Artificial Intelligence and Damages: Assessing Liability and Calculating Damages

Benhamou, Yaniv; Ferland, Justine

How to cite

BENHAMOU, Yaniv, FERLAND, Justine. Artificial Intelligence and Damages: Assessing Liability and Calculating Damages. In: Leading Legal Disruption: Artificial Intelligence And A Toolkit For Lawyers And The Law. Giuseppina D'Agostino, Aviv Gaon, Carole Piovesan (Ed.). Montréal : Thomson Reuters - Yvon Blais, 2021. p. 165–197.

This publication URL: https://archive-ouverte.unige.ch/unige:152226

Artificial Intelligence and Damages: Assessing Liability and Calculating Damages

Yaniv Benhamou and Justine Ferland[*]

I. Introduction

Artificial intelligence (AI)[1] has undoubtedly brought along key societal benefits in the past years—one can notably think about fighting climate change with more accurate predictions and quicker responses to natural disasters, increases in patients' wellbeing and health outcomes with robot-assisted surgery and medical diagnosis assistance, and increased productivity and operational efficiency in the workplace with automated and optimized routine tasks. It may in many cases reduce the risk of injuries or damages in comparison to those arising when humans perform similar tasks. Yet, the widespread adoption of AI has also led to unwanted and sometimes serious consequences. We have already seen, amongst other issues, privacy violations, discrimination, and fatal accidents caused by the use of AI, and it is probably just a matter of time before other, wider-scale examples are added to this list.

Establishing liability for damages caused by AI can be rather straightforward when only one or few stakeholders are involved, or when the AI can only take a limited range of pre-defined decisions in accordance with specific parameters defined by a human programmer. However, AI usually involves several stakeholders and components (e.g., sensors and hardware, software and

[*] Yaniv Benhamou is attorney-at-law and Professor in digital law at the Faculty of Law of the University of Geneva. Justine Ferland is attorney-at-law and a PhD student. The authors sincerely thank Ms. Ana Andrijevic and Mr. Dino Vajzovic for their helpful comments.

[1] For a definition at the European level, see EC, European Commission, *White Paper on Artificial Intelligence - A European approach to excellence and trust* of 19 February 2020 (COM(2020) 65 final) [EC, *White Paper on AI*] at 16, suggesting a flexible definition ("the definition of AI will need to be sufficiently flexible to accommodate technical progress while being precise enough to provide the necessary legal certainty"), referring to the definition of the High Level Expert Group, A definition of AI, at 8 ("Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.").

applications, data itself and data services, connectivity features, etc.), which makes it difficult to allocate liability between all stakeholders. Moreover, recent forms of AI are increasingly able to learn without human supervision and make autonomous decisions, which poses tremendous challenges for addressing questions of AI-related liability. Indeed, no jurisdiction has granted legal personhood to AI or machines so far, meaning that an AI cannot be held personally liable for the damage it causes.[2] In this contribution, we will deal with AI systems falling along all points of the autonomy spectrum, ranging from passive agents responding to specific human instructions to complete autonomous entities having the capacity to learn, make decisions, and perform actions unrelated to their initial programming. Because no specific legal regimes currently define or regulate the operation of modern AI, courts dealing with these questions must attempt to solve liability issues by applying general laws often drafted years before the advent of this technology. We can therefore easily understand why AI-related liability has become one of the main areas of concern for many experts today, along with other issues such as software accessibility, accountability, and ethics.[3]

Much work remains to be done—not only via legal research but also on the policy, technical, and business sides—before we can satisfactorily answer all questions related to AI liability. The goal of this chapter is to give an oversight of the general principles that may guide legal practitioners and academics when reflecting on liability for damages caused by modern AI. We do not aim to provide a detailed analysis of the potentially applicable law in a specific jurisdiction, but rather to look at the question from a global and comparative law perspective. We will do so by first mapping various liability regimes (II.1) and identifying their challenges and shortcomings (II.2), before exploring lines of

---

[2] There have been many proposals for extending some kind of legal personality to emerging digital technologies, some even dating from the last century. See EC, European Commission, *Liability for Artificial Intelligence and other emerging digital technologies: Report from the Expert Group on Liability and New Technologies — New Technologies Formation* (Luxembourg: Office for Official Publications of the European Communities, 2019) at 37, n 98, DOI: < 10.2838/573689 > [EC, *Liability for AI*] and EC, *European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))*, [2017] P8-TA-2017-0051 [EC, *Resolution of 16 February 2017*]. However see *contra* EP, *European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence* (2020/2014(INL)), P9_TA-PROV(2020)0276 [EP, Resolution of 20 October 2020] at para. 7. For a discussion on whether current liability regimes can address AI-related challenges, see Yavar Bathaee, "The artificial intelligence black box and the failure of intent and causation" (2018) 2 Harv JL & Tech 889 at 891; Hannah R Sullivan & and Scott J Schweikart, "Are Current Tort Liability Doctrines Adequate for Addressing Injury Caused by AI?" (2019) 21:2 AMA J Ethics 160 at 160—66.

[3] There are great ongoing initiatives and reports at the European level. See EC, *Liability for AI*, *supra* note 2 at 12 (and references of preexisting works made thereto). See e.g. Allianz Global Corporate & Specialty, "The Rise of Artificial Intelligence: Future Outlook and Emerging Risks: Future Outlook and Emerging Risks" (March 2018), online (pdf): *Allianz Global Corporate & Specialty* < www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Artificial-Intelligence-Outlook-and-Risks.pdf >

thought to close the gaps through policy-driven (*lege ferenda*) solutions (II.3) and enhanced duties of care (*lege lata*) (II.4). Finally, we will map the damages caused by AI systems, ranging from injury to a person or physical property, and how to calculate them (III).

II. Assessing Liability

1. Potentially relevant existing liability regimes

By nature, AI is constantly developing and keeps surprising us with unexpected achievements. In this context, it is difficult to draft any kind of legislation specifically governing it, including to cover liability issues, as such legislation would need to be both universal and constantly amended in order to remain effective—an impossible task due to the static nature of legal institutions.[4] For this reason, it appears reasonable to start an analysis of AI liability by relying on existing general legal principles to both find elementary answers and identify their shortcomings. We may then assess how gaps could be closed.

Amongst the potential liability regimes that may be the most directly applicable in the context of AI-related tort claims are (a) general tort liability and (b) product liability. Because AI systems fall on a spectrum[5]—they may be anything between passive agents responding to specific human instructions and autonomous entities having the capacity to learn, make decisions and perform actions unrelated to their initial programming—these regimes may sometimes suffice to hold a natural or legal person liable for an AI's actions and ensure proper indemnification of its victim(s). In complex cases involving several stakeholders or more advanced "intelligent" AI, however, they may not be sufficient, as will be discussed in the next section.

It should be noted that we chose not to discuss vicarious liability—which imposes strict liability on one person (the principal) for the negligence or wrongdoing of another (the agent)[6]—under the current section. Indeed, even if

---

[4] Paulius Čerka, Jurgita Grigiene & Gintare Sirbikyte, "Liability for damages caused by artificial intelligence" (2015) 31:3 Computer L & Sec Rev 376 at 384. A regulatory approach that deals with the constant evolution of the technologies is to adopt legislations that follow the principle of *technological neutrality* (*i.e.* focusing on regulating the conduct of the various actors and not the technology itself). This principle of *technological neutrality* is very important to Switzerland for instance, recalled at recent legislative updates (e.g. see the revised Swiss Copyright Act, see Federal Council's Message of the Draft Bill of 22 November 2017, p. 19) and its Policy Strategy (e.g. see the Digital Foreign Policy Strategy 2021-2024, p. 9, considering this principle as a "*moderate approach which promotes and does not stifle the potential of new technologies, while at the same time counteracting specific risks*").

[5] See Omri Rachum-Twaig, "Whose Robot Is It Anyway?: Liability for Artificial-Intelligence-Based Robots" (2019) 2020 U Ill L Rev 1 at 8.

[6] Examples include liability of the employer for the acts or omissions of its employees that took

the AI system could perhaps be seen as having a sufficient degree of autonomy and intelligence to be treated under vicarious liability principles,[7] this type of liability requires that the agent (e.g., the AI) has legal personality which is currently not the case for AI in any jurisdiction.[8] Helpful parallels that could be pleaded to apply rules akin to those of vicarious liability principles to AI will, however, be discussed in the next section.

i. Tort Liability

Tort liability is the general liability regime applying to a civil wrong committed by one person against another person. Although there are differences between common law and civil law jurisdictions,[9] we may broadly summarize that tort law is based on fault and implies failure to take reasonable care to avoid causing injury or loss to another person. The plaintiff must prove a breach of duty of care (in common law jurisdictions)[10] or a wrongful action or a fault (in civil law jurisdictions).[11] Once the breach/faulty behaviour has been established, the plaintiff must also prove that it suffered a damage and establish a causal link between the fault and the damage, thus giving rise to compensation.

Tort law may sometimes be applied to hold a person liable for damages related to the use of AI. For instance, if a physician relies on an AI-powered clinical decision support software to prescribe medication but the software issues a flawed recommendation that would have been noticed and ignored by a reasonably competent physician, then the physician will likely be liable in tort for resulting and foreseeable injuries to the patient notwithstanding the AI's wrong recommendation.[12] However, as we shall see, the application of tort law principles faces significant challenges and shortcomings (see Section II.2, below).

---

place in the course of their employment and liability of the parent for the acts of their minor children. For legal sources, see e.g. Art 1463 CCQ.

7 See Emad Abdel Rahim Dahiyat, "From Science Fiction to Reality: How will the Law Adapt to Self-Driving Vehicles?" (2018) 7:9 J Arts & Human 34 at 39 [Dahiyat, "From Science Fiction to Reality"].

8 See Rachum-Twaig, *supra* note 5 at 11.

9 Common law jurisdictions often refer to negligence as the default tort liability rule, whereas civil law jurisdictions are based on the Roman concept of delict.

10 See e.g. *McAlister (Donoghue) v. Stevenson*, [1932] A.C. 562, [1932] All E.R. Rep. 1 (U.K. H.L.).

11 See e.g. Art 1382 CcF; Art 41 Civil Code (Swiss); Art 1457 CCQ.

12 Another upcoming question will be to know what is the liability of the physician (in the above example) who decides not to be assisted by an AI-system, although it has proven its effectiveness and has become the state of the art in the respective sector.

ii. Strict Liability

Strict liability means that a party can be held liable irrespective of fault, attached to specific risks linked to some object or activity which was deemed permissible, though at the expense of a residual risk of harm linked to it. Strict liability has been introduced in certain areas, such as transport (e.g., trains or motor vehicles), energy (e.g., nuclear power, power lines), or pipelines.[13] With AI and its inherent risks (e.g., when causing harms to life, health, physical integrity, and property), the European Union (EU) is currently considering the introduction of a strict liability regime, in particular for high-risk AI systems or in case of repeated incidents resulting in serious harm or damage.[14]

iii. Product Liability

Although the scope of concerned parties may vary depending on the jurisdiction, product liability generally targets, at the very least, manufacturers of finished products and manufacturers of raw parts or components included in a finished product. It may also apply to importers, designers, distributors, suppliers, and retailers of the product amongst others (we will generally refer to "manufacturers" in this article unless specific distinctions apply). Product liability may concern (1) manufacturing defects, (2) design defects,[15] and (3) failure to warn users against the product's inherent, nonobvious dangers.

In many jurisdictions including the European Union, product liability is a form of strict liability: if a defective product causes any physical damage to consumers or their property, the injured person shall be required to prove the damage, the defect, and the causal relationship between defect and damage. However, once this burden of proof is fulfilled, the manufacturer or producer has to provide compensation irrespective of whether there is negligence or fault on their part.[16] In the United States, product liability claims may be brought under three liability theories depending on the situation and jurisdiction: negligence, strict liability, or breach of warranty.[17]

---

[13] See EC, *Liability for AI*, at 25, and the references made thereof.

[14] See EP, *Resolution of 20 October 2020*, *supra* note 2, and the suggested article 4 of its proposed Regulation (Strict liability for high-risk AI-systems).

[15] Design defects are clearly covered by product liability law in some jurisdictions, such as the United States. See Rachum-Twaig, *supra* note 5 at 16. In the European Union, however, the EC, *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] OJ, L 210/29 [EC, *Product Liability Directive*] does not clearly cover design defects. In practice, courts limit the application of strict liability under this directive to manufacturing defects, while generally applying negligence principles to design and instruction defects. See Martin Ueffing, "Directive 85/374 — European Victory or a Defective Product Itself?" (2013) 4 Marble Research Papers 373 at 392.

[16] See EC, *Product Liability Directive, supra* note 15 arts 1, 4.

[17] See Margaret Horn & Kelly Dawson, "Product Liability: United States" in Simon Castley & Gregory L Fowler, eds, *Getting the Deal Through—Product Liability* (2019) s. 18—19.

Manufacturers can be cleared of liability under certain specific conditions that are unrelated to considerations of fault or negligence. It is generally admitted, for instance, that manufacturers may raise as a defense that the state of scientific or technical knowledge at the time the product was put into circulation could not allow them to detect the defect.[18] Manufacturers may also evade liability if they prove that no defect existed when the product left their hands.[19]

At first glance, product liability seems like an attractive regime to hold manufacturers of AI-powered products responsible for injuries caused by these products. For instance, when an autonomous vehicle is manufactured or designed in a flawed way that is inherently dangerous to those around it, or when a manufacturer fails to inform customers of the dangers associated with the vehicle, product liability principles may be applicable. However, just like with tort liability principles, we shall see that the application of product liability principles to modern AI faces significant challenges and shortcomings (see Section 2 below, specifically 2.v).

2. Challenges and shortcomings

As previously mentioned, AI systems fall on a spectrum. Whereas the aforementioned liability regimes may suggest appropriate answers in "simpler" cases of damages caused by AI, their application may be barred by insurmountable obstacles when dealing with cases implicating the most advanced forms of AI.[20] Amongst these obstacles are: (A) a high number of potentially involved stakeholders; (B) AI's autonomy; (C) lack of explainability; and (D) lack of foreseeability. Specific considerations also further complicate the application of product liability principles to an AI's actions (E).

i. High number of involved stakeholders

Emerging digital technologies, including AI, are becoming increasingly complex due to the interdependency between their different components such as: (i) the tangible parts/devices (sensors, actuators, hardware); (ii) the different software components and applications; (iii) the data itself; (iv) the data services (i.e., collection, processing, curation, analysis); and (v) the connectivity features.[21] The number of stakeholders involved in the creation and operation

---

[18] See e.g. Horn, *supra* note 17 s. 29 (in the US); EC, *Product Liability Directive, supra* note 15 art 7(d) (in the EU).

[19] See e.g. EC, *Product Liability Directive, supra* note 15 art 7(b) (in the EU).

[20] See e.g. Emad Abdel Rahim Dahiyat, "Intelligent agents and liability: is it a doctrinal problem or merely a problem of explanation?" (2010) 18:1 AI & L 103 at 107—08 [Dahiyat, "Intelligent agents and liability"].

[21] EC, *Liability for emerging digital technologies Accompanying the document: Communication from the Commission to the European Parliament, the European Council, the Council, the European*

of AI systems is concurrently rising; hardware manufacturers, software designers, sellers, equipment and software installers, facility owners, AI owners, AI users and trusted third parties, amongst others, may all have a role to play in ensuring that the AI does not cause harm, and allocating liability in this context is not an easy task.

Some legal regimes, such as product liability, may facilitate the allocation of liability by prescribing joint liability between some of these potential defendants; however, this is not the case for all liability regimes, and in any event, the current provisions on joint liability may not adequately cover all relevant stakeholders in an AI context.

It may also be especially unfair to assign blame under strict liability principles (such as product liability law) to a manufacturer or designer "whose work was far-removed in both time and geographic location from the completion and operation of the [original] AI system."[22] Similarly, if the AI is modified after its manufacturing or programming via open source software, for instance, then we can hardly conclude that the product sold initially caused the injury and rely on product liability principles.[23] Moreover, even in cases of strict liability, it is necessary to determine which of the commercial parties along the AI value chain can be held liable (if only for the jointly liable defendants to allocate liability between themselves in the context of a recursory action), which may prove impossible when conclusions are autonomously reached by AI.

In addition, digital technologies are continuously modified after their launch into the market via incorporation of new data, software updates, or patches applied either by the manufacturer of the AI system, manufacturers of individual system components, or even third parties. These new codes add or remove features in ways that change the risk profile of the "original" AI and affect the behaviour of the entire system or of individual components which can affect the safety of AI as a whole.[24] In this context, for all types of liability, and more specifically for tort liability, it has become increasingly difficult to pinpoint who is responsible when something goes wrong, it being specified that often there is a chain of contracts between stakeholders that specifies everyone's duties and liabilities (e.g., the software developers' general terms and conditions providing an obligation to update insecure software, which may

---

Economic and Social Committee and the Committee of the Regions, [2018] COM, SWD/2018/137 final.

22 Sullivan, *supra* note 2.

23 See Woodrow Barfield, "Liability for Autonomous and Artificially Intelligent Robots" (2018) 9:1 Paladyn J Behavioral Robotics 193 at 197. On the hand, mitigating the risk of causing harm could mean in our view for the manufacturer or programmer to prevent from the possibility of the AI-system to integrate open sources software, in order to ensure "safety by design".

24 *Ibid.*

lead to its liability in case of non-compliance).[25] Also, the performance of the AI may be well tested when it is launched, but there will be little or no scientific evidence of the AI's features at the time giving rise to damages.[26] The legal decision regarding a possible lack of diligence will have to be taken based on possibly outdated and incomplete information. Moreover, it may be useless to try to compare AI tools as conclusions reached for one AI tool (i.e., the one that is defective) will not be transposable to a second AI tool because the two—even when designed together—will have, over time, learned and evolved differently.[27]

ii. AI's increased autonomy

Today's AI is becoming increasingly autonomous in that, although initially programmed by a human counterpart, it can now process data, learn from it, and make independent decisions that can hardly, if at all, be linked to the initial design or programming.[28]

Notwithstanding which liability regime is considered, courts confronted with liability claims arising from an AI's actions must attempt to determine which legal or natural person is responsible for the damage caused by these actions. AI's increased autonomy makes a fundamental liability assessment difficult, if not impossible in some cases. Whereas the existing rules on liability cover cases where the cause of the AI system's act or omission can be traced back to a specific human agent (e.g., manufacturer, operator, owner, or user) and where that agent could have foreseen and avoided the AI system's harmful behaviour, in the scenario where the AI makes autonomous decisions, the traditional rules will not suffice to give rise to legal liability for damage caused by the AI system since they would not make it possible to identify the party that caused the damage.[29] Indeed, the more autonomous an AI system becomes, the

---

[25] For the duties of care of the stakeholders, including software developers, see 4.i (Enhanced duties of care).

[26] Valérie Junod, "Liability for damages caused by AI in medicine : progress needed" in Christine Chappuis & Bénédict Winiger, eds, *Journée de la responsabilité civile 2018* (Zürich: Schulthess, 2019) 119, referring to Ernst & Young (2018), with the support of Technopolis Group and VVA Consulting, European Commission, Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products, Final Report, January 2018, p. 85: *"[I]n the field of robotics, it could be difficult to distinguish between a defect which was present at the moment in which the robot was put into circulation from a defect that appeared after that moment, given the characteristics of self-learning systems*".

[27] Junod, *supra* note 26, referring to the judgment of the EU Court of Justice in C-503/13 of 5 March 2015.

[28] In particular in cases of unsupervised learning, such as AI relying on deep learning mechanisms, see below note 40.

[29] See EC, *Resolution of 16 February 2017*, *supra* note 2.
On this topic, see also Barfield, *supra* note 23; Mark A Chinen, "The co-evolution of autonomous machines and legal responsibility" (2016) 20:2 Va JL & Tech 338; George S Cole,

less control physical parties have over it, and the general liability principles founded on agency, control, and foreseeability collapse.[30]

Under tort law, assessing how and when entities such as manufacturers, operators, and/or users of AI may commit a breach of duty or a fault and establishing causation is not simple when an AI system with a high degree of autonomy is concerned. In cases where AI decisions are not directly related to one party but rather result from the AI's interpretation of reality, who is to blame and in which proportion? Even if a person can be seen as having played a role in causing damage (e.g., the programmer who instructed the AI to take a specific type of data into account), should its responsibility be proportional to the degree of autonomy of the concerned AI, and how may we properly evaluate this degree of autonomy?[31] When an AI reinforces itself without human input by learning from its own past experiences and making adjustments to improve efficiency, then acts on this new knowledge, is it even possible to speak of "fault" or "breach of duty" from any of the persons who may have been involved with the AI at some remote point in time?

AI's autonomy also poses problems under product liability law which is currently not designed to cover errors resulting from the autonomous AI thinking—a major flaw in the current legal approach to AI, according to some authors.[32] Indeed, in many cases, it will simply not be possible to draw the line between damages resulting from the AI's autonomous decisions and damages resulting from a product defect. Even if fault needs not be proven, the plaintiff has to demonstrate that the product was defective; this is not an easy task when AI-powered systems operate successfully without a mechanical defect, but still cause property damage or injuries due to their machine learning capabilities.[33] As previously mentioned, under most regimes, it will be possible for manufacturers and producers to escape liability if they can establish that, at the time the AI was put into circulation, they were not aware and could not have been aware of the risk which later materialized, i.e., that they could not have known that the AI was dangerous or defective when it left their hands.

However, because AI develops and reinforces itself with machine learning and adjusts on its own to become more "intelligent" without human intervention, it might simply not be the same AI at a later point in time than it was when it left the manufacturer's hands,[34] thus leaving the victim uncompensated almost every

---

"Tort liability for artificial intelligence and expert systems" (1990) 10:2 John Marshall J Inf Tech & Privacy L 127.

30 See Sullivan, *supra* note 2.

31 See Giangiacomo Olivi, Claudio Orlando Miele & Valeria Schiavo, "Robots and Liability: who is to blame?", *Dentons* (20 December 2018).

32 See Barfield, *supra* note 23 at 196; Čerka, s*upra* note 4 at 386.

33 See Barfield, *supra* note 23 at 196.

34 Junod, *supra* note 26 at 123.

time. Therefore, the fact that the operator is exercising control over an AI system may be a determining factor regarding liability; AI systems that self-develop autonomously may trigger the liability of their manufacturers and producers who left the door open for unexpected results and accepted the associated potential risks, instead of designing a secure AI system with a limited capacity to produce unexpected results. Therefore, policymakers are considering applying different rules depending on the risk, including a strict liability regime for those high-risk autonomous AI systems.[35]

In any event, applying product liability principles to the most autonomous forms of AI has been said to be unfair and commercially unreasonable towards manufacturers as it would equate to holding them liable for actions over which they have absolutely no control and thus potentially stifle innovation. Indeed, in cases where AI is meant to replace human decision making, applying product liability law in cases of "defective" decisions would imply that manufacturers are liable in almost every case (due to strict liability), yet humans making those same mistakes could plead the absence of fault or negligence under general tort law principles. For instance, a manufacturer could be held strictly liable if an AI-powered medical device fails to detect a specific condition, yet a physician would benefit from the more lenient tort liability regime in the same situation and could escape liability by proving that he did not act negligently. Moreover, too large a burden on manufacturers could lead them to shield their identities or stop the progress of technological development in official markets, opting to move to unofficial ones.[36]

iii. Lack of explainability (the "black box" phenomenon)

The operation of AI is based on the achievement of goals.[37] AI's designers do not program all the possible scenarios in advance nor give specific instructions for each of them; rather, they set a goal for the machine and let the AI process the data input, learn from it, and decide the best course of action to reach its goal. This leads to the scenario where the AI's programmers may not have an exact understanding of how it reached such a goal or what the stages leading to success were;[38] in other words, they cannot explain the AI's "thought process" leading to the final result. The same is true for an AI's failures, which cannot always be explained or understood by humans. For instance, algorithms in precision medicine process patient and hospital data to predict patient risk

---

[35] See EP, *Resolution of 20 October 2020*, *supra* note 2, considering that "*an AI-system that entails an inherent high-risk risk and acts autonomously potentially endangers the general public to a much higher degree, [so that] it seems reasonable to set up a common strict liability regime for those high-risk autonomous AI-systems*."

[36] Čerka, *supra* note 4 at 386.

[37] See Čerka, *supra* note 4 at 383; Rachum-Twaig, *supra* note 5 at 7; Barfield, *supra* note 23 at 193.

[38] See Rachum-Twaig, *supra* note 5 at 7—8.

and formulate diagnoses, but it is not always possible to identify which data elements were processed, the weight that was given to each element in the global assessment, and whether there was unethical bias in the processing.[39] Even in cases wherein the algorithm itself is rather simple, the data fed into the algorithm may be so diverse and ever changing (in the case of autonomous vehicles, one may think about inputs from cameras, sensors, lasers, microphones, etc.) that it is often impossible to reproduce the environment in which the injury happened and identify its source.

This so-called "black box" nature of AI creates challenges of interpretability and eventually affects causation and allocation of liability for all aforementioned liability regimes. Indeed, identifying the cause of an AI system's failure to perform is the key element for establishing a fault/breach of duty of care and a causal link in tort claims, or a link between defect and damage in product liability claims. In the context of judicial proceedings, if a plaintiff cannot trace the chain of data processing and recreate the circumstances of the AI's reasoning process to understand what led to a specific (faulty) output, its action may very well be doomed as he will not be able to fulfill the basic evidentiary requirements regarding fault and/or causation.[40]

Some authors have argued that in order to mak AI more explainable and remedial, its designers should be legally required to disclose algorithms' codes and implement a way to record all aspects of their functioning.[41] Similarly, the European Commission has recently suggested, while assessing its existing product safety legislation, that developers of algorithms should be obliged to disclose the design parameters and metadata of datasets in case accidents occur.[42] This would allow one to reconstruct and understand the causes of its behaviour to facilitate liability assessments. However, this suggestion is not always possible with modern AI and also raises important issues with regard to intellectual property, trade secrets, and competition law.[43]

---

39 See Barfield, *supra* note 23 at 195.

40 See Junod, *supra* note 26 at 124; Chris Temple, "AI-Driven Decision-Making May Expose Organizations to Significant Liability Risk", *Corporate Compliance Insights* (11 September 2019). See also Dahiyat, *supra* note 7 at 38.

41 See Shane O'Sullivan et al, "Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery", *The International Journal of Medical Robotics and Computer Assisted Surgery* 15:1 (05 November 2018) at 7, DOI: < doi.org/10.1002/rcs.1968 > .

42 European Commission, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, Brussels, 19 February 2020, COM(2020) 64 final at 9 [EC, *Report of 19 February 2020*].

43 See O'Sullivan, *supra* note 41 at 5; Junod, *supra* note 26 at 124, n 30 (citing other sources).

iv. Lack of predictability or foreseeability

The more advanced an AI is, the less predictable or foreseeable it becomes. This is because many forms of modern AI function based on unsupervised learning (as opposed to supervised learning). In cases of supervised learning, the AI's designers (and potentially users, if they participate in the process) have considerable control over the results of an operation as they provide the basis for the AI's decisions; they can therefore foresee, at least up to a certain point, how the AI will react to new data (e.g., with intelligent telephones who can identify someone in a photo). However, in cases of unsupervised learning (such as an AI relying on deep learning mechanisms),[44] the algorithms are only given input data without corresponding output values, and are left free to function "as they please." The inherent lack of predictability or foreseeability in these processes challenges the liability principle that a defendant will only be found liable if it could reasonably anticipate and prevent the potential results of an action.[45]

Indeed, when trying to apply tort law principles to an AI's actions, unforeseeability may cause problems in evaluating both the fault/breach of duty of care aspect as well as causation.[46] On the side of fault, because an AI's actions are unpredictable, it is difficult for a person operating or interacting with it to anticipate: (a) the probability that it will eventually inflict harm on others; (b) the optimal precautions that should be put in place by its programmers or operators; (c) the safety measures that should be taken by potential victims engaging with it; and (d) all the potentially new and unpredictable types of harms that may be inflicted by it.[47] In this context, we may hardly expect human stakeholders to be able to take preventive measures to avoid harm caused by AI. Similarly, when an AI acts in an unexpected way after having learned from its own experiences, it will be difficult to conclude a fault or breach of duty on the part of manufacturers or programmers if they can demonstrate that: (a) the AI was properly developed and tested before release; (b) their employees and auxiliaries were well trained and supervised; and (c) they implemented proper quality control mechanisms.[48] Even in cases in which we can identify a fault from a human stakeholder interacting with an AI

---

[44] See Eduardo Magrani, "New perspectives on ethics and the laws of artificial intelligence", *Internet Policy Review*, 8:9 (2019).

[45] See Rachum-Twaig, *supra* note 5 at 13 (citing various references in common law); Barfield, *supra* note 23 at 199; Dahiyat, "Intelligent agents and liability", *supra* note 20 at 113.

[46] See Andrew D Selbst, "Negligence and AI's Human Users" (2019) BUL Rev at 26 [forthcoming in 2020]; Rachum-Twaig, *supra* note 5 at 15. See also Barfield, *supra* note 23 at 193, citing Andreas Matthias, "The responsibility gap: ascribing responsibility for the actions of learning automata" (2004) 6:4 Ethics & Inf Tech 175.

[47] See Rachum-Twaig, *supra* note 5 at 23, 27; Barfield, *supra* note 23 at 194, 200.

[48] See Junod, *supra* note 26 at 130.

system, the lack of foreseeability will, in many cases, break the link of causation between this person's fault and the injured victim.[49]

AI's lack of foreseeability poses similar problems under product liability principles. In many jurisdictions, the law specifically states that manufacturers are only liable for defects or inadequate instructions when there was a foreseeable risk of harm posed by the product.[50] Once again, because many AI-related risks are unforeseeable by nature, they simply cannot be covered by the product/design defect or duty of warning and instruction doctrines.[51]

v. Special considerations regarding product liability law

Finally, one specific challenge is worth noting when attempting to apply product liability law principles to an AI's actions: the fact that modern AI may simply not be covered by these principles at all as it may not be a "product." Indeed, although the term "product" may be interpreted broadly, product liability generally only concerns tangible movables (such as hardware), not services;[52] and key modern technologies such as software and algorithms are most often considered services, not products.

Moreover, in AI's complex environment characterized by an interdependency among different components, "products" and "services" are increasingly intertwined, and it can be difficult to identify whether a failure is due to either one of those components. In some cases, damage may be caused by a simple hardware (product) defect, but it may also stem (amongst other examples) from

---

[49] See Rachum-Twaig, *supra* note 5 at 23.

[50] See e.g. *United States Restatement (Third) Of Torts: Product Liability* §2(b) (1998) [*Restatement*] (which states that the manufacturer is liable for design defects "when the foreseeable risk of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission, of the alternative design renders the product not reasonably safe" as well as for its "inadequate instructions or warnings when the foreseeable risks of harm posed by the product could have been reduced or avoided by the provision of reasonable instructions or warnings by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the instructions or warnings renders the product not reasonably safe". A similar rule exists under EC, *Product Liability Directive, supra* note 15, art 7(b) and under the *Swiss Product Liability Act* (RS 221.112.944), art 5(b), amongst others, establishing the "development risk" defense that manufacturers are likely to raise in cases of AI's unforeseeable actions. Under this defense, producers can escape liability if they can establish that, at the time the AI was put into circulation, they were not aware and could not have been aware of the risk which materialized.

[51] See Rachum-Twaig, *supra* note 5 at 19; Junod, *supra* note 26 at 128, and 135, suggesting to remove from the (Swiss) Product Liability Act the risk exception (i.e. providing that the manufacturer is not liable if he/she can prove that the state of knowledge could not foresee such a defect at the time of putting the product on the market), so that the product liability may also apply to unforeseeable harm.

[52] The European Union Commission is currently exploring whether the definition should also cover software embedded in (or downloaded on to) a physical product but has not implemented concrete changes in the law so far.

miscommunication between the physical infrastructure and the AI's "brain," from incorrect data analysis, or from corrupted third-party data being fed into the AI algorithm. In these contexts, doctrinal opinions vary as to whether AI software should be qualified as a product[53] or service.[54] Should AI, or a relevant part thereof, be considered a service, plaintiffs may be barred from relying on product liability law and rather need to resort to the general negligence/delict-based tort liability principles by proving the fault or negligence of the defendant entities. In addition, when AI is personalized or unique (for instance, handcrafted for a single client by a research laboratory), it might not be considered a product, as it is not generic.[55] It should, however, be noted that this distinction might evolve over time,[56] as it is currently being criticized by many authors who hold that it is ill-defined and outdated.[57]

Lines of thought to develop solutions and to close these gaps of distinction between products and services, as well as to clarify the point in time at which a product is placed into circulation, will be addressed below (II.3.iv).

3. Policy-driven solutions (*lege ferenda* solutions)

The shortcomings and challenges discussed above illustrate that notwithstanding the concerned jurisdiction, current liability regimes are ill-adapted to adequately allow the indemnification of an AI's potential victims. Yet, setting clear, ex-ante liability rules pertaining to AI would have multiple advantages, including: (i) dissuading actors from engaging in risky activities, thus preventing and reducing accidents while promoting safety standards; (ii) facilitating the correct pricing of AI products or services as companies may better appreciate risks; (iii) encouraging innovation investment by mitigating uncertainty over the litigation process; and (iv) enhancing consumer trust, thus encouraging the uptake and use of AI systems in various fields.[58]

Although more academic and political discussion and development is required before concrete solutions can be implemented, this section aims to present a few creative propositions which may inspire policymakers dealing with questions of AI liability. It is, however, by no means exhaustive, especially

---

[53] See Marguerite E Gerstner, "Comment: Liability Issues with Artificial Intelligence Software" (1993) 33:1 Santa Clara L Rev 239 at 255; Junod, *supra* note 26 at 126, citing Kerstin Noëlle Vokinger, "Artificial Intelligence and Machine Learning in der Medizin", *Jusletter* (28 August 2017.

[54] See Cole, *supra* note 29.

[55] See Barfield, *supra* note 23 at 197.

[56] *Ibid.*

[57] See notably Junod, *supra* note 26 at 126, citing Jessica Allain, "From Jeopardy! To Jaundice: The Medical Liability Implications of Dr. Watson and Other Artificial Intelligence Systems" (2013) 73:4 La L Rev 1049 at 1067.

[58] Tatjana Evas, *Civil liability regime for artificial intelligence, European added value assessment*, study, European Parliamentary Research Service, September 2020 at 5.

with regard to policy-driven solutions where multiple other avenues have been evoked in the past years.[59]

i. Granting legal personality to AI

One way to circumvent the pitfalls currently associated with AI is to find a way to hold it directly liable for its actions instead of looking for a faulty human behind it. By reviewing the existing legal framework, lawmakers could decide to ascribe legal personhood to modern AI, thus giving it rights and a corresponding set of duties. The idea itself is not shocking and may possibly be implemented without requiring too many legal reforms since the law already grants legal personality to other non-natural persons such as corporations or rivers, and AI likely fits (if not exceeds, in comparison to corporations) the requisite criteria to benefit from a similar status.[60] In fact, the European Commission considered this pathway in 2017 and suggested studying the implications of "creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personhood to cases where robots make autonomous decisions or otherwise interact with third parties independently."[61]

---

[59] To give a few examples, the following solutions have notably been put forward: (1) the creation of regulatory rules regarding coding and design of robots and autonomous products (Rachum-Twaig, *supra* note 5 at 32 (citing others)); (2) establishing a system where the AI would need to be licensed (John Kingston, "Artificial Intelligence and Legal Liability" (Paper delivered at the International Conference on Innovative Techniques and Applications of Artificial Intelligence, November 2016), DOI: < 10.1007/978-3-319-47175-4_20 > (citing others); Junod, *supra* note 26 at 136 (for medical products)); (3) developing a system where AI developers and manufacturers would agree to adhere to certain ethical guidelines to govern AI, providing a framework that courts could use to resolve legal claims where AI is implicated (Allianz Global Corporate & Specialty, *supra* note 3); (4) establishing a regulatory authority dedicated to regulating and governing the development of AI (Matthew U Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies" (2016) 29:2 Harv JL & Tech 353 at 393—97); (5) creating a compensation fund to guarantee compensation if damage caused by AI is not covered by insurance, thus "allowing the manufacturer, the programmer, the owner or the user to benefit from limited liability if they contribute to a compensation fund, as well as if they jointly take out insurance to guarantee compensation where damage is caused by a robot" (EC, *Resolution of 16 February 2017*, *supra* note 1 at para. 59(c); EC, *Liability for AI, supra* note 2 at 62).

[60] Shawn Bayern, "The Implication of Modern Business-Entity Law for the Regulation of Autonomous Systems" (2015) 19 Stan Tech L Rev 93; Shawn Bayern et al, "Company Law and Autonomous Systems: A Blueprint for Lawyers, Entrepreneurs, and Regulators" (2017) 9 Hastings Sci & Tech LJ 135; Paulius Čerka, Jurgita Grigiene & Gintare Sirbikyte, "Is it possible to grant legal personality to artificial intelligence software systems?" (2017) 33:5 Computer L & Sec Rev 685.

[61] See EC, *Resolution of 16 February 2017*, *supra* note 2 at para. 59(f). However, see *contra* EP, *Resolution of 20 October 2020*, *supra* note 2, at para. 7: "all physical or virtual activities, devices or processes that are driven by AI-systems may technically be the direct or indirect cause of harm or damage, yet are nearly always the result of someone building, deploying or interfering with the

Key questions, however, remain to be settled before concretizing this idea. Contrary to corporations, AI would not necessarily have a patrimony of its own and would thus not be able to indemnify its potential victims even if it is found liable. This could, however, be circumvented if some form of compulsory insurance scheme for human stakeholders involved with AI (either designers, manufacturers, service providers, and/or end users) or a compensation fund was to be established. In-depth analyses and reflections would also be required to cover the other consequences of granting legal personality to AI, such as the implications concerning its potential criminal responsibility.

This suggested solution is also criticized by many. Following the European Parliament's proposal, more than 250 experts from various AI-related fields signed an open letter in 2018 calling on the European Commission to reject it as it would be—in their opinion—inappropriate, ideological, nonsensical, and non-pragmatic.[62] Some have held that, contrary to what is the case with corporations, it will not always be possible to identify a natural person behind the (legal person) AI who may in all cases be ultimately responsible, thus leaving liability voids in some cases.[63] Moreover, even if AI was to have legal personality, problems of unexplainability and unforeseeability would remain;[64] it would not be straightforward to establish that the AI should have been able to avoid the mistakes it made, nor to understand its "thought process" and the specific steps that led it to make a particular decision.

ii. Creating a new form of strict liability for operators of high-risk technologies

Strict liability regimes could be the most appropriate way to ensure compensation, in particular for operators of technology that exposes third parties to an increased risk of harm, such as AI-driven robots in public spaces (non-private environments). Such strict liability regimes could eventually be combined with a compulsory liability insurance scheme. This solution is currently suggested in the European Union, where the parliament has recommended drafting a new regulation setting up a common strict liability regime for operators of "high-risk autonomous AI-systems."[65]

---

systems; [the Parliament] notes in this respect that it is not necessary to give legal personality to AI systems." See also *contra*, EC, *Liability for AI, supra* note 2 at 37.

62 See "Open Letter to the European Commission Artificial Intelligence and Robotics" (2018), online: *Robotics: OpenLetter.Eu* < www.robotics-openletter.eu/ > ["Open Letter"].

63 See O'Sullivan, *supra* note 41 at 7; EC, *Opinion of the European Economic and Social Committee on 'Artificial intelligence — The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society'*, [2017] OJ, C 288/01 at para. 3.33, [EC, *Opinion 2017*]; "Open Letter", *supra* note 62.

64 See Dahiyat, "Intelligent agents and liability", *supra* note 20 at 107—12.

65 See EC, *Report of 19 February 2020*, *supra* note 2 at 16; EP, *Resolution of 20 October 2020*, *supra* note 2, considering "reasonable to set up a common strict liability regime for [...] high-risk autonomous AI-systems and underlining] that such a risk-based approach, that might encompass

Assessing AI liability under strict liability theories may require legislative changes, but could also potentially be done through case law to reach faster results, at least in some circumstances and/or jurisdictions if courts were to follow creative legal arguments and render innovative decisions. Amongst the suggested sources of inspiration are the following liability theories:[66]

- **Liability for greater sources of danger or ultra-hazardous activities.** Some jurisdictions have established a strict liability regime holding those who create or handle particularly dangerous items or perform abnormally dangerous activities to be held liable for the damage caused by such items or activities, even if they took every reasonable step to prevent this damage.[67] Some authors hold that "since AI is able to draw individual conclusions from the gathered, structured, and generalized information as well as to respond accordingly, it should be accepted that its activities are hazardous."[68] Because AI's activities are inherently risky and the risk may not always be prevented by safety precautions, an AI system may meet the requirements for being considered a greater source of danger,[69] which would imply that either its developer or manager should be required to assume strict liability for its actions and potentially be required to take out compulsory insurance to cover its civil liability.[70] This would be especially true when an AI is performing a function in which mistakes may be directly life threatening (e.g., administering medicine to a patient).[71]

---

several levels of risk, should be based on clear criteria and an appropriate definition of high risk" and recommending that all high-risk AI-systems shall be exhaustively listed in an Annex to its proposed Regulation on liability for the operation of AI-systems. For a start in the definition and categorization of "high-risk AI-systems", see EC, *White Paper on AI*, p. 17, *supra* note 1. It should be noted that the European solution only establishes strict liability for "high-risk AI-systems", whereas other types of AI still remain subject to general, fault-based liability rules. See also EC, *Liability for AI, supra* note 2 at paras 39, 41 (which defines "operator" (and abandoning the traditional concepts of owner owner/user/keeper) as the person who is in control of the risk connected with the operation of emerging digital technologies and who benefits from such operation. "Control" is a variable concept, ranging from merely activating the technology, to determining the output or result (such as entering the destination of a vehicle or defining the next tasks of a robot), and may include further steps in between, which affect the details of the operation from start to stop). For a discussion on compulsory insurance schemes, see section 3d below.

66 For a detailed analysis of various strict liability provisions found in the national laws of European countries, see Evas, *supra* note 58 at 13-33.

67 See e.g. *Restatement*, *supra* note 50, § 20 (2009) (in the United States); *Rylands v. Fletcher*, [1868] UKHL 1 (U.K. H.L.) (in the United Kingdom); Čerka, *supra* note 4 at 386 (examples of ultra-hazardous activities include the use or storage of explosives, disposing of nuclear wastes and activities involving radioactive materials); Evas, *supra* note 58 at 14-22 (analysis of how various European jurisdictions have introduced strict liability for dangerous "things" and "activities").

68 See Čerka, *supra* note 4 at 386.

69 *Ibid. Contra* Rachum-Twaig, *supra* note 5 at 21 (who argues that this theory likely does not apply to AI).

70 See Čerka, *supra* note 4 at 386.

71 See Kingston, *supra* note 59.

- **Liability for animals.** Although liability for the acts of animals is generally based on fault or negligence by their owners or keepers, it can also be strict in some jurisdictions and circumstances.[72] In the United Kingdom, for instance, the *Animals Act 1971* provides that the keeper of a dangerous animal (e.g., its owner who is in its possession, a head of household, or a keeper) is strictly liable for any harm which may have been caused by that animal, notwithstanding whether or not he was at fault.[73] Under another United Kingdom law—the *Dangerous Wild Animals Act 1976*—keepers of dangerous wild animals are required to take out insurance policies against liability for damage caused to third parties and to be licensed by the local authority.[74] Some authors, as well as the European Commission, have linked the unpredictability of AI systems to that of animals, "where liability is typically attributed to those responsible for supervising the animal because they are in the best position to adopt measures to mitigate the risk of damages";[75] we could therefore imagine creating a strict liability regime akin to what exists for dangerous animals in the United Kingdom for users or supervisors of AI systems.
- **Common enterprise liability.** One author argues that a new strict liability regime for AI could be established based on the common enterprise liability doctrine, under which each entity within a set of interrelated companies may be held liable jointly and severally for the actions of other entities that are part of the group, allowing the injured party to obtain redress without having to assign every aspect of the general wrongdoing to one party or another.[76] Under this liability scheme, persons working towards a common aim, such as the manufacturers, programmers, and designers of an AI and its various components, would jointly share the responsibility of indemnifying the plaintiff for the AI's wrongdoings and no finding of fault would be required. The defendant(s), having indemnified the plaintiff in such a suit, would have the opportunity to file a recursory action to obtain reimbursement from other potential defendants. In order for this solution to be implemented, however, courts would need to depart from some of the traditional criteria of common enterprise liability; indeed, they usually apply this doctrine when the liable entities have

---

[72] For an analysis of how various European jurisdictions have incorporated principles of strict liability for damages caused by animals, see Evas, *supra* note 58 at 22-26.

[73] (UK), c 22.

[74] (UK), c 38.

[75] See J Scott Marcus, "Liability: When Things Go Wrong in an Increasingly Interconnected and Autonomous World: A European View", *IEEE Internet of Things Magazine* (December 2018) 4; see also Evas, *supra* note 58 at 32. However, some authors disagree about the possibility of making such a parallel. *Contra* Čerka, *supra* note 4 at 386.

[76] See David C Vladeck, "Machines Without Principals: Liability Rules and Artificial Intelligence" (2014) 89:1 Wash L Rev 117. See also Čerka, *supra* note 4 at 386; Sullivan, *supra* note 2.

some sort of organizational relationship, which may not always be the case with AI.[77]

These solutions are appealing in that they allow one to circumvent issues of AI autonomy, unexplainability, and unforeseeability discussed above; lawmakers and courts should, however, remain careful before implementing them as they may also have a "chilling effect" on the manufacturing, design, and use of future AI-based products. As previously mentioned, holding human stakeholders responsible for acts performed by AI beyond their control—with no regard as to whether or not they exercised an appropriate level of care—may be placing too high of a burden on their shoulders and may lead to less innovation and/or use of AI in the future.

iii. Applying vicarious liability principles for operators of autonomous technologies

Vicarious liability regimes—holding a principal liable for the action of its agent—could be the most appropriate way to ensure compensation, particularly for autonomous technologies.[78] This proposal is based on the way AI's actions are interpreted in the field of contracts, where strict liability rules apply to a machine's actions and bind the person on whose behalf it acts, regardless of whether these actions were planned or envisaged, and "complies with the general rule that the principal of a tool is responsible for the results obtained by the use of that tool since the tool has no independent volition of its own."[79] This is consequent with many decisions rendered by courts around the world wherein the actions of automated technologies have been attributed to the person using them and have considered the user liable even when he was unaware of the operations of his automated machines.[80] By considering AI as a

---

[77] Under the common enterprise doctrine, courts may find that a common enterprise exists if, for example, businesses (1) maintain officers and employees in common, (2) operate under common control, (3) share offices, (4) commingle funds, and (5) share advertising and marketing. See *FTC v. Washington Data Resources*, 856 F.Supp.2d 1247 (M.D. Fla., 2012) at 1271.

[78] See EC, *Liability for AI, supra* note 2 at 45; Čerka, *supra* note 4 at 384—385, citing Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts,* Law, Governance and Technology Series, vol 10 (Netherlands: Springer, 2013) at 98. For an analysis of how various European jurisdictions apply vicarious liability principles, see Evas, *supra* note 58 at 26-31.

[79] *Ibid.* The authors notably evoke article 12 of the United Nations Convention on the Use of Electronic Communications in International Contracts, under which a person (whether a natural person or a legal entity) on whose behalf a computer was programmed should ultimately be responsible for any message generated by the machine. See also UN, *Explanatory note by the UNCITRAL secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts*, sales no E07V2 (New York: UN, 2007) at 70 para. 213; Dahiyat, "Intelligent agents and liability", *supra* note 20 (also gives the example of the "Guide to Enactment" accompanying the UNCITRAL Model Law, which provides that "the Data messages that are generated automatically by computers without human intervention should be regarded as "originating" from the legal entity on behalf on which the computer is operated").

[80] Dahiyat, "From Science Fiction to Reality", *supra* note 7 at 37.

tool, we could therefore hold persons on whose behalf it acts or at whose disposal and supervision it is (which could be either users or owners of the AI) liable for its actions.[81] Such users or owners could not evade liability towards a plaintiff by claiming that they did not instruct the AI to act like it did; however, they would have the opportunity to claim damages against the manufacturer or designer of the AI under product liability rules when possible (e.g., if they can prove that the AI was defective, that such a defect existed while the AI was under the manufacturer's or designer's control, and that the defect caused the damages suffered by the plaintiff).[82]

Other authors are, however, wary of this solution. Indeed, according to some, even if we were to hold that AI can be assimilated to an agent or tool allowing the application of vicarious liability to its actions, its autonomy creates challenges that remain difficult to overcome. An agency relationship implies some form of control by the principal over the agent,[83] which becomes tenuous as AI's autonomy increases,[84] making it difficult to conceptualize truly intelligent machines as mere agents or tools of humans. In other words, "a machine that can define its own path, make its own decisions, and set its own priorities may become something other than an agent. Exactly what that may be, though, is not a question that the law is prepared to answer."[85] Moreover, due to the ever-changing nature of AI, identification of a specific liable principal could prove difficult, as different stakeholders could be considered the (agent) AI's principals at different points in time and/or in different contexts.[86]

iv. Extending product liability to producers of emerging technologies (including services)

The product liability of producers should apply to emerging technologies, regardless of whether they are incorporated into hardware. The distinction between products and services makes less and less sense with respect to IT tools. Since the risks and benefits are the same, whether or not the product is

---

81 Čerka, *supra* note 4 at 384—385.

82 *Ibid.*

83 See e.g. *Restatement*, *supra* note 50, §7.03—07 (2006) (stating that a principal is subject to vicarious liability for an agent's actions only when the agent is acting within the scope of employment, which is not the case when the employee's act occurs within an independent course of conduct not intended by the employee to serve any purpose of the employer).

84 See Dahiyat, "Intelligent agents and liability", *supra* note 20 at 106.

85 See Vladeck, *supra* note 76 at 145, citing Pagallo, *supra* note 78. See also Rachum-Twaig, *supra* note 5 at 12 (who holds that "[i]n some cases, no human being could be considered the principal behind the AI-robot acts").

86 See Rachum-Twaig, *supra* note 5 at 12 (who states e.g. that "when a corporation (whether designing the product or distributing it) is actually operating it, we may think of the robot as being operated on behalf of such corporation. In other cases, a user may be considered as a principal with respect to a machine that it operates, while the designer of such robot would likely not be considered a principal in this context").

physically incorporated, the legal regime should be the same.[87] Damage caused by defective digital content should trigger the producer's liability because digital content fulfils many of the functions tangible movable items used to fulfil when product liability schemes were drafted and implemented.[88]

The point in time at which a product is placed on the market should not set a strict limit on the producer's liability for defects when, after that point in time, the defect is a result of the producer's interference or failure to interfere with the product already put into circulation (for example, by way of a software update that is required to maintain the expected level of safety within the time period for which the producer is obliged to provide such updates).[89] Finally, due to the lack of explainability and predictability explained above, there shall be no development risk exception (which allows the producer to avoid liability for unforeseeable defects, such as the one set out in the EU Product Liability Directive), at least in cases where it was predictable that unforeseen developments might occur.[90]

v. Compulsory insurance schemes

Insurance shifts risks from potentially liable persons to insurance carriers who will defend and indemnify their insureds for losses and pay for settlements or judgments to resolve third-party claims. Insurance can be fault-based (a system based on tort liability, in which each insurance company pays for the damages sustained by a victim according to the degree of fault of their policyholder) or no-fault (where each individual insurance company compensates—generally up to a certain threshold—its policyholder for injuries without regard as to who is

---

87 See Junod, *supra* note 26; EC, *Liability for AI, supra* note 2; EC, *Report of 19 February 2020*, *supra* note 2 at 13; EP, *Resolution of 20 October 2020*, *supra* note 2 at para. 8.

88 See EC, *Liability for AI, supra* note 2 at 43 ("[t]his is all the more true for defective digital elements of other products, some of which come separately from the tangible item (for example, as a control app to be downloaded onto the user's smartphone), or as over-the-air updates after the product has been put into circulation (security updates for example), or as digital services provided on a continuous basis during the time the product is being used (for example, navigation cloud services").

89 See EC, *Liability for AI, supra* note 2 at 43, referring to (i) the Directive (EU) 2019/771 on the sale of goods that recently confirmed 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 (ii) the Directive (EU) 2019/770 that establishes a similar regime for digital content and digital services.

90 See EC, *Liability for AI, supra* note 2 at 43 (which also discusses the difficulty for the average user to prove facts such as the expected level of safety and the capacity for the producer to prove such relevant facts (asymmetry) and justifies consequently the reversal of the burden of proof and an alleviation of evidentiary burden with regard to the causal relationship between a defect and the damage. If we fully support this type of mechanisms (reversal or alleviation of burden of proof), they shall apply in our view to other liability regimes as well, as the discussed justification (asymmetry of available information between the average consumer and the producer) is relevant for the other liability regimes as well).

responsible).[91] One area in which compulsory insurance (either fault-based or no-fault) applies, and which may be a source of inspiration, is with regard to vehicles.

Establishing a compulsory fault-based insurance scheme regarding AI could allow a victim to be easily indemnified in most cases,[92] but the issues discussed above would subsequently remain for insurers attempting to allocate liability between their respective policyholders. As for the adoption of a no-fault compulsory insurance scheme in the field of AI, this could be, according to some authors[93] and policymakers,[94] an interesting solution that would allow one to circumvent the challenges discussed above. In fact, the United Kingdom—which has a fault-based insurance regime in place for regular vehicles—has enacted the *Automated and Electric Vehicles Act 2018*, under which an insurer is liable for damage where an accident is wholly or partly caused by an automated vehicle "driving itself" that is insured at the time of the accident,[95] notwithstanding any reference to a specific person's liability (driver, manufacturer, etc.). It has thus established a form of no-fault—although not yet compulsory[96]—insurance regime for automatic (AI-powered) vehicles.

Some authors, however, raise concerns regarding this solution, notably regarding the "lack of deterrence" effect caused by no-fault insurance regimes on humans' and/or AI's behaviour at large, the difficulty to impose such a system on all stakeholders involved with AI, and the fact that it might be extremely challenging to determine insurance premiums in this context.[97] In every case, this solution may unsatisfactorily cover the foreseeability issues discussed above since insurers could potentially attempt to exclude unforeseeable damages from their coverage. Moreover, although mandatory insurance is an interesting option for AI-powered items in sector-specific fields where regular (non-AI) products are already insured, such as the field of vehicles, it may not be appropriate or feasible when dealing with products that do not normally require insurance, at least not in the near future. Indeed, for a compulsory insurance scheme to work, insurers notably need sufficient data to assess the expected frequency and size of claims, sufficient similarity in the risks being covered,

---

91 For an analysis of the cyberinsurance schemes in Swiss and comparative law with several references to the doctrine, jurisprudence and cyberinsurance policies, see Jacques de Werra / Yaniv Benhamou, "Cyberassurance : instrument utile pour la cybersécurité des entreprises ?" (2020), Jusletter 24 August 2020.

92 The European Parliament recommends mandatory insurance for operators of high-risk AI systems, see EP, *Resolution of 20 October 2020*, *supra* note 2 at para. 23-25.

93 See notably Jin Yoshikawa, "Sharing the Costs of Artificial Intelligence: Universal No-Fault Social Insurance for Personal Injuries" (2019) 21:4 Vanderbilt J Ent & Tech Law 1155; Junod, *supra* note 26 at 135.

94 See notably EC, *Resolution of 16 February 2017, supra* note 2 at paras 57—59.

95 See *Automated and Electric Vehicles Act 2018* (UK), c 18, art 2(1).

96 *Ibid* art 2(2) (indeed, article 2(2) of the Act also provides that where an accident is wholly or partly caused by an automated vehicle which is driving itself at the time *but is not insured*, the registered owner is liable for the loss and damage).

97 See Rachum-Twaig, *supra* note 5 at 29—32.

sufficient insurance/reinsurance capacity, and adequate competition, which is currently not the case for AI-powered items in general (outside of any sector-specific items).[98]

4. Developing the current fault liability regime (*legal lata* solutions)

Instead of considering new liability principles (solutions that require certain amendments to the current liability regimes), one may consider simply adapting current fault-based liability regimes with enhanced duties of care and precisions regarding shared liability and solidarity between tortfeasors, which could potentially be done through case law in most jurisdictions.

i. Enhanced duties of care

Adapting current fault-based liability regimes may be contemplated, simply by enhancing the negligence principles with supplementary rules that will set a predetermined acceptable level of care, applicable to producers and operators of emerging technologies.[99] This fault liability can apply exclusively or cumulatively with other strict liability regimes. In other words, these enhanced duties of care are without prejudice to any other liability regimes that may apply or be developed (e.g., enhanced product liability or vicarious liability regimes).

This solution is based on the premise that stakeholders involved with AI are better situated to implement supplementary rules and intervene to prevent or mitigate potential harms. Those who fail to meet this level of care—whether a manufacturer, designer, programmer, operator or end-user[100]—would be exposed to liability under a presumption of negligence. On the other hand, meeting the level of care would trigger the application of the basic negligence rule and plaintiffs would have to prove actual negligence, forming a quasi-safe harbor for the concerned stakeholder.[101] This solution would allow one to circumvent one of the important shortcomings of the product liability regime—e.g., its applicability to products only—as well as the unique problems related to modern AI, such as foreseeability and agency.

Amongst the contemplated obligations that could lead to this quasi-safe harbor are:

- With respect to operators, they should have to comply with an adapted range of duties of care relating to: (a) the choice of technology,

---

98 See "Insight briefing - Compulsory insurance : when it works and when it doesn't" (8 November 2017); "Autonomous Vehicles Handing Over Control: Opportunities and Risks for Insurance" (25 April 2014), at 8.

99 See EC, *Liability for AI, supra* note 2 at 44; Rachum-Twaig, *supra* note 5 at 32.

100 Rachum-Twaig, *supra* note 5 at 36—38.

101 *Ibid* at 33.

particularly in light of the tasks to be performed and the operator's own skills and abilities; (b) the organizational framework provided, in particular with regard to proper monitoring; and (c) maintenance, including any safety checks and repair. Failure to comply with such duties may trigger fault liability regardless of whether the operator may also be strictly liable for the risk created by the technology.[102] The European Union is currently considering formally imposing such enhanced duties of care on the operator in a recent regulation proposal.[103]

- With respect to producers, while the risk of insufficient skills should still be borne by operators, it would be unfair to leave producers entirely out of the equation. Rather, producers—whether or not they incidentally also act as operators within the meaning of the definition—should also have to: (a) design, describe, and market products in a way that effectively enables operators to comply with the operator's duties; and (b) adequately monitor the product after putting it into circulation—taken in light of the characteristics of emerging digital technologies, and, in particular, their openness and dependency on the general digital environment, including the emergence of new malware. This (superior) monitoring duty could be fulfilled by supervising and studying an AI system even after its release.[104] This could be achieved by implementing anomaly-based monitoring systems programmed to give a warning when an AI behaves in an unexpected manner as well as by upstream observation of the tendencies of the AI to predict such behaviours.[105] Once such monitoring is implemented, a duty to inform potential victims of the AI would follow.[106] When feasible, producers should be required to include mandatory backdoors ("emergency brakes" by design), shut-down capabilities, or features allowing operators or users to shut down the AI or make it "unintelligent" at the press of a button. Not doing so would be considered a design defect under the product liability doctrine. Depending on the circumstances, manufacturers or operators could also be required to shut down the AI themselves as part of their monitoring duties.[107]

---

[102] See EP, *Resolution of 20 October 2020*, *supra* note 2, Annex B, para. 18 ff. and art. 8(2) for examples of situations in which it could be presumed that the operator of an AI-system has observed the due care that can reasonably be expected from him. See also EC, *Liability for AI, supra* note 2 at 44 (giving the following illustration, "Despite adverse weather conditions due to a heavy storm, which were entirely foreseeable, retailer (R) continues to employ drones to deliver goods to customers. One of the drones is hit by a strong wind, falls to the ground and severely injures a passerby. R may not only be strictly liable for the risks inherent in operating drones, but also for its failure to interrupt the use of such drones during the storm").

[103] EP, *Resolution of 20 October 2020*, supra note 2.

[104] See Junod, *supra* note 26 at 136.

[105] See Rachum-Twaig, *supra* note 5 at 33.

[106] *Ibid* at 34.

Similar to the already-existing post-sale duties of warning and instruction, as well as the duty to recall defective products, producers could also have support and patching duties.[108] This suggested duty is consistent with other recent developments regarding software developers' potential obligation to update insecure software; indeed, although no law clearly contains an explicit obligation to do so yet, some courts have started to interpret existing legal norms in a way that creates such an obligation.[109]

- The liability of producers and operators could be reduced when end-users do not meet their own duties of care with regard to AI, for instance, if they do not install available safety updates on software, which could be regarded as contributory negligence.[110]
- The burden of proof concerning causation and fault could also be reversed when the potentially liable party has failed to log the data relevant for assessing liability or is not willing to share such data with the victim.[111]

ii. Solidarity rules between tortfeasors

With AI, the number of stakeholders, the interconnectedness of emerging digital technologies, and their increased dependency on external input and data make it increasingly doubtful whether the damage at stake was triggered by a single original cause or by the interplay of multiple (actual or potential) causes.[112] Even if something is proven to have triggered the harm (for example, because an autonomous car collided with a tree), the real reason for it is not always equally evident.

Tort law regimes handle these cases of multiple potential sources of harm quite differently. When it remains unclear which one of several possible causes was the decisive influence to trigger the harm, the classic response by existing tort laws in such cases of alternative causation is that, either all parties are jointly and severally liable (which is undesirable for those who did not in fact

---

[107] *Ibid* at 35. See EC, *Report of 19 February 2020*, *supra* note 2 at 3: "For instance, during the recall of one of its devices in 2017, a smartphone producer carried out a software update to reduce to zero the battery capacity of the recalled phones, so that users would stop using the dangerous devices."

[108] *Ibid.*

[109] See e.g. Pieter Wolters' analysis of the Dutch Consumentenbond v Samsung decision in his recent article. Pieter TJ Wolters, "The obligation to update insecure software in the light of Consumentenbond/Samsung" (2019) 35:3 Computer L & Sec Report 295 at 295—305. According to this decision, software developers would have a general duty of care to update (e.g. make their product conform) and to provide security updates to consumers that bought their product from an intermediary. This duty of conformity could be extended to extracontractual obligations; such an obligation could also perhaps exist under a general duty of care in some jurisdictions. Failure for software developers to do so could be seen as negligence or a fault.

[110] EC, *Report of 19 February 2020*, *supra* note 2 at 15; EP, *Resolution of 20 October 2020*, *supra* note 2, Annex B, art. 10.

[111] EC, *Report of 19 February 2020*, *supra* note 2 at 16; EC, *Liability for AI, supra* note 2 at 47

[112] See EC, *Liability for AI, supra* note 2 at 22.

cause harm), or none are liable (since the victim fails to prove causation of one cause—again, undesirable for the victim).[113] The problem of who really caused the harm in question will therefore often not be solved in the first round of litigation initiated by the victim, but on a recourse level, if ever.

To remediate the cases of alternative causation, the following solutions should be contemplated:

- **With respect to the victim**, when more than one person is liable for the same damage and where it remains unclear which one of several possible causes was the decisive influence to trigger the harm, there shall be joint liability of all tortfeasors, i.e., the victim may request payment of the full sum or part of the sum from any of the multiple tortfeasors at the victim's discretion, but the total sum requested may not exceed the full sum due. In any case, there shall be joint liability when tortfeasors act with knowledge of the other tortfeasors' wrongful conduct (*wrongful cooperation*).[114]
- **With respect to the recursory action**, each tortfeasor should be liable only for its individual share of responsibility for the damage when only part of the damage can be attributed to one or more tortfeasors (*identified shares*) unless some of them form a commercial and/or technological unit, in which case the members of this unit should be jointly and severally liable for their cumulative share to the tortfeasor seeking redress.[115] Such a unit rule may apply when the parties have a joint or coordinated marketing for their respective elements (commercial unit) or when their elements present a technical interdependency and interoperation (technical unit). When no individual shares can be identified between tortfeasors, each potential tortfeasor shall be liable to a quota corresponding to the likelihood that each of them in fact caused the harm in question (proportional liability).[116]

This solution is also in the interest of efficiency, as parties are incentivized to make contractual arrangements for tort claims in advance.[117]

---

[113] *Ibid*, quoting Bénédict Winiger et al, eds, *Digest of European Tort Law: Volume 1: Essential Cases on Natural Causation* (Vienna: Springer, 2007) at 387ff.

[114] Under Swiss law, see Vincent Perritaz, "La solidarité: un monde imparfait" (Revue Responsabilité et assurance REAS / HAVE 2018), at 63 ss: in the first case, the terms "perfect solidarity" (*solidarité parfaite*) within the meaning of CO 50 are used and, in the second case, the terms "imperfect solidarity" (*solidarité imparfaite*) within the meaning of CO 51 are used.

[115] See EC, *Liability for AI, supra* note 2 at 23 (giving the following illustration, "[t]he producer of hardware has a contract with a software provider and another one with the provider of several cloud services, all of which have caused the damage, and all of which collaborate on a contractual basis. Where another tortfeasor has paid compensation to the victim and seeks redress, the three parties may be seen as a commercial unit, and the paying tortfeasor should be able to request payment of the whole cumulative share from any of the three parties").

[116] See Israel Gilead, Michael D Green & Bernhard A Koch, eds, *Proportional Liability: Analytical and Comparative Perspectives* (Berlin: De Gruyter, 2013).

III. Calculating the Damages

1. General Considerations

The main purpose of tort law is to indemnify victims for losses they should not have to bear themselves entirely on the basis of an assessment of all the interests involved. Traditionally, such indemnification is governed by the compensation principle (according to which only the actual harm must be compensated).[118] With AI, there may be several types of harms ranging from injury to a person or a physical property (e.g., a self-driving car crashing into a pedestrian or a house), damage resulting from the infringement of an intellectual property right or a privacy rule, to pure economic loss (e.g., costs associated to repair damage to data).

However, only compensable harm, meaning damage to a limited range of interests that a legal system deems worthy of protection, will be indemnified.[119] While there is unanimous accord that injuries to a person or physical property, and damage resulting from the infringement of an absolute right, are compensable harms, this is not universally accepted for pure economic loss (i.e., losses that are not directly linked to physical injury or property damage, including damage to data, such as alteration or suppression of data).[120] Pure economic loss may nevertheless be compensated via contractual liability (e.g., an insurance contract extending the coverage to these losses). Policymakers, cyber insurers, and courts also tend to recognize a damage to data.[121]

---

[117] See EC, *Liability for AI, supra* note 2 at 23.

[118] See Yaniv Benhamou, "Compensation of Prejudice for Infringements of Intellectual Property Rights in France, under the Directive 2004/48/EC and Its Transposition Law: New Notions?" (2009) Intl Rev IP & Competition L 126. For high level considerations relating to damages and AI, see EP, *Resolution of 20 October 2020*, *supra* note 2.

[119] Some scholars consider that any type of harm caused by AI should be compensated for; otherwise users and consumers will be left without proper compensation for their injuries. See Vladeck, *supra* note 76 at 128. Others authors consider that an injury must be compensated for only if the injurer has a correlative duty to refrain from inflicting the harm to begin with (corrective justice approach) or only if it is efficient to do so under a cost-benefit analysis (e.g. in order to internalize negative externalities or in order to deter wrongdoers from doing wrong in the first place) (economic analysis approach). See Guido Calabresi & A Douglas Melamed, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral" (1972) 85 Harv L Rev 1089.

[120] Damage caused by self-learning algorithms on financial markets, for example, will therefore often remain uncompensated, because some legal systems do not provide tort law protection of such interests at all or only if additional requirements are fulfilled, such as a contractual relationship between the parties or the violation of some specific rule of conduct. In the European Union, since pure economic loss and damage to personal data or privacy is not explicitly covered by the *Product Liability Directive*, some Member States allow for their recovery but others do not; see Evas, *supra* note 58 at 12.

[121] For an analysis of the cyberinsurance schemes and their contractual shortcomings in Swiss and comparative law, see Jacques de Werra / Yaniv Benhamou, *supra* note 91.

While compensation for physical property damage or bodily injuries do not raise specific issues, and compensation for pure economic losses is rather a matter for policymakers (whether or not recognizing a damage to data per se) or for contractual liability (whether or not the insurance or service contract covers such losses), damage resulting from the infringement of an absolute right, in particular, deserves more analysis, as their intangible nature makes the damage less quantifiable.

2. Intellectual Property Right Infringements

Tort liability applies where the relevant data is protected by intellectual property law or a similar regime, such as database protection or trade secret protection (collectively referred to as "IPR") and is used in connection with an AI (e.g., as input to feed an AI).[122] However, the quantification of damages is delicate.

The quantification of damages varies between jurisdictions, but damages are mostly of two kinds: actual damage, which is defined as the claimant's loss incurred or lost profits,[123] and unfair profits, which refer to the profits unduly made by the infringer with the infringement of the right. Actual damage or unfair profits may be relevant when the concerned data forms the predominant part of an AI (e.g., when a software is used for analytic purposes or a whole database for feeding the AI). However, actual damage may be difficult to claim when the claimant is a small or medium-sized enterprise (SME) without capacities to commercialize the data, as it will fail to prove that there was a decline in, or a non-increase of, its turnover (actual damage) and that, in the absence of IPR infringement, it would have sold his products instead of the infringer (lost profits). Unfair profits may also be delicate when the relevant data forms part of a complex multifaceted device, which shall be the rule (e.g., when several interconnected elements compose a particular process or environment, such as in the Internet of Things context) as only the profits attributable to the infringement shall be recordable and reduced accordingly if there are other factors causing that profit (such as non-infringing components incorporated into a multifaceted device).[124] Another difficulty is when the relevant data is not recognizable in the output (e.g., because the input is used simultaneously with

---

[122] For a recent analysis of the legal regimes that apply to inputs, analytics and outputs from a comparative law perspective, see Yaniv Benhamou, "Big Data and the Law: a holistic analysis based on a three-step approach. Mapping property-like rights, their exceptions and licensing practices" (2020), Revue suisse de droit des affaires et du marché financier 4/2020, at 392 and seq.

[123] International Association for the Protection of Intellectual Property Resolution, "2017 — Study Question (General): Quantification of monetary relief" (2017) at 1.

[124] For a discussion regarding the delicate calculation of unfair profits with references to case-law and doctrine (notably the American case Apple-Samsung), see Yaniv Benhamou, "Damages, profits, statutory and punitive damages" in *ALAI Enforcement of Intellectual Property Rights*, (Montreal: Themis, 2020) s. 100.

thousands of other inputs to generate a single output),[125] or not even expressed in the output (e.g., because the input is used for training purposes only),[126] as most jurisdictions consider that there is an act of reproduction no matter whether the input exists or is recognizable in the output.[127]

In these cases (multifaceted device, or no input used or recognizable in the output), when the claimant cannot claim unfair profits due to a delicate causation test, or actual damage due to a lack of his own capacities, the claimant may rely on a royalty fee provided by legislation and/or granted by case law as a minimum standard in lieu of actual damage (i.e., without the proof of a lost royalty fee).[128] The reasonable royalty is assessed on a case-by-case basis, usually with reference to comparables (i.e., previous licensing agreements, tariffs, or recommendations of the respective sectors) or to a hypothetical negotiation (i.e., based on what "*reasonable parties*" would have agreed to based on all the circumstances and with full knowledge of the relevant facts).[129] The principles set out in the patent-related US decision *Georgia-Pacific Corp v United States Plywood Corp*[130] might be relevant to the determination of the amount of the hypothetical license fee, and is often also quoted by case law outside the US. Consequently, the claimant may claim damages up to the amount he would have claimed as a royalty fee in a contract with the tortfeasor for the use of the relevant data. No matter whether the data is existent or recognizable in the output, and whether the claimant may be able

---

[125] Think of the Edmond de Balamy portrait, 1st painting based on 15,000 portraits, sold at an auction house for $432,000 USD, Google Dream trained on open access images. Edmond de Balamy, "The shadows of the demons of complexity awaken by my family are haunting to me" (2020) online: < obvious-art.com/edmond-de-belamy.html > .

[126] Think of the making a copy of a student's papers for the purposes of detecting plagiarism.

[127] This is linked to the broad interpretation of the reproduction right, which covers identical, partial, direct or indirect reproduction by any means, in whole or in part. Reproduction right covers the "*exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part*" (EC, *Copyright Directive 2001/29/CE CJUE Infopaq,* [2001] OJ, C-5/08 s. 51).

[128] For EU-Law, see EC, *Directive 2004/48 of 29 April 2004 on the enforcement of intellectual property rights,* [2004] OJ, 2004/48 art 13 ("Enforcement-Directive") ("*as an alternative to [lost profit and unfair profits, Courts] may, in appropriate cases, set the damages as a lump sum on the basis of elements such as at least the amount of royalties or fees which would have been due if the infringer had requested authorisation to use the intellectual property right in question*"). For national transpositions into German and French law and several case-law granting a reasonable royalty-fee, see Yaniv Benhamou, *Dommages-intérêts suite à une violation de droit de la propriété intellectuelle*, (Berne, Switzerland: 2012) , at 37. For American Law and several case-law granting a reasonable royalty-fee, *ibid* s. 87.

[129] See Reto M Jenny, *Die Eingriffskondiktion bei Immaterialgüterrechtsverletzungen: unter Berücksichtigung der Ansprüche aus unerlaubter Handlung und unechter Gesch.ftsführung ohne Auftrag* (Zurich: Schulthess, 2005) at 317 (depending on the concrete needs of the parties, the reasonable royalty can be a lump-sum, a per-unit royalty, a percentage of revenues or, or a combination of the aforementioned).

[130] *Georgia-Pacific Corp. v. United States Plywood Corp*., 446 F.2d 295, 170 U.S.P.Q. 369 (2d Cir., 1971), which established that the licensor's established policy and marketing program to maintain its monopoly by not licensing others to use his invention.

to prove actual damages or unfair profits, he may be able to receive this amount as a minimum indemnification. The share to which the royalty fee applies shall be the identified share for each tortfeasor (unless there is a commercial and/or technological unit) or, when no individual shares can be identified, to the quota corresponding to the likelihood that each of them in fact caused the harm in question (*proportional liability*).

3. Privacy Violations

Tort liability also applies when the relevant data is personal information protected by the rules of privacy. A separate sum of money may be claimed in the event of injury to personality rights (e.g., infringement of moral rights of the copyright owner) in which its seriousness may justify an additional separate sum of money. Depending on the nature of the data, a claimant could be entitled to additional damages determined either at trial or set statutorily in certain jurisdictions.

In the authors' view, the above calculation methods shall apply equally for personal data breaches, at least when data is tradable in a similar fashion as IPR. Indeed, personal data has become tradable as users commonly consent to make their personal data available in exchange for other services. In a standard business model for the internet, that data is used by the online platforms (e.g., social networks, search engines, content streaming services, etc.) to offer targeted advertising for other products or services. Although data protection authorities are reluctant to consider personal data as a simple commodity, and given the difficulties of valuating data, the new framework for data protection has somewhat validated the idea that personal data is part of the market exchange and "*contractual practice treats data like property rights.*" Consequently, every time personal data is used without authorization, the subject of the data should be able to claim for damages in the form of a royalty, if not unfair profits, based on the whole end product. From the outset, however, it must be recalled that not all unauthorized use of an IPR may lead to damages. In particular, courts tend to conclude that there are no damages in case of works subject to *open access*,[131] specifically *open licenses*,[132] as the copyright owner intended to distribute his work freely. Similarly, not all unauthorized use of personal data may lead to damages. This will depend on

[131] Open access is understood here as the possibility to view the work, which may be either fully unrestricted (in particular covering the right to reproduce, share, and disseminate the digitized work) or restricted (in particular permits users to view but not to reproduce, share, and disseminate the digitized work).

[132] Open licenses are understood here as standardized licenses (whether partly restricted or not), such as those proposed by certain organizations, such as Creative Commons for literary and artistic works by creativecommons.org, or General Public Licenses (GPL) for software by the Free Software Foundation.

the relevant market (i.e., whether the relevant marketplace draws benefits in exchanging the personal data).

4. Economic Methods and "Flat-rating" Damages

Given the difficulties in calculating damages and taking into account the specificities of IPR or privacy rights,[133] additional economic methods may be considered to calculate the damages in general, such as the *Discounted Cash Flow Method* (DCF), the *Financial Indicative Running Royalty Model* (FIRRM), and the *Royalty Rate Method* (for reasonable royalty calculations).[134] Case law about Fair, Reasonable and Non-Discriminatory (FRAND) license terms for disputes about the licensing of Standard Essential Patents (SEP) may also be relevant to set reasonable royalties. If courts are still reluctant to rely on economic methods, it is because plaintiffs do not bring this type of evidence and because courts are not all familiar with these economic methods. We further believe that each method gives a useful index value for the courts (a sort of benchmark for calculating damages) and that the solution consists of a combination of these methods. Finally, this path is in line with the increasing complexity of IP infringements (e.g., software incorporated into multi-component products, or infringements of online content without visible loss or lost profits).

As an outcome, there will certainly be a "flat-rating" of damages ("*barémisation*" or "*forfaitisation*"). Economists have just started talking about the value of personal data; similarly, regulators have started fining personal data breaches (e.g., with the General Data Protection Regulation). Consequently, IP lawyers and courts will be asked to calculate the related damages bearing in mind that breaches usually do not show any quantifiable loss. These economic methods and flat-rating losses will certainly be an answer. Personal data is a valuable asset,[135] but the actual value of any given personal data or dataset is context-dependent; their value varies, in particular, according to (a) the category of personal data (e.g., basic usage data—such as age, gender, ethnicity, and zip-code—have been estimated at $0.005 USD per record; data regarding credit history, criminal records, bankruptcies, or convictions have been estimated at $40 USD per record) and (b) the business models from the stock value of a firm or profit per record (e.g., usage-based pricing, package pricing, flat pricing, and freemium; the value per record of a big data broker is about $1 USD per record).[136]

---

[133] See Yaniv Benhamou, supra note 128, at 5 (for specificities of IP rights in general), at 7 (for repercussions on the quantum of damages).

[134] For an in-depth analysis of the calculation of damages based on these economic methods, *ibid* s. 286. For the DCF method, see Benoît Chappuis, "Quelques dommages dits irréparables: Réflexions sur la théorie de la différence et la notion de patrimoine" (October 2010) ss 165, 269.

[135] See Rodrigo Zapata, "How much is data worth?" (2018), online: DOI: 10.13140/RG.2.2.16113.74085.

[136] It seems to be extremely valuable in the hands of sophisticated data processors, such as Facebook,

Without claiming to be exhaustive, and as a very simple path for the future, the following chart may be contemplated to help lawyers and courts when pricing data and flat-rating damages:

Criteria	**Description**	**Estimated price**
Category of personal	**Demographic** (e.g., name, gender, age, address, nationality, income level, occupation, or biometric markers, such as face, voice, or DNA) **Geographic** (e.g., IP address, current location, or visited locations) **Behavioural** (e.g., sites browsed, interactions with other websites, purchases, content consumed, or devices used) **Psychographic** (e.g., preferences, values, beliefs, motivations, or lifestyle)	
Business models	**Usage-Based Pricing** **Package Pricing** **Flat Pricing and Freemium**	
Total		

IV. Conclusion

Existing liability regimes already offer basic protection to victims, to the extent that specific characteristics of emerging technologies such as AI are taken into account. Consequently, instead of considering new liability principles (solutions that may very well work but require certain amendments to the current liability regimes), one should consider simply adapting current fault-based liability regimes with enhanced duties of care and precisions regarding shared liability and solidarity between tortfeasors, which could potentially be done through case law in most jurisdictions.

When it comes to the calculation of damages, given the difficulties in calculations, and taking into account the specificities of IPR or privacy rights, economic methods may be considered to quantify the damages in general, such as the *Discounted Cash Flow Method* (DCF) and the *Financial Indicative Running*

---

which online marketing consumer targeting services represents 97% of its revenue. In 2018, the average revenue per user was Worldwide 5,97$, US & Canada 25,91$ and Europe 8,76$. See Zapata, *supra* note 135.

Royalty Model (FIRRM). To set reasonable royalties, the *Royalty Rate Method* as well as case law about Fair, Reasonable and Non-Discriminatory (FRAND) license terms for disputes about the licensing of Standard Essential Patents (SEP) may also be relevant. This path will lead to a certain "flat-rating" of damages ("*barémisation*" or "*forfaitisation*"), at least when IPR and personal data are illegally used by AI tools and mostly not visible, hence barely quantifiable in terms of damages.