in data protection legislation,[103] subjects involved in the design, development and use of EDTs should conduct risks assessment analyses and, consequently, take appropriate action from an organizational and technical standpoint to foresee and prevent, or at least mitigate, any risk potentially incurred by any stakeholder because of EDTs.[104] Moreover, periodic review of impact assessment, combined with demonstrable governance processes, regular audits and contractually-binding instructions for business partners, could ensure a consistent level of compliance with law and soft law by all interested actors and stakeholders throughout the entire chain of EDTs. In this context, independent public authorities or private bodies could contribute with regard to standards, certification schemes, supervision and penalties.[105]

The issues raised by EDTs could also be tackled by empowering civil society—an empowerment that will not be caused by market forces spontaneously, but should be guided by scholars and activists[106] and could consists in providing users with greater awareness and tools for monitoring online markets for consumer policy purposes.[107] This assumption underlies, for instance, the CLAUDETTE project of the European University Institute in Florence, i.e., a machine learning powered system aimed at automatically detecting non-compliant privacy policies and potentially unlawful clauses in online terms of service.[108]

A further option could be to make mandatory for designers, developers, owners and users of EDTs to pay a tax, fee or contribution into a fund specifically established to ensure compensation for possible victims.[109] As

102 Infantino, *supra* note 97, at 1800.
103 GDPR, *supra* note 25, art. 5(2).
104 Comandè, *supra* note 37, at 184–185.
105 *Id.* at 187.
106 Hans W. Micklitz and Przemysław Pałka, *Algorithms in the Service of the Civil Society,* 1 J. OF EUROPEAN CONSUMER AND MARKET L. 1 (2019).
107 The European Commission financially supports initiatives in the area of consumer law, digital market surveillance and consumer law enforcement in digital markets in EU Member States; *see, e.g.*, *Exploratory Study: Exploring IT/AI tools for monitoring online markets for consumer policy purposes*, EUROPEAN COMMISSION (Dec. 12, 2018), JUST/2018/CONS/PR/CO01/0123, https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=639900.
108 *See* http://claudette.eui.eu.
109 Ryan Abbott, & Alex Sarch, *Punishing Artificial Intelligence: Legal Fiction Or Science Fiction*, 53 UC DAVIS L. REV. 323, 383 (2019).

suggested at the European level for drones[110] and AI,[111] the compensation fund should cover damage deriving from EDTs in relation to any inherent risk, in light of their characteristics and potential applications, as well as cases where an accident occurs and the responsible person is not identified or has failed to pay the due amount to the fund.

A similar (even complementary) path has been recommended also by the Expert Group on Liability and New Technologies of the European Commission,[112] as well as by the European Parliament with specific regard to robots: "establishing a compulsory insurance scheme where relevant and necessary for specific categories of robots whereby, similarly to what already happens with cars, producers, or owners of robots would be required to take out insurance cover for the damage potentially caused by their robots."[113] Such an option could be extended to EDTs more generally: for instance, for autonomous vehicles insurance could be a precondition for accessing the streets, and a "kill switch" could automatically disable the car in the event of missing insurance. After all, many legal systems already compel owners of vehicles to purchase third-party insurance covering damage caused to others while circulating. Depending on the circumstances, insurance coverage could be imposed to the owner alone or to a pool consisting of all parties involved in the production and distribution chain of EDTs, and the "insurance premium" would likely be built into the EDT sale price.[114] However, the introduction of a compulsory insurance scheme raises a number of issues: for instance, how to determine when an EDT is sophisticated enough to require coverage, to what extent to impose such an obligation on manufacturers—if completely absolved, they would no longer be incentivized to refine safety measures—or owners or users, how to address the case of damage not covered by mandatory insurance policies, and so on.[115]

Not even the latter solution would shield the industry from the need of reforming the current liability framework. On the contrary, liability insurers themselves support such a review in order to reduce current unpredictability of liability costs: ambiguity reduction and enhanced predictability would make it easier to set premiums for the insurance industry, which, as is well known, "embraces risk and abhors uncertainty".[116] In fact, the insurance market may simply not offer coverage for a certain risk, if missing experience makes it difficult to calculate it—and this could be a recurring problem with EDTs.[117] At

110 Andrea Bertolini, *Artificial Intelligence and civil law: liability rules for drones*, POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, EUROPEAN PARLIAMENT (November 2018), https://www.europarl.europa.eu/RegData/etudes/STUD/2018/608848/IPOL_STU(2018)608848_EN.pdf. *See id.* at 67.

111 Report, *supra* note 22, at 62.

112 *Id*. at 61.

113 European Parliament, *supra* note 50, art. 59(a). *See also* Andrea Bertolini, *Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rule*, 5 LAW, INNOVATION AND TECH. 214, 214–47 (2013).

114 Vladeck, *supra* note 44, at 124 n.27. *See also* Evas, *supra* note 51, at 26; Diana Cerini, *Dal decreto smart roads in avanti: ridisegnare responsabilità e soluzioni assicurative*, 4 DANNO E RESPONSABILITÀ 401 (2018).

115 M.O. Wagner, *You Can't Sue a Robot: Are Existing Tort Theories Ready for Artificial Intelligence?*, 1 THE J. OF ROBOTICS, ARTIFICIAL INTELLIGENCE & L. 231, 233 (2018).

116 Mark A. Geistfeld, *Legal Ambiguity, Liability Insurance, and Tort Reform*, 60 DEPAUL L. REV. 539, 540-41 (2011).

117 Report, *supra* note 22, at 61.

the same time, one should not forget those damages that can be compensated but not fully insured, given that monetary compensation alone would not be enough in relation to, for instance, the loss of a person's life or harm to irreplaceable environmental goods. In such cases, tort liability plays a crucial role as a policy instrument.[118]

All options mentioned in this work have limits to some extent, but this does not imply that they cannot serve a constructive role with respect to risk and liability distribution. Rather than looking for a one-size-fits-all solution, European law will have to assess and reinvent its strategy, as anchored in the checks and balances of the rule of law, without being harnessed in traditional legal theories—that can only point the way. To capitalize on the benefits of EDTs and prove up to the challenges raised by innovation, a multi-faceted approach should be pursued, whereby different regulatory and policy instruments are combined and continuously reviewed as EDTs evolve.

118 Joni Hersch & W. Kip Viscusi, *Assessing the Insurance Role of Tort Liability After Calabresi*, 77 LAW AND CONTEMP. PROB. 135, 162-63 (2014).