Civil Liability Regime for Artificial Intelligence:  
A Critical Analysis of European Parliament’s Proposal for a Regulation**

Ş. Barış Özçelik *

Introduction

One of the prominent issues in the law globally, in parallel with the developments in artificial intelligence (AI), is the question of who will be liable for the harm or damage caused by AI and under which conditions. The prominence of this topic is founded upon, on the one hand, the idea of the “non-deprivation of the persons that suffer damages of compensation” that is considered to be the traditional rationale of tort law, and the concern of “not impeding innovation (promoting innovation)” on the other. It is clear that judicial systems that better balance these two concerns will significantly contribute to the welfare of their societies. In fact, a study conducted for the European Union (EU) predicts that by 2030, the determination of an explicit common civil liability regime concerning AI can create an added value of EUR 54.8 billion and this figure can reach EUR 498.3 billion considering the indirect effects.

In the face of these predictions, the topic has naturally acquired an important place in the agenda of the EU. In this context, resolutions have been adopted and reports have been prepared by appointed experts within the EU on various occasions. Finally, on 20 October 2020, the European Parliament adopted a resolution titled “Civil Liability Regime for Artificial Intelligence” (hereinafter referred to as the “Resolution”), to which a Proposal for a Regulation (hereinafter referred to as the “Proposal”) attached. The Proposal deserves special attention since it is the first concrete legislative attempt at the EU level to regulate liability for AI which appears to be produced by considering the relevant literature, previous reports and resolutions.

This paper aims to analyze and assess the most significant issues in the above-mentioned Proposal, i.e. rejection of the electronic personhood approach (I), inclusion of immaterial harm (II), operator’s liability (III), classification of AI systems as “high-risk and others” (IV) and the ambiguity regarding decision supporting AI systems (V).

I. Rejection of the Electronic Personhood Approach

The first salient point in the Proposal is the rejection of the so-called “electronic personhood” approach, which is suggested as a response to liability issues related to AI systems. In the Resolution, recognition of the legal personality of AI systems is not found necessary for the time being because of the fact that in nearly all instances, the harm and damage that is directly or indirectly caused by AI systems can be attributable to a person who builds, uses or is somewhat related to the system.

As is known, the electronic personhood approach has been one of the most striking suggestions in the EP Resolution on “Civil Law Rules On Robotics” of 16 February 2017, regarding civil liability issues arising from developments in AI and robotics. In the above-mentioned Resolution, it has been suggested, in the long term, to create a specific legal status of “electronic personality” for robots, at least, a high level of sophistication so that they could be held liable for harm and damage caused by their autonomous decisions or the independent interactions they form with third parties.

The idea of providing some kind of legal personality for AI systems similar to the status of corporations is not new; on the contrary, it is much-debated since Lawrence Solum’s seminal article. The EP Resolution of 2017, so to speak, “inflamed” the discussion among European schol-

---

* Assoc. Prof. Dr., Faculty of Law, Bilkent University, Ankara, Turkey. bozcelik@bilkent.edu.tr, ORCID: 0000-0002-3666-8566.

** This paper is based on the research of the author within the project on ‘Artificial Intelligence and Law’ (2019-2021), funded by Scientific and Technical Research Council of Turkey (TÜBİTAK) (Grant No. 119K323). The author is grateful to TUBITAK for its support and to Ms. Sıla Öztür, Ms. Boyda Sıker and Ms. Ece Deniz Ginet for their assistance in the preparation of this paper.


4 Resolution, para. 7.


ars. Even though there are authors who find such an idea plausible, it seems that the majority considers it inappropriate or unnecessary.\(^7\)

Rejection of the electronic personhood approach in the Proposal seems to be an appropriate preference to the existing social and legal reality considering the current level of technology. It is true that the electronic personhood approach improves the status of the injured party as it provides her with a single and clear address see. However, such a liability regime is only meaningful with assets from which the compensation may be obtained. On the other hand, even though assets are created for electronic persons at the expense of raising the costs, this does not guarantee an advantageous position for the injured party, as the source of the compensation would be limited to the allocated assets.\(^8\)

Nevertheless, it should be noted that neither rejecting nor accepting the electronic personhood approach in precise terms seems accurate. To date, even though it is not deemed necessary to establish a system in which AI systems have legal personality considering the various costs that this might entail, the factors which determine whether such a necessity shall arise include the level of development and prevalence of the technology.

II. Inclusion of Immaterial Harm

According to Article 2(1) of the Proposal, compensation for damages caused by the physical or virtual activity of an AI system is possible for harm or damage to the life, health, physical integrity of a natural person, to the property of a natural or legal person and significant immaterial harm resulting in a verifiable economic loss.

This provision brings important and unanswered questions as to the inclusion of immaterial harm resulting in a verifiable economic loss caused by the physical or virtual activity of AI-systems, since immaterial harm is traditionally excluded from strict liability.\(^11\) In fact, the Parliament itself has requested further examination from the European Commission on the national laws of the Member States regarding compensation for immaterial harm to determine whether it is necessary and appropriate, to include such harm in the legal instruments for AI at EU level.\(^12\)

It should first be determined that loss of earnings, for example, due to not being able to work caused by physical injury, should be considered as material harm in terms of Article 2(1) of the Proposal. On the other hand, according to Article 2(1) of the Proposal, only economic loss that results in significant immaterial harm is compensable.\(^13\) In other words, the Proposal does not seem to cover "pure" economic loss.\(^14\) For example, certain damages arising from a transaction driven by an AI system such as loss of money or the purchase of goods for a higher value cannot be considered under the scope of the Proposal since they do not result from immaterial harm. Similarly, mere pain or stress that the injured party suffered from cannot be compensated under the Proposal either, unless it has resulted in a verifiable economic loss. On the contrary, compensation can be sought under strict liability for harm or damage arising from, for instance, loss of reputation that results in an economic loss inflicted by a high-risk AI system.

The inclusion of immaterial harm which results in a verifiable economic loss is subject to differing views in the literature. Some authors find the scope of the provision being limited to immaterial harm that causes verifiable economic loss in the exclusion of other immaterial harm unfair and qualify it as a restriction on the injured person’s right of access to justice.\(^15\) Some others, on the contrary, argue that any type of immaterial harm should not be compensated through strict liability which only requires a causal link between the regulated risk and the harm or damage, since this would make the compensable damages indefinite, making it impossible to calculate the liability risks, thus the insurability of liability.\(^16\)

Undoubtedly, it is an issue of legal policy whether to include immaterial harm in the scope of strict liability. The inclusion of such damage would increase the risk and therefore the cost of insurance, whereas its exclusion would leave such harm without compensation under the Proposal.

---

\(^7\) H.S. Antunes, Civil Liability Applicable to Artificial Intelligence: A Preliminary Critique of the European Parliament Resolution of 2020, p. 18 (Electronic copy available at: https://ssrn.com/abstract=3743242) This page was last accessed on 25 September 2021.

\(^8\) For the open letter opposing the adoption of the suggestion in question written by certain European experts addressing the European Commission see, http://www.robotics-openletter.eu/ This page was last accessed on 25 September 2021; for differing views on granting legal personality to AI see, Bertolini, ibid, p. 33 et seq.; S. Chesterman. 2020. Artificial Intelligence and the Limits of Legal Personality, International and Comparative Law Quarterly, 69 (4), p. 819 et seq.


\(^11\) See, Wendehorst, ibid, p. 167 et seq.

\(^12\) Resolution, para. 19.

\(^13\) Preamble of the Proposal states that “[…] Significant immaterial harm should be understood as meaning harm as a result of which the affected person suffers considerable detriment, an objective and demonstrable impairment of his or her personal interests and an economic loss calculated having regard, for example, to annual average figures of past revenues and other relevant circumstances. […]” (para. 16).

\(^14\) For a different view, see Wendehorst, ibid, p. 166 et seq.

\(^15\) Antunes, ibid, p.13.

\(^16\) Wendehorst, ibid, p. 167.
It is true that the Proposal would generate unfair results if it is accepted that immaterial harm can also be compensated under a strict liability regime. For instance, if an AI system that writes news and publishes content regarding a person which includes negative information, and thus damages his/her reputation, this person could not claim compensation according to the above-mentioned provision for his/her mere sadness and sorrow. On the contrary, if the same scenario happens regarding the products or services of a person, the person suffering damage to his/her reputation could claim compensation by proving economic loss. Not only is this an unfair result, but also it is a restriction of the injured person’s right of access to justice without a just and legitimate reason.17

On the other hand, it should be submitted that the limitation of the above-mentioned provision as to “verifiable” economic loss caused by immaterial harm does not eliminate the obstacles voiced by the view that immaterial harm cannot be subjected to strict liability. An examination of the preparatory work of the Proposal shows that the provision as to immaterial harm was not included in the text of the first draft of 27 April 2020 prepared by the Committee of Legal Affairs,18 but it was added by an amendment19 upon the suggestion of three members of the Committee on 28 May 2020. The underlying rationale for this amendment could be that the difficulties in calculating the monetary equivalent of the immaterial harm may not be present for immaterial harm that causes a verifiable economic loss and that there is no reason to exclude such harm from the scope of compensation. However, such calculation cannot be made ex-ante since the injured party, and the amount of damage or harm cannot be known in advance. Thus, the foremost reason opposing the inclusion of immaterial harm, i.e. rendering the insurance risk unpredictable and leading operators to pay high premiums, sustains its validity.

Although neither the Proposal nor the Resolution provides clarity on the issue, even if it was assumed that the inclusion of immaterial harm has resulted from the aim of rendering damage to data compensable20, it can be seen that the current Proposal has exceeded this goal and another formula is required to achieve the said aim.

III. Operator’s Liability

In the Proposal, without prejudice to the other sources of liability such as product liability and contractual liability, the approach of holding the persons who operate the AI systems (operators) liable for damages caused by those systems is adopted (Articles 4, 8). According to the Resolution, what makes the liability of the operator plausible is that the operator is the person in control of the risks related to the AI system and, similar to the driver of an automobile, that the operator is mostly the first contact for persons that suffer damages, considering the complexity and the interconnectedness of AI systems (para. 10).

Thus, it can be understood that the Proposal follows the approach suggested by the New Technologies Formation of the Expert Group on Liability and New Technologies in its Report titled “Liability for Artificial Intelligence and Other Emerging Digital Technologies” (NFT Report) of 21 November 2019.21 In the Report, it is stated that the reason for preferring the term “operator” instead of the traditional concepts of owner/user/keeper is the fact that these traditional concepts are inadequate, and the term operator is more neutral and flexible compared to these concepts. The Report defines the operator as “the person in control of the risk arising from the operation of an emerging digital technology and who benefits from this operation”.

On the other hand, the term “operator”, among the persons in control of the risks arising from the operation of the system, refers both to persons in direct interaction with the persons that suffer damages and who are benefitting from this operation (frontend operator) and the persons who determine the characteristics of the technology, provide data and technical support service in the background in a continuous manner (backend operator) (Article 3 (d), (e), (f)). The Preamble to the Proposal explains this preference in that the backend operator who determines and affects the algorithms that have an essential role in the advanced autonomous systems has, de facto, greater control over the risk related to the operation (para. 10). Consequently, it is understood that the Proposal follows the approach suggested in the NFT Report regarding this issue as well.

According to the Proposal, frontend and backend operators have joint liability before the persons who suffer damages22 (Article 11) and their liability is proportional among themselves to the respective degrees of control they had over the risk related to the operation of the AI system. The operator who indemnifies more damages to the injured persons than their share becomes the successor to the injured persons’ rights in the recourse action (Article 12).

Moreover, agreements eliminating or limiting the rights and obligations arising from the Regulation made between the operators and the natural or legal persons who suffer damages, before or after the damage has occurred, are in-

17 Antunes, ibid., p. 13.
20 Antunes, ibid., p. 12.
21 Supra, note 2.
22 According to Art. 11 of the Proposal, “[…] If a frontend operator is also the producer of the AI-system, this Regulation shall prevail over the Product Liability Directive. If the backend operator also qualifies as a producer as defined in Art. 3 of the Product Liability Directive, that Directive should apply to him or her. If there is only one operator and that operator is also the producer of the AI-system, this Regulation should prevail over the Product Liability Directive.”
valid in respect to these rights and obligations (Article 2(2)).

In the Proposal, backend operator is defined as “any natural or legal person who, on a continuous basis, defines the features of the technology and provides data and an essential backend support service and therefore also exercises a degree of control over the risk connected with the operation and functioning of the AI system” (Article 3(f)). However, the fact that the elements stated in the definition are provided cumulatively seems to be capable of decreasing the number of liable parties. The designers of the AI algorithms and the data providers could be different real or legal persons. In that case, the question as to which of these persons will be considered as the backend operator requires clarification.23

On the other hand, the Proposal states that frontend and backend operators shall be liable in proportion to their respective control over the risks arising from the operation of the AI system. According to the adopted formula, since the frontend operator is mostly the one merely operating the system, it is not difficult to foresee that most of the liability lies with the backend operator.24 In this respect, the Proposal reflects the signs of the general approach of the EU on the subject, that is, the risk-based approach. Although this is, without doubt, correct from many aspects, it might result in the overprotection of the frontend operator, particularly when the AI systems are used for commercial or professional purposes since taking only the control over the risks into consideration may result in neglecting the other legitimacy ground for the responsibility, that is the element of “benefit”. However, the principle “Qui sentit commodum, sentire debet et onus”25 (who enjoys the benefit ought also to bear the burden) is almost a universal principle of law. Thus, a formula which requires the frontend operator, who benefits from the operation of the AI system - for instance by saving time and personnel costs or gaining reputation through the accuracy and reliability of the results of its work - to be liable for a part of the damage, at least in the recourse stage, would be more in accordance with the above-mentioned principle and seems to stand as a fairer solution.

IV. Classification of AI Systems as “High-Risk and Others”

1. Concept of High-Risk AI System

The Proposal subjects the AI systems to a dual categorization as high-risk AI systems and others and includes two different sets of provisions on liability for these categories. According to the Proposal, “high-risk” refers to the potential of harm to one or more persons by an autonomous AI system that is higher than what can be coincidentally or reasonably expected.26

According to Article 4(2) of the Proposal, an exhaustive list of high-risk systems and critical sectors will be attached to the Regulation, and the European Commission is empowered to adopt delegated acts to include or delete AI systems in or from this list, or change the critical sectors for the existing AI systems. AI systems which are not listed as such will be considered as low-risk and subject to fault liability with reversed burden of proof.

It can easily be understood that the purpose of such a listing is to ensure legal certainty for operators of AI systems. Thus, it is aimed at providing foreseeability in advance as regards the liability regime to which possible harm or damage caused by AI system is subject. Nevertheless, some authors, considering the diversity of AI systems, argue that listing only high-risk systems would not suffice to ensure legal certainty, since operators cannot be completely sure as to whether their AI system would be considered low-risk before harm or damage occurs.27

Categorizing AI systems as “high-risk” and “others” reflects the risk-based approach adopted by the EU on other legal issues related to AI. This categorization was used previously in the White Paper28 of 19 February 2020 and was taken as a basis in the Commission’s Proposal of 21 April 2021 for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts (AI Act Proposal) accordingly.29 However, as rightly pointed out in the White Paper, depending on the area, different categorizations regarding risks can be made.30 Thus, the Proposal can be criticized for using the categorization of “high-risk and others” as the unique criterion and not considering any other factors to determine whether an AI system is subject to strict liability or fault liability with the reversed burden of proof.31

On the other hand, it should be kept in mind that the characteristics of AI systems such as complexity, opacity and self-learning that create difficulties regarding legal lia-

---


24 Wendehorst, ibid, p. 176.

25 D. 50,17,10 (Paulus).

26 According to the Preamble of the Proposal, “[. . .] Determining how significant the potential is of a high-risk AI system to cause harm or damage is dependent on the interplay between the purpose of use for which the AI system is put on the market, the manner in which the AI system is being used, the severity of the potential harm or damage, the degree of autonomy of decision-making that can result in harm and the likelihood that the risk materializes. [. . .]” (para. 13).

27 Bertolini/Episcopo, ibid, p. 7.

28 For details, see White Paper, (supra, note 2), p. 17.


31 For a criticism of this approach and as regards factors that would be considered see Bertolini/Episcopo, ibid, p. 6.
bility for the operation of the AI are present for low-risk and high-risk AI systems alike. Moreover, low-risk systems are also capable of causing severe harm. Therefore, there is no reason justifying the providing of less protection for the persons harmed due to such applications. Furthermore, subjecting the statute of limitations, the amount and scope of damage to the laws of the member state in which the damage occurs seems against the EU’s aim of unification.

Another legitimate criticism directed at the Proposal is the contradiction caused by the fact that the Product Liability Directive, which is also developed as a solution for liability issues brought about by the technological complexity similar to AI, does not subject products to any distinction such as high-risk or low-risk. Moreover, the Proposal or the Resolution do not explain the reason for this difference which creates not only a disadvantaged position for the producer as opposed to the operator but also seems to violate the principle of vested rights.

2. Consequences of the Operation of a High-Risk AI System

a) Strict Liability and Burden of Proof

According to the Proposal, the most significant effect of considering an AI system as high-risk in terms of civil liability is the providence of the strict liability of the operator for the damages caused by such systems while liability for low-risk AI systems is subject to fault-based liability where the burden of proof lies with the operator. Whereas operators of high-risk systems can be exempted from liability only if they can prove that the damage is caused by force majeure (Article 4(1), (3)); operators of low-risk systems can avoid liability on the condition that they prove that they have acted in due diligence that can be expected of them (Article 8).

First of all, the Proposal does not include an explicit provision on the burden of proving causation. Considering both the general principles as to liability and the arguments in the preparatory work of the Proposal, it can be understood that the burden of proof lies with the persons that suffer damages. As opposed to the suggestion in the NTF Report, the Proposal does not either contain any provision that might alleviate the burden of proving causation. This can be considered as a significant deficiency for the Proposal since causation is not only the decisive element of strict liability, but also the most complex issue regarding liability for AI.

The Proposal provides for the option of using the data generated by an AI system for the injured party’s convenience in proving the harm and damage. Still, such an option would not be functional since the injured party would probably lack the necessary technical knowledge and infrastructure to utilize the data without resorting to an expert.

Moreover, the duty of cooperation of the producers of AI systems, envisioned in favor of the operator and the injured party, is provided merely for low-risk systems. However, since the same obligation could be needed in the strict liability regime to which high-risk systems are subject, it would be more appropriate if this provision was provided as applying to both types of systems.

On the other hand, as stated above, force majeure is provided as a general ground for evading liability in the Proposal. However, it should be borne in mind that apart from the acts of God, this term has different meanings depending on the context in which it is used. Different elements of this term have also been accepted in different legal systems and different answers can be given to the question of whether a particular event can be considered as force majeure. Both the Proposal and the Resolution are silent on what constitutes force majeure. As generally accepted, since the typical risks of an activity cannot be considered force majeure, it must be clarified if, for instance, a power cut or a connectivity problem would constitute force majeure under the Proposal.

b) Mandatory Insurance

According to Article 4(4), the frontend operator of a high-risk AI system is obligated to ensure that the activities of the said system are adequately covered by liability insurance, to the amount and extent provided under Articles 5 and 6 of the Proposal. Likewise, the backend operator is under obligation to ensure its services are covered by a business liability or product liability insurance that is in line with the scope provided for in Articles 5 and 6. It can be understood that the Proposal adopts the approach suggested in the NTF Report.

Article 5 of the Proposal provides for the monetary upper limit of the amount of compensation whereas Article...

32 Bertolini/Episicopo, ibid, p. 9.
34 Antunes, ibid, p. 7.
35 According to the NFT Report, (supra, note 2), if the damage caused by emerging technologies is sourced from a breach of safety rules, the burden of proving causation and/or fault and/or defect should be reversed. In the Report, on the issue of proving causality, while it is deemed appropriate that, as a principle, the person who suffers damages bears the burden of proof, as in the current liability regime; it is suggested that a lower standard of proof shall be applied for certain situations regarding technology considering the complexity and opacity of the emerging technologies (Key Findings, para. 26 and p. 49 et seq.).
36 Bertolini, ibid, p. 82.
37 Galbois-Lehalle, ibid, p. 3.
38 See NFT Report, (supra, note 2), Key Findings para. 33 and p. 61 et seq.
39 Up to a maximum amount of EUR two million in the event of the death of, or in the event of harm caused to the health or physical integrity of, an affected person, resulting from an operation of a high-risk AI system; up to a maximum amount of EUR one million in the event of significant immaterial harm that results in a verifiable economic loss or of damage caused to property, including when several items of property of an affected person were damaged as a result of a single operation of a single high-risk AI-system.
6 provides for the damages and costs within the extent of compensation for high-risk AI systems. The above-mentioned provisions seem to intend to keep the risk calculable in terms of insurance. These topics for the low-risk systems are not included in the Proposal and are subject to the law of the Member State in which the damage has occurred (Article 9). 40

In the EP Resolution of 2017 and in the NTF Report, one of the solutions suggested to guarantee compensation for the damages caused by the operation of AI systems is the creation of compensation funds. 41 Without any doubt, establishing compensation funds for AI systems is particularly important if the liability for system failures has not been insured. 42 In fact, the Resolution encourages the member states to establish compensation funds as regards such cases. 43 Nevertheless, the Proposal does not provide for the possibility of setting compensation funds for the low-risk systems, which are outside the scope of mandatory insurance.

c) Limitation Period for Claims

The statute of limitations, to which liability is subject, is another topic expressly provided for under the Proposal. According to Article 7, the limitation period for civil liability claims arising from harm to life, health or physical integrity is 30 years from the date on which the harm occurred. For property damage or verifiable economic loss resulting from significant immaterial harm, it is 10 years starting from the date of occurrence or 30 years from the date on which the operation of the damaging or harming high-risk AI system took place. The statute of limitations for low-risk systems, similar to the issues of the amount and extent of compensation, is subject to the law of the Member State in which the damage has occurred (Article 9).

V. Ambiguity Regarding Decision Supporting AI Systems

The Proposal describes its scope as “where a physical or virtual activity, device or process driven by an AI system has caused harm or damage” (Article 2(1)). According to this description, there is no doubt that the provisions of the Proposal shall be applied when, for instance, a fully autonomous vehicle hits a pedestrian and causes her death where a patient suffers damage due to the faulty intervention of a surgical robot that operates entirely based on AI.

However, today, AI systems are widely used as systems supporting human decisions. As such, experts (such as doctors, financial advisors or lawyers) make professional decisions based on the data generated by the expert system and act according to that decision. Since the Proposal excludes economic loss from its scope as a principle (unless it is a verifiable result of immaterial harm), it is clear that any damage caused by the operation of AI systems as systems supporting human decisions in the sectors such as finance or investment will not be compensated. Nevertheless, it must be decided whether the Proposal covers liability for damages caused by AI as a system supporting human decisions in the health sector, since compensation for the damage to the health of a real person is within its scope. On the other hand, in the health sector, it is not clear whether the provisions of the Proposal are intended to apply to any damage caused by a faulty diagnosis and/or a treatment based on the data provided by a system supporting human decisions. A clear answer to this question cannot be derived from the Resolution either.

Considering the words “driven by an AI system” and “caused” in the Proposal, it can be argued that the above-mentioned situations are excluded from the scope of the Proposal. For example, in cases where a doctor makes a faulty judgement for diagnosis or treatment depending on an AI system, it can be argued that this decision relies on the doctor and is not entirely “AI-driven” or “AI-caused”. If this approach is adopted, the existing liability regimes of the Member States would be applied. Generally, the doctor or their affiliated entity would be liable under fault liability and/or vicarious liability. The injured party would not be able to refer directly to the backend operators, and the liability of the backend operator would be in question only during the recourse action of the liable party who compensated the injured party.

If situations in which the AI systems are used to support human decisions are considered within the scope of the Proposal, it first ought to be decided if such systems are classified as high-risk. Although health applications are not included in the high-risk systems list attached to the AI Act Proposal, it is stated that such applications will be considered high-risk systems and the related safety regulations will be included in the specific legislation (NFL) to avoid reiteration and complication. 44 If one assumes that this approach will be adopted in the high-risk list attached to the proposed liability Regulation as well, it can be stated that health applications will be subject to the regime for the high-risk systems provided in the Proposal. Thus, health applications will be subject to a strict liability regime. The frontend operators (usually the entity that is the owner of the hospital) and the backend operators (the developer

\[40\] For a criticism of this provision from the stand point of private international law see, J. Von Hein, Forward to the Past: A Critical Note on the European Parliament’s Approach to Artificial Intelligence in Private International Law, available at: https://conflictoflaws.net/2020/forward-to-the-past-a-critical-note-on-the-european-parliaments-approach-to- artificial-intelligence-in-private-international-law/ This page was last accessed on 25 September 2021.


\[42\] Antunes, ibid, p. 16.

\[43\] Resolution, para. 22.

\[44\] The Preamble of the AI Act Proposal, (supra note 28) paras. 28-29.
and the updater of the software) will be jointly and severally liable to the injured party and will be liable in ratio to their respective control over the system among themselves, unless they prove that the damage was caused by force majeure. Furthermore, such systems will be subject to the special provisions provided for by the Regulation for the high-risk systems on the issues of mandatory insurance (Article 4(4)), amount and extent of compensation (Articles 5–6), and limitation periods (Article 7).

The fact that the Proposal does not provide clarity on the issue of systems supporting human decisions in the health sector, which is currently the strongest area in which AI systems are used, qualifies as a deficiency. This issue must be further elaborated and clarified during the legislative process.

Classifying health applications as high-risk systems, and thus subject to strict liability in terms of the Proposal, seems to be an appropriate preference in terms of legal policy. Considering said applications as low-risk would mean that the injured party would not benefit from the advantages of strict liability. In that case, if the person harmed in the example of wrong medical diagnosis or treatment refers to the doctor/hospital, she would face the defense that the due diligence requirement has been fulfilled by using the system and basing the decision upon the system or the defenses provided for in Article 8(2)(b) of the Proposal. On the contrary, where the injured party refers to the developer of the system, it would be raised that the direct cause of the damage was the doctor’s decision so that there was no adequate causal link between the fault in the system and the damage or harm occurred. Such a situation would harm public confidence in AI systems, thus would create an unwillingness to use these systems. On the other hand, the preference favoring a strict liability regime that covers the indirect damage and harm caused by AI, providing better protection for the injured party, would increase the confidence in the above-mentioned reliability. Even though strict liability seems to oppose the interests of the developers of the AI systems at first glance, the confidence in AI products resulting in an adequate liability regime (undoubtedly combined with an effective safety regime) would increase the demand for these systems and, in the long term, be in the developers’ interest.

**Conclusion**

New developments in AI technologies are heard almost every day, followed by contemporary examples of harmful events involving said systems. Due to developments in this domain, an inclination to regulate several aspects of AI is observed, particularly in the EU. Dealing with the liability for harm or damage caused by AI systems, the Proposal of the European Parliament analyzed in this paper demonstrates one such attempt and should be welcomed as being the most concrete step taken towards the aforementioned inclination. It should also be considered as a step forward, at least symbolically, to reassure the public for its partially legitimate concerns regarding emerging technologies and increasing the public trust in AI systems.

Nevertheless, the Proposal is not free of criticism. As such, one of the main issues is the way “immaterial harm” is provided for. To provide consistency, as it is submitted in this paper, either the Proposal should cover all types of immaterial harm or immaterial harm should be entirely excluded from the scope of the Proposal. Secondly, considering the possibility that designers of the AI algorithms and data providers can be different persons, the question of which of the above-mentioned shall be determined as the backend operator should be clarified. Thirdly, as regards at least the recourse relationship between frontend and backend operators, a new formula—that also takes the benefits obtained by the frontend operator of the AI systems into account—should be developed. There is also a need for further clarification as to the meaning of “force majeure” as a general ground for exemption from liability. Last but not least, the existing ambiguity regarding situations where AI systems are used for supporting human decisions should be eliminated.

It is beyond doubt that the above-mentioned concerns would only be valid if liability for AI caused harm or damage were made subject to a single and general instrument, such as one intended by the Proposal. Where such an instrument takes the form of a regulation, there would be an advantage of creating a uniform legal framework in the EU and thus assuring legal certainty and preventing law shopping. Nevertheless, it should also be admitted that such a single and general instrument always bears the risk of adopting a sole criterion to be applied to every situation (such as the “high-risk and others” criterion adopted in the Proposal at hand) which would undermine the diversity of AI applications and legal necessities related to such diversity.

Thus, it seems simpler and more appropriate (i) to amend the Product Liability Directive to clearly cover AI systems as “products” within its scope as well as to alleviate the burden of proof of the injured as to causation and (ii) to regulate all other issues in sector-specific instruments to eliminate possible drawbacks that a general instrument would have due to different types and usages of AI systems.

---

45 For the suggestion of holding either the hospital or the provider or the producer of the medical assistive technology strictly liable see Bertolini, ibid, p. 116 f.; for another point of view that suggests strict liability of the producer of the medical recommender system in conjunction with strong defenses see Wendehorst, ibid, p. 169 et seq.