UNIVERSITY OF HELSINKI

https://helda.helsinki.fi

# Artificial Intelligence and (Compulsory) Insurance

**Faure, Michael; Li, Shu**

**2022-05-13**
de Gruyter
http://hdl.handle.net/10138/358072
Faure, M & Li, S 2022, 'Artificial Intelligence and (Compulsory) Insurance', Journal of European Tort Law, vol. 13, no. 1, jetl-2022-0001, pp. 1-24. https://doi.org/10.1515/jetl-2022-0001

Downloaded from Helda, University of Helsinki institutional repository. https://helda.helsinki.fi
This is an electronic reprint of the original article.
This reprint may differ from the original in pagination and typographic detail.
Please cite the original version.

Michael Faure* and Shu Li**

# Artificial Intelligence and (Compulsory) Insurance

**Abstract:** This article discusses the compulsory liability insurance for AI-related harm proposed in the ongoing EU policy debate. We not only explain from the demand side why liability insurance would not be the only financial security needed to deal with the risks created by emerging technologies, but we also clarify from the supply side the obstacles concerning the application of liability insurance in the digital age. This article argues that, even if policymakers are determined to mandate liability insurance for AI-related risks, it must be established in a balanced and evidence-based manner. Compulsory financial security is only indicated when there is a risk that the activity may cause serious damage and could lead to insolvency.

## I Introduction

There has recently been much activity by various legislators with respect to the regulation of artificial intelligence (AI). Some even refer to a race for regulation.[1] An important aspect of the search for this regulatory framework is the design of an appropriate liability regime. Many agree that at EU level, the traditional framework provided by the European Product Liability Directive[2] is not fit to deal with the many challenges provided by AI.[3] Most recently, at EU level, a variety of proposals have been launched in relation to liability for AI-related harm. In this respect, we can mention the important work (in 2019) of a European Expert Group on Liability and New Technologies (EG-NTF).[4] In addition, in 2020 the European Commission launched a White Paper on Artificial Intelligence[5] and the European Parliament adopted a Resolution (EP Resolution) calling on the Commission to make a regulation with respect to the liability of AI

* Michael Faure is Professor of Comparative Law at Maastricht University and Professor of Law and Economics at Erasmus University Rotterdam, The Netherlands. E-Mail: michael.faure@maastrichtuniversity.nl

** Shu Li is Postdoctoral Researcher of Law and Artificial Intelligence at University of Helsinki, Finland. E-Mail: shu.li@helsinki.fi The author would like to thank the help of project funding granted by the Academy of Finland, decision number 330884 (2020).

1 *NA Smuha*, From a 'Race to AI' to a 'Race to AI Regulation': Regulatory Competition for Artificial Intelligence (2021) 13 Law, Innovation and Technology 57.

2 Council Directive 85/374/EEC of 25 July 1985 on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] Official Journal (OJ) L 210/29. For comments, see *P Machnikowski*, European Product Liability: An Analysis of the State of the Art in the Era of New Technologies (2016).

3 See eg *P Machnikowski*, Producers' Liability in the EC Expert Group Report on Liability for AI (2020) 11 Journal of European Tort Law (JETL) 137.

4 Expert Group on Liability and New Technologies – New Technologies Formation (EG-NTF), Report on Liability for Artificial Intelligence and other emerging digital technologies (2019) <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid= 36608>.

5 European Commission, White Paper on artificial intelligence, COM(2020) 65 final, 6.

operators.[6] Even more recently (April 2021), the Commission published a proposal for a regulation concerning harmonised rules on artificial intelligence (AI Act).[7]

Even though none of these many proposals has official status yet, it is interesting that, within the context of the discussion on liability for AI, a discussion concerning the role of insurance has also emerged. In the EP Resolution, it was even explicitly mentioned that it would be desirable to make liability insurance for particular operators (of high-risk AI systems) mandatory.[8] The EP Resolution also proposed that the Commission should work together closely with the insurance sector to guarantee that insurance policies which can offer adequate coverage for an affordable price are made available.[9] Much has been published meanwhile on liability for AI.[10] Most of those studies mention the suggestion at the European policy level to introduce mandatory insurance for AI operator liability,[11] but they do not provide further analysis of the insurance obligation.[12]

This contribution aims to take a step back from the often-heated discussion on liability for AI-related risks, in order to discuss the role of insurance in managing AI-related liability risks. The central research question will be whether the proposals recently made at the policy level to introduce mandatory insurance for AI-related risks can be supported by our analysis. In order to be able to answer that question, we will discuss more generally the role of insurance, ie why an individual may have a demand for insurance and for which particular risks and why society may in some situations have the need to impose a duty to seek financial cover. We will therefore not discuss, at least not in detail, the liability regime for AI-related risks, as that has already been analysed in other studies, but we will rather focus on insurance and insurability. We consider that it is still important to recall that liability and insurance are closely connected. It is sometimes argued that 'liability follows insurance' in the sense that an expansion of liability (such as in the case of AI) is often made conditional upon the availability of insurance cover. Policy-makers are often reluctant to introduce far-reaching liabilities for which no financial security can be obtained. Although we recognise that, from a policy perspective, this is obviously important,

---

6 European Parliament Resolution, Report with recommendations to the Commission on a civil liability regime for artificial intelligence, 2020/2014(INL) <https://www.europarl.europa.eu/doceo/document/A-9-2020-0178_EN.html>.

7 European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (ARTIFICIAL INTELLIGENCE ACT) and Amending Certain Union Legislative Acts, COM(2021) 206 final, 2021.

8 EP Resolution (fn 6) art 4(4).

9 EP Resolution (fn 6) nos 24–25; Recitals 21–22.

10 See *B Koch*, Liability for Emerging Digital Technologies: An Overview (2020) 11(2) JETL 115; *C Wendehorst*, Strict Liability for AI and other Emerging Technologies (2020) 11(2) JETL 150; *P Machnikowski*, Producers' Liability in the EC Expert Group Report on Liability for AI (2020) 11 JETL 137. See also, *M Buiten/A De Streel/M Peitz*, EU Liability Rules for the Age of Artificial Intelligence (2021) SSRN 3817520; *B Schütte/L Majewski/K Havu*, Damages Liability for Harm Caused by Artificial Intelligence – EU Law in Flux (2021) 69 Helsinki Legal Studies Research Paper; *G Wagner*, Liability for Artificial Intelligence: A Proposal of the European Parliament (2021) SSRN 3886294.

11 The proposal in that respect from the European Parliament was not created in isolation. Already the EG-NTF Report had equally suggested a strict liability with compulsory insurance. See EG-NTF (fn 4) 39 ff; see also *G Borges*, New Liability Concepts: The Potential of Insurance and Compensation Funds, in: S Lohsse/R Schulze/D Staudenmayer (eds), Liability for Artificial Intelligence and the Internet of Things (2019).

12 See in this respect inter alia *A Bertolini/F Episcopo*, The Expert Group's Report on Liability for Artificial Intelligence and Other Emerging Digital Technologies: a critical assessment (2021) 12 European Journal of Risk Regulation (EJRR) 644.

from an academic point of view, the question of a desirable liability regime is a different one, having different goals than the financial security regime. That is why in this contribution we mostly focus on the aspect of financial security.

The remainder of our contribution is structured as follows: first, we provide some background concerning AI, liability and financial security (II). Then we move to the perspective of the individual who might seek financial security, explaining why there might be a demand for financial security (III). We then move to the supply side, explaining who could provide financial security, equally discussing conditions of insurability (IV). Next, we analyse the question of the circumstances in which it may be in society's interest to make financial security mandatory, both generally as well as in the specific case of AI (V). At the same time, we clarify that mandatory financial security should only be imposed when particular strict conditions are met (VI). Another important question is who should be given the duty to provide financial security if such a mandatory mechanism were to be introduced (VII)? Section VIII concludes.

# II Background

## A What is AI?

Artificial intelligence, in essence, is a prediction technology,[13] which is a very broad notion sometimes covering relatively simple and limited interventions to support decision-making by man until situations where machines would be self-learning and autonomous (although that is to a large extent still rather futuristic).[14] From a technological perspective, the method employed by AI could be largely different. For example, some AI systems are driven by algorithmic tools that apply statistical models or logic trees to formalise or represent knowledge (eg expert systems). A more advanced category of AI, which has raised considerable debate in recent years, is based on big data analytics and machine learning. In this context, AI is employed with further self-learning ability to detect patterns and discover optimal mathematical relationships by processing a large scale of data.[15]

The policy documents at the EU level have not delivered a consolidated notion of AI. Nevertheless, it seems that the scope of AI systems is much broader than our expectations. For example, according to the EP Resolution, the notion of AI 'comprises a large group of different technologies, including simple statistics, machine learning and deep learning'.[16] Likewise, the proposed AI Act also defines AI as a technology that is developed with one of diverse techniques (eg machine learning, logic- or knowledge-based or statistical approach).[17] The result of overly defining AI would be that a large number of parties would be covered and influenced by the regulation of AI.

---

[13] *A Agrawal/J Gans/A Goldfarb*, Prediction Machines: The Simple Economics of Artificial Intelligence (2018).

[14] *P Čerka/J Grigienė/G Sirbikytė*, Liability for damages caused by artificial intelligence (2015) 31 Computer Law & Security Review 376.

[15] *C Coglianese/B Dor*, AI in adjudication and administration: A status report on governmental use of algorithmic tools in the United States (2021) Brooklyn Law Review 796.

[16] EP Resolution (fn 6) no F.

[17] AI Act (fn 7) art 3(1); Annex 1.

## B EU policy proposals

The various policy documents mentioned in the introduction have proposed a rather wide-ranging liability for various actors involved in the AI chain. The reason why policymakers are aiming at the design of a liability regime is that there is a lot of fog surrounding the use of AI. It is clear that, on the one hand, AI can bring huge benefits to society, thus increasing the happiness of mankind and social welfare, so-called positive external effects. At the same time, these technologies can bring particular risks of damage, so-called negative external effects.

By setting up liability rules, there will be an effect of providing incentives for the stakeholders involved to follow an optimal care level.[18] It could thus have a preventive effect. The ongoing policymaking at the EU level and the scholarly debate have been focusing on developing liability rules applicable to the different parties along the supply chain. The bottom line of these proposals is that some party along this chain should be liable for the harm caused by AI systems.[19] In the context of AI, a revisit of the liability attributed along the value chain is necessary. For AI systems, which can create severe harms, strict liability should be imposed upon particular parties.[20] A specific public consultation has been initiated to consider how to adapt liability rules to the age of AI, in which the efficacy of the Product Liability Directive (PLD) and the necessity of establishing a liability regime for AI would be investigated.[21]

According to the EG-NTF, the developer of an AI system should be strictly liable for the harm caused by the defects of an emerging technology, irrespective of whether they take a tangible or digital form.[22] In addition, operators of an AI system should also be subject to strict liability if they have a high degree of control over the AI system and their activity has the potential to cause significant harm.[23] The EP Resolution further proposes a risk-based approach to decide the liability of operators, according to which, the operator of a high risk AI system would be subject to strict liability, whereas others would be subject to a fault-based rule.[24]

To the extent that the stakeholder is held liable, the liability rule could also lead to compensation. The already mentioned ongoing policy debate on the appropriate liability regime indicates that there may be different parties (potential victims and injurers) that may have a demand for financial security to deal with AI-related risks.

---

[18] This incentivising effect of liability rules is especially stressed in the law and economics literature. See *S Shavell*, Economic Analysis of Accident Law (1987); *W Landes/R Posner*, The Economic Structure of Tort Law (1987).

[19] *H Zech*, Liability for AI: Public Policy Considerations (2021) 22 ERA Forum 1; *A Panezi*, Liability Rules for AI-Facilitated Wrongs: An Ecosystem Approach to Manage Risk and Uncertainty, in: PG Mexía/FP Bes (eds), Artificial Intelligence and the Law (2021).

[20] *Wendehorst* (2020) 11(2) JETL 150, 171.

[21] For the information about the Consultation, see <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en>. For the response to the Consultation, see eg European Law Institute, <https://www.europeanlawinstitute.eu/news-events/upcoming-events/events-sync/news/response-to-the-european-commissions-public-consultation-on-civil-liability/?tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=8f9f81bf40ed505078e3f8c5afc89232>.

[22] EG-NTF (fn 4) 42.

[23] EG-NTF (fn 4) 39.

[24] EP Resolution (fn 6) arts 4 and 8.

### C Financial security

Financial security instruments (of which insurance is one) are a response to risk. Risk can be expressed as the probability (likelihood) that an event, which causes a particular damage related to AI, might occur.[25] The most important reason why there would be a demand for financial security to deal with risk is risk-aversion. Individuals often have an aversion against risks with a potential high magnitude of damage, especially when the damage could endanger their entire wealth. Given the limited assets of most individuals, a majority of the population is averse to risks and may seek financial security (for example, insurance) in order to be protected from risk.[26] So, also for AI-related risks, there may be a demand for financial security, especially if the potential damage were to be large and individual assets limited. We will now address the questions of who would demand financial security for AI-related risks, and why (Sec III) and of who could provide this financial security (Sec IV) after which we will examine whether there are arguments, in particular conditions, to make financial security mandatory.

## III The demand for financial security

### A Insuring damage or liability: first- and third-party cover

As we have just explained, there are potential risks that may emerge in relation to AI, which could consist of personal injury or property damage. As a consequence, there may be a demand for financial security to cover those losses. Two fundamental ways of providing financial security can be generally differentiated: first-party and third-party techniques.

First-party financial security provides cover to an individual (or firm) who is exposed to a particular risk, whereby the potential victim seeks financial security for that particular risk. In this situation, the financial cover is directly provided to the person or entity exposed to the risk and, as a consequence, that entity will also pay (for example, an insurance premium) for that financial security.

Third-party financial security provides cover for the risk that a party may have to compensate the damage suffered by a third party on the basis of liability. That is referred to as third-party cover as it is not the potential victim who directly seeks financial cover, but the financial cover is rather provided for the case where someone will be liable to cover the damage suffered by a third party (the victim). Liability insurance is a typical example of third-party cover.

### B Example

Suppose that there is a robot serving the plates in a restaurant (assuming for a moment that the robot makes decisions, such as when to start or stop moving and when to place dishes on or collect plates from the table, by collecting and analysing the data from their real-time interaction

[25] This goes back on Frank Knight's famous distinction between risk and uncertainty. See *FH Knight*, Risk, Uncertainty and Profit (1921).

[26] *KJ Arrow*, Uncertainty and the Welfare Economics of Medical Care (1963) 53 American Economic Review 941; *KJ Arrow*, Aspects of the Theory of Risk-Bearing (1965).

with the environment). Several incidents could occur with different types of damage that can illustrate the difference between third-party and first-party losses. A first possibility would be the one where the robot collapses and (suppose that it is a Michelin-star restaurant) a variety of expensive dishes fall on the floor and break and the carpet in the restaurant is ruined as well. This is a typical situation of a first-party loss to the restaurant owner.

Suppose now that the robot again has an incident in which it collapses, and all the plates fall on a client, not only ruining her expensive Chanel dress, but equally causing burns to her skin. This is a typical situation where the restaurant owner might be liable to compensate the harm to the victim, third-party cover.

## C Demand for financial security depends on risk aversion

The previous example shows that there may be a demand for financial security to cover the loss, but that mostly depends on whether the operator has risk aversion. The aversion towards risk will depend upon the potential magnitude of the loss and on the owner's assets. As far as the first-party loss (spoiling the food and the carpet) is concerned, if the owner has reasonable assets to cover the losses and if the potential damage is relatively low, the owner could bear its own losses. For most of those losses there would, in other words, not be any risk aversion and consequently no demand for financial security. It may be that the restaurant owner has no risk aversion for an incident with losses of an average magnitude, but he may be averse to exceedingly high losses. In that case, the restaurant could, for example, take out so-called excess cover, for example indicating that he only demands cover if the losses were higher than say € 100,000. For those high losses also, the restaurant owner would be risk averse.[27] It is important to understand that consequently the demand for financial cover depends, on the one hand, on the size of the potential loss and, on the other hand, on the available assets. That will determine the restaurant owner's attitude towards risk and consequently the demand for financial cover.

## D Liability

In the context of third-party (liability) cover, the same also applies: assuming for a moment that the restaurant owner would be liable for the harm to the lady, he would have a need for financial security if the potential damage was expected to be high, especially in relation to his own assets. Since personal injury is involved with possible non-pecuniary losses related to the burn wounds, damages could potentially be substantial or at least there could be uncertainty, which may trigger risk aversion and thus a demand for financial cover from the restaurant owner.

However, a crucial element in this context is obviously whether or not the restaurant owner would be liable for the losses.[28] As mentioned above, the various scenarios discussed in EU policy documents and in the literature usually distinguish between the potential liability of, on the one hand, the developer of the software and, on the other hand, the operator.[29] The above

[27] Obviously, the premium a restaurant owner would have to pay if he only took excess cover (as in this example) would be substantially lower than if the restaurant owner took complete cover, also for small losses.

[28] *Borges* (fn 11) 148.

[29] As far as the operators are concerned, a distinction is further made between so-called frontend and backend operators. The issues, such as to which kind of liability rule these parties are subject and under which liability regime they will be placed, fall beyond the discussion of this article. The bottom line here is that, as long as these

example with the robot can illustrate the different situations and the corresponding demand for financial security from the perspective of the restaurant owner: suppose in a first scenario that the robot committed the incident as a result of an erroneous design in the software. That would most likely point to liability of the software developer, in which case (of course strongly dependent upon the specificities in the legal system where the example might occur), the victim would have to address her claim for damages to the developer of the software in the robot and there would be no liability of the restaurant owner and as a consequence no need for financial security.

If, however, in a second scenario, the software was perfectly designed and timely maintained by the designer, but it appeared that, for example, the restaurant owner ignored explicit instructions or used the robot for a purpose for which it was not intended, as a result of which the robot caused the incident, then this would point to a potential liability of the operator. In that particular case, the operator could be exposed to liability and would thus have a need for financial security.

Obviously there may be refinements in the legal system, as a result of which, for example, the victim might have the possibility to first sue the restaurant owner (even in the case when it was a flaw in the design of the software that caused the incident), as a result of which the restaurant owner subsequently has to take recourse against the software developer. But the important point to recall for now is that in the liability setting, the first element to determine whether there will be a need for financial security is obviously the simple question of whether the particular individual (such as the restaurant owner in the example) is exposed to liability at all. Only in that case might there be a demand for financial security. And it should be noted that demand will again depend upon his risk attitude (resulting from the magnitude of the potential damage and his assets).[30]

# IV The provision of financial security

## A The basics

Even though there may be differences between the various forms of financial security, there are a few basic elements that are common to most forms of financial security, but these are mostly discussed in the context of probably the most common form of financial security, in other words insurance. It is a mechanism whereby a risk-averse individual can shift a risk to another entity, the insurance company. The reason that an insurance company can take over the risk is the law of large numbers: because a large number of individuals exposed to a similar risk can be pooled together in a risk pool, the insurer is able to spread the risk. As insurance relies on the law of large numbers, it is crucial that there is a sufficiently large amount of insured to be included in

---

parties may give rise to some risks in the process of either creating or operating the AI system, they may have to ultimately share some of the liability.

[30] For the moment we assume that the individual (like the restaurant owner) has a demand for financial security as long as the potential damage could be higher than the individual wealth. However, there may be situations where the operator would not have a demand for financial security beyond their own assets as it would in that way (via insolvency) have the possibility of shifting the damage to society. That insolvency risk is precisely the reason why we will argue below (see section V) that there may be a reason to make financial security mandatory.

the pool. Statistical predictability can only be created when a large enough insurance pool is created in order to spread the risk. A large number of insured is, moreover, necessary in order to collect the premium income needed to cover the damage.

Moreover, insurers need to have sufficient information to be able to calculate a premium. In most simple terms, the premium is the result of the multiplication of the probability and the potential damage. That constitutes what is called the actuarially fair premium. In order to determine the probability with known risks, the insurer relies on statistics. Statistics are usually derived from past damage and risk histories. When there is little or no information on the damage or the probability, insurers are unable to calculate an actuarially fair premium and this may lead to 'uninsurability'.[31] In such a case, to some extent modelling and risk assessment models could be used. However, insurers may have doubts when there is little information with respect to the risk and also uncertainty about the magnitude of the potential damage. It is a situation referred to as 'insurer ambiguity', which may lead an insurer to charge an additional risk premium.[32] In some cases, there may be a different perception of the risk between, for example, an operator seeking insurance coverage and considering the risk to be fairly low, versus the insurer, who may have less information and, as a result of insurer ambiguity, demands a relatively high premium.

## B Conditions of insurability

From these sketched basics of insurance, it appears that predictability is the key to insurance. An important condition for insurability is therefore that the insurer can determine the probability of the accident as well as the magnitude of the damage. There may be particular uncertainties related to AI-related risks, which could endanger insurability.

An important issue in this respect is legal certainty concerning the liability regime. For an insurer, it is important to be aware of the scope and possibility of liability during the insurance period, thus allowing the insurer to calculate the premium. Currently, there are still many debates and uncertainties related to liability for AI risks, inter alia concerning the liable party.[33] This could seriously endanger the insurability of AI-related risks.[34] There are other conditions that need to be fulfilled for insurability, which may precisely be a problem in the case of AI, given the numerous uncertainties, inter alia concerning causation.[35] As the scope of liability for AI-related risks is, as of now, not very clear, it may be extremely difficult today for insurers to assess the exact scope of the risk exposure, which may seriously endanger insurability.

Another condition of insurability is that the problems of adverse selection and moral hazard have to be addressed. Adverse selection refers to the fact that insurance is always more attractive

---

[31] *MG Faure*, The Limits to Insurability from a Law and Economics Perspective (1995) 20 The Geneva Papers on Risk and Insurance: Issues and Practice 454.

[32] *H Kunreuther/R* Hogarth/*J Meszaros*, Insurer Ambiguity and Market Failure (1993) 7 Journal of Risk and Uncertainty 71.

[33] For an overview of this legal uncertainty regarding AI-related harm, see Section II.B.

[34] Legal uncertainties, for example, equally endanger the insurability of liability in other emerging technologies such as 3D printing. For a further analysis, see *MG Faure/S Li*, Risk Shifting in the context of 3D printing: An Insurability Perspective (2020) 45 The Geneva Papers on Risk and Insurance 482.

[35] See generally on conditions of insurability, *MG Faure/T Hartlief*, Insurance and Expanding Systemic Risks (2003) OECD 81 ff. The question of how causal uncertainty affects the insurability of disruptive technologies (eg 3D printing) is discussed by *Faure/Li* (fn 34) 492 ff.

for those who are exposed to higher risks and who would therefore be more in need of insurance. If insurance only attracted those high risks, a situation of uninsurability would arise.[36] Moral hazard refers to the tendency of individuals receiving full insurance coverage to increase the risk, as they are themselves no longer exposed to risk, since this has been transferred to the insurer.[37] In order for a risk to be insurable, insurers need to ensure that their policies are sufficiently differentiated according to risks. This practice would result in distinguishing between the various risk types so that a lower risk is rewarded with a lower premium. This would allow insurers to remedy adverse selection. Insurers could also impose policy conditions, such as experience rating, to deal with moral hazard. Without the required differentiation and appropriate policy conditions, adverse selection and moral hazard could undermine insurability. [38] Risk differentiation is easier with first-party insurance policies than with third-party insurance. The reason is that, under first-party insurance, the insurer can exactly know the insured person and may thus have a better idea of the risk. This is in contrast to a third-party situation, where a range of potential third parties could incur damage and thus there may be more uncertainty.[39]

Adverse selection and moral hazard may obviously also appear when financial security is provided for AI-related risks. The appropriate remedy requires that the insurer has information on the behaviour of the particular insured, which may generally be a large problem with cyber-related risks. It may simply be extremely costly for the insurer to access private information on the individual behaviour of the insured that may affect the risk.[40] More particularly, given the many uncertainties in the digital world, it could be that traditional insurers are often rather reluctant to cover digital risks. Some policies might be available to cover AI, but the amount of companies offering such cover may be limited, which obviously has an effect on the premiums.[41] Also in other domains related to the digital world, such as cyber security, insurers are generally reluctant to provide cover as they often consider the risks of the digital world to be largely unknown and thus difficult to calculate.[42]

Besides cyber security vulnerability, the current policymaking at the EU level is also discussing the possibility of making 'significant immaterial harms' caused by AI to be compensable under the liability regime. [43] Imagine that, in the future, a claim of being discriminated against by an online advertising recommender system may lead to the liability of

---

[36] Because in that situation adverse selection and the well-known market for lemons would emerge. See *GA Akerlof*, The Market for 'Lemons': Quality, Uncertainty and the Market Mechanism (1970) 84 Quarterly Journal of Economics 488. For the theory enshrined in insurance, see *GL Priest*, The current insurance crisis and modern tort law (1986) 96 Yale Law Journal (Yale LJ) 1521.

[37] *S Shavell*, On Moral Hazard and Insurance (1979) 93 Quarterly Journal of Economics 541.

[38] As Koch mentioned, the insurer should tailor the policies according to the various aspects of the risk, ideally with respect to each insured entity. See *BA Koch*, Comparative Report, in: BA Koch (ed), Economic Loss Caused by Genetically Modified Organisms: Liability and Redress for the Adventitious Presence of GMOs in Non-GM Crops (2008) 615.

[39] See on this point especially *Priest* (1986) 96 Yale LJ 1521.

[40] Similar dangers also emerge in other digital technologies, such as insuring 3D printing. See *Faure/Li* (fn 34) 495 ff.

[41] *A Bugra*, Room for Compulsory Product Liability Insurance in the European Union for Smart Robots? Reflections on the Compelling Challenges, in: P Marano/K Noussia (eds), InsurTech: A Legal and Regulatory View (2020) 176 f.

[42] See generally *C Biener/M Eling/J Wirfs*, Insurability of cyber risk: An empirical analysis (2015) 40 The Geneva Papers on Risk and Insurance 131.

[43] EP Resolution (fn 6) art 5.

an operator; it would be rather more difficult for insurers to predict the risk when operators attempt to avoid the risk. In addition, the EP Resolution, as well as other documents, are considering removing the development risk defence.[44] A producer or an operator will therefore be responsible for updating the AI system on a continuous basis, regardless of whether or not such a risk can be predicted by the state of art. Such proposals would further prevent insurers from accurately predicting the risk, which may result in a high premium or even make the risk uninsurable. It is therefore equally to be expected that, as far as AI-related risks are concerned, there may be considerable reluctance among insurers to provide cover.

## C Various financial security instruments

Regarding the concrete financial security instruments applicable to AI-related harms, the EG-NTF Report has advised that: '[t]he more frequent or severe potential harm resulting from emerging digital technology, the less likely it is that the operator is able to indemnify victims individually, and the more suitable mandatory liability insurance for such risks may be.'[45] In this case, the Expert Group correctly indicated that mandatory liability insurance should be limited to cases where risk is high and there is a danger of insolvency. The EP Resolution proposed that mandatory liability insurance should be based on a risk-based approach, requiring operators of high-risk AI systems to ensure that their activities are covered by liability insurance.[46] This approach is also an important choice for the Commission when attempting to adapt civil liability to the digital age.[47] In addition, the EP Resolution 'believes that a compensation mechanism, funded with public money, is not the right way to fill potential insurance gaps'. [48] A compensation fund is only applicable in very exceptional cases when an AI-system is not yet classified as high-risk.[49] The EP Resolution therefore has a narrow perspective on financial security instruments by merely referring to mandatory liability insurance.[50]

That is remarkable for a number of reasons. The first reason is that many policy documents (like international conventions) that do introduce a duty to provide financial security do not usually just limit financial security to insurance, but either formulate a broad obligation to provide solvency guarantees, without specifying which form this should take, or provide examples of various financial security mechanisms that could be employed to constitute the solvency guarantee. Most international conventions refer to insurance or other acceptable

---

44 EG-NTF (fn 4) 39 ff.

45 EG-NTF (fn 4) 61.

46 EP Resolution (fn 6) art 4(3) and (4).

47 See the Commission, 'Inception Impact Assessment', option 1.c(i) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en>.

48 EP Resolution (fn 6) no 25.

49 EP Resolution (fn 6) Recital 22.

50 In comparison, the function of no-fault schemes as a financial security has been widely discussed in the US literature. For example, Pearl has argued that the no-fault victim compensation fund can assure quick and fair compensation for the harms caused by autonomous vehicles. *T Pearl*, Compensation at the Crossroads: Autonomous Vehicles & Alternative Victim Compensation Schemes (2018) 60 William and Mary Law Review (Wm & Mary L Rev) 1827; see also *MA Lemley/B Casey*, Remedies for Robots (2019) 86 The University of Chicago Law Review 1311, 1381 f; *KS Abraham/R Rabin*, Automated Vehicles and Manufacturer Responsibility for Accidents (2019) 105 Virginia Law Review 127, 156 ff.

financial securities. For example, international regimes on nuclear liability provide a duty for the operator to maintain insurance or other financial security up to the cap of its liability.[51] Other international conventions do not specify the type of financial security to be provided or refer broadly to 'insurance, bonds or other financial guarantees including financial mechanisms providing compensation in the event of insolvency'.[52] In fact, there is no international convention that would limit a duty to provide financial security to insurance.[53] Other European documents that do impose a duty to seek financial security would normally not limit this financial security to insurance. For example, art 7(10) of Directive 2009/31/EC on the geological storage of carbon dioxide (CCS Directive) states that applications for storage permits must include proof that the financial security or other equivalent provisions will be valid and effective before the injection of carbon dioxide begins. A European Commission Guidance Document details a wide variety of security mechanisms that operators could use to provide financial security. The Guidance Document refers to funds, escrow, bank guarantees, letters of credit and many other alternatives.[54] And even art 14 of the EU Environmental Liability Directive[55] only refers broadly to financial mechanisms which could be used by operators in case of insolvency. It is therefore striking that for AI-related risks, the policy documents suddenly only refer to insurance.

This is also remarkable from a contents point of view. The point is precisely, as just mentioned, that as these risks related to AI liabilities are still relatively new, insurers may generally lack the necessary information to accurately determine actuarially fair premiums and to engage in the necessary risk differentiation in order to overcome adverse selection and moral hazard. Insurer ambiguity may lead to too high premiums and thus to uninsurability. Not surprisingly, one can therefore also observe that in many markets concerning either new or highly specialised risks, it is not primarily insurance that plays the major role, but the market rather uses alternative forms of risk transfer. For example, in the case of offshore oil pollution, major operators often use reserves (referred to as self-insurance) or create captives (their own insurance companies) as they consider these a more attractive option than shifting risks to insurers. For example, when the Deepwater Horizon incident occurred, BP did not have insurance cover but was still able to cover spectacular amounts of damage via self-insurance.[56] Of course, self-insurance may not be an adequate tool when the operator does not have sufficient assets and there would be a risk of insolvency.[57] But that could be verified through sufficient

---

[51] Paris Conventions art X; Vienna Convention art VII. For details, see *MG Faure/J Liu/N Philipsen*, Liability for Terrorism-Related Risks under International Law, in: L Bergkamp/MG Faure/M Hinteregger/N Philipsen (eds), Civil Liability in Europe for Terrorism-Related Risk (2015) 24.

[52] Eg in art 11(1) of the 2003 Protocol on civil liability and compensation for damage caused by transboundary effects of industrial accidents on transboundary waters. See *Faure/Liu/Philipsen* (fn 51) 44 ff.

[53] See a comparison of different liability regimes in international treaties in *Faure/Liu/Philipsen* (fn 51) 52.

[54] See *MG Faure/R Partain*, Carbon Capture and Storage: Efficient Legal Policies for Risk Governance and Compensation (2017) 168 ff.

[55] Directive 2004/35/EC of the European Parliament and of the Council of 21 April 2004 on environmental liability with regard to the prevention and remedying of environmental damage [2004] OJ L 143/56.

[56] *MG Faure/H Wang*, The Use of Financial Market Instruments to Cover Liability Following a Major Offshore Accident, in: MG Faure (ed), Civil Liability and Financial Security for Offshore Oil and Gas Activities (2017) 238 ff.

[57] For critical reflections, see *C Mackie/V Fogleman*, Self-Insuring Environmental Liabilities: A Residual Risk-bearer's Perspective (2016) 16 Journal of Corporate Law Studies 293, 296; see also *C Mackie/L Besco*, Rethinking the Function of Financial Assurance for End-of-Life Obligations (2020) 50 Environmental Law Reporter 10573, 10583 ff.

monitoring of the adequacy of the type of financial security offered. Precisely since new and technically specialised risks are often hard to insure, one can also observe the emergence of so-called risk-sharing agreements, more particularly for specialised environmental risks.[58] Risk-sharing is, for example, provided by the so-called Protection & Indemnity Clubs (P&I Clubs) being mutual insurance associations established by ship owners to cover third-party liabilities related to the use and operation of ships. This risk-sharing via P&I Clubs, for example, intervenes in covering the damage related to oil pollution.[59] And most recently, given the problems in obtaining adequate insurance cover for cyber security risks, risk-sharing has equally been advanced as a tool for dealing with cyber security.[60] Risk-sharing agreements more particularly emerge when insurers have difficulties in obtaining information on the specific risks, and operators may be better situated to control moral hazard via mutual monitoring. That is why, in many hospitals, medical malpractice is covered through risk-sharing agreements, rather than via insurance. That may well be a viable solution when, for example, a robot with AI supporting a physician's medical diagnosis makes a fatal mistake. Assuming that the mistake is not due to the developer but rather to the operator, it is a typical example where risk-sharing via hospitals (also leading to the sharing of information via mutual monitoring) may be better able to provide financial security than traditional insurance.

In sum, the European policy documents wrongly focus only on insurance as the sole mechanism of financial security whereas 1) other policy documents refer to a broad plethora of other available solvency guarantees and 2) other mechanisms may be better able to deal with AI-related risks than insurance.

# V Arguments for mandatory financial security

So far we have analysed financial security from the perspective of the demand that an individual could have to be protected in the case of risk aversion (Sec III) and we have equally addressed the question of who could provide that financial security (Sec IV). We will now move away from the individual exposed to risk and who is demanding cover, to turn to society's perspective, examining whether there are arguments to make the provision of financial security mandatory in general (Sec V.A) and for the specific case of AI liability (Sec V.A).

## A Mandatory financial security: general

There are important arguments from society's perspective to make financial security mandatory in some cases. Usually, especially for the context of AI, the discussion focuses on mandatory third-party (liability) financial security. But there are cases in which also first-party (victim) financial security is made mandatory. In fact, the entire domain of social security, for example providing health insurance and benefits in the case of being unable to work, could be qualified as a mechanism of mandatory first-party financial security, even though it is usually not the private

[58] See on the differences between insurance and risk-sharing, see *J Liu/MG Faure*, Risk-sharing Agreements to Cover Environmental Damage: Theory and Practice (2018) 18 International Environmental Agreements: Politics, Law and Economics 255, 258 ff.

[59] *Liu/Faure* (2018) 18 International Environmental Agreements: Politics, Law and Economics 264 ff.

[60] See further *MG Faure/B Nieuwesteeg*, The Law and Economics of Cyber Risk Pooling (2017) 14 New York University Journal of Law and Business 923.

market that will provide the cover, but rather social security institutions.[61] Moreover, some have argued that there may be particular arguments to make comprehensive financial cover against disasters mandatory. The main reason is that disasters are low probability high damage events, which are difficult to be imagined by individuals. As a result, cognitive biases will lead to a too low demand for disaster insurance even though it could increase utility. It is for that reason that mandatory first-party insurance for disasters has been advocated.[62] Various countries, and more particularly France, have indeed introduced such a mandatory first-party insurance for disasters.[63] But the mandatory insurance that, for example, the European policymakers refer to in the context of AI, is mandatory liability insurance. The most important reason for mandating financial security for third-party liability is the risk that the party liable for AI-related risks could be insolvent.[64] Insolvency may have as effect that there will not be adequate compensation for the victim. But it can also have as a consequence that the liable party no longer has incentives to take preventive measures. If the expected damage largely exceeds the injurer's assets, the injurer will only have incentives to purchase insurance up to the amount of its own assets.[65] Insolvency (also referred to as the judgment proof problem) can lead to under-insurance and thus to under-deterrence.[66] A duty to purchase financial security for the amount of the expected loss can achieve better results than with insolvency, whereby the magnitude of the loss exceeds the injurer's assets. The reason is that a provider of financial security (like an insurance company) will control the particular risk of the liable injurer (in order to control the moral hazard risk) and thus engage in risk differentiation, imposing conditions that the liable party has to fulfill in order to obtain financial security. In other words: via the control of the moral hazard risk, the financial security provider can implement particular preventive measures and thus avoid the risk of externalising the harm to society, which might otherwise occur with insolvency.[67]

## B Mandatory financial security for AI? - high-risk ≠ insolvency

How do the arguments in favour of mandating financial security compare to the specific case of AI? The crucial question is whether AI applications may entail a risk of serious damage caused by operators with limited assets, thus leading to insolvency. That will of course very much depend upon the specific circumstances of the case and the technology where AI is applied. The EP Resolution makes a distinction in that respect between high-risk and low-risk activities, but

---

61 There are fundamental differences between cover via the private market (and more particularly insurance) and social security. For details, see *MG Faure*, The Applicability of the Principles of Private Insurance to Social Health Care Insurance: Seen from a Law and Economics Perspective (1998) 23 Geneva Papers on Risk and Insurance 265.

62 More particularly *H Kunreuther*, The Case for Comprehensive Disaster Insurance (1968) 11 The Journal of Law and Economics 133.

63 *MG Faure*, Financial Compensation for Victims of Catastrophes: A Law and Economics Perspective (2007) 29 Law & Policy 339, 350 ff.

64 *MG Faure*, Economic Criteria for Compulsory Insurance (2006) 31 The Geneva Papers on Risk and Insurance 141; see also *Borges* (fn 11).

65 *P Jost*, Limited Liability and the Requirement to Purchase Insurance (1996) 16 International Review of Law and Economics (Int'l Rev Law & Econ) 259.

66 *S Shavell*, The Judgment Proof Problem (1986) 6 Int'l Rev Law & Econ 43.

67 *Faure* (2006) 31 The Geneva Papers on Risk and Insurance 141.

this distinction does not necessarily correspond to the question of whether there is also an insolvency risk (that would be the main criterion for making financial security mandatory).[68]

Let us consider the example provided above of the robot spilling food and damaging the dress of one of the restaurant's guests. If the damage was indeed limited to that, the magnitude of the damage might not be very high and the restaurant owner would be able to compensate (assuming for the moment that it would be the restaurant owner who would be liable for the harm). If, however, this robot caused a burn wound to one or even more guests, the potential damage that could result from this would be huge. If there was equally an insolvency risk for this latter situation, it might be an argument for compulsory financial security. Meanwhile, there are also examples indicating that 'high-risk' AI applications are unlikely to generate an insolvency risk.[69] Nevertheless, according to the ongoing policy debate, mandatory liability insurance would apparently be applied to such situations even though no insolvency had been evidenced there. From the insurance perspective, insolvency should be decided on an evidence-based approach. Without identifying the situations where insolvency risk occurs, mandating liability insurance on a risk basis could lead to undesirable outcomes. The crucial question is whether the potential damage related to the involvement of AI could be higher than the assets of the liable party. A good example of where, in almost all countries for that reason mandatory financial security was introduced, is the case of motor vehicle accidents. There is typically a high risk of serious damage and drivers may have few assets and could thus be exposed to insolvency.

# VI Cautions and conditions

If there was a particular situation where there could be an insolvency risk, this might be an argument to make financial security mandatory for specific AI applications. But at the same time there are equally warnings formulated in the literature when such a duty to purchase financial security would be introduced:

- A first important aspect is that the duty should be formulated broadly and not limited to insurance. The reason is simple: if the policymaker only mandated the purchase of (liability) insurance, it would make the legislator de facto dependent upon the insurance market. It would, moreover, turn insurers into de facto licensors of AI. If insurance for a particular AI application were not available on the market, that technology could no longer be used, and this might stifle innovation.
- Particularly since AI is still a relatively new technology and there are many uncertainties with respect to the potential risks and losses, it is important to formulate a broad duty to purchase financial security if that were judged necessary for particular applications. That also has the advantage that it would allow the market to develop various alternatives, such as self-insurance, bank guarantees, bonds, capital markets, risk-sharing and many others. It has already been mentioned above that, in many other EU policy documents,

[68] The initial purpose of the risk-based approach followed in the EP Resolution was to determine the scope of strict liability. However, the mere fact that a particular activity constitutes a high-risk does not necessarily imply that there would equally be an insolvency risk, which could justify the introduction of mandatory financial security.

[69] For example, according to the proposed AI Act, an AI system used for recruitment or selection of natural persons would be defined as a high-risk AI system. While such a risk relates to human dignity and should thus be reduced, it should not necessarily lead to an insolvency risk. See AI Act (fn 7) Annex III (4).

the duty to provide solvency guarantees is formulated in a broad manner where a guidance note indicates which types of financial security could be accepted by the authorities.

- It is clearly important that a duty to purchase financial cover should only be introduced if it is clear that sufficient financial cover is available on the market. If such a duty were to be introduced when the relative market was not sufficiently developed, this would have as a consequence that the AI technology could no longer be used and also that, as a consequence, the positive externalities (the benefits of AI) may be lost as well.[70] The current policy documents show a belief that the access to massive and high quality data could be further developed by insurers in the near future.[71] However, no evidence has explicitly indicated whether this expectation could be met in all sectors where AI systems are defined as high-risk and mandatory liability insurance is proposed.
- Since not all AI activities may potentially lead to extensive damage and since not all liable parties (developers or operators) would be unable to compensate the harm, a duty to purchase financial security should only be imposed in the specific cases where it is clear that an insolvency risk may emerge. This is important as it has to be taken into account that providing financial security leads to substantial costs as well. Compulsory financial security should only be introduced in an evidence-based manner (upon proof of potentially serious damage and insolvency). It is therefore important to differentiate between the various AI applications and to look for a technology-specific solution rather than a one-size-fits-all approach.[72]
- If a duty to purchase financial cover were introduced, details of the specific design also need to be worked out, for example the possibility of a direct action of the victim against the provider of financial security (such as an insurer), whereby the insurer cannot call on defences based on the contract with the insured (as is also customary with mandatory motor vehicle insurance).[73] Moreover, if victim compensation were the real goal of the mechanism (as mentioned in the European policy documents), then a mechanism would also have to be worked out which would provide compensation to victims when the conditions of the financial security no longer apply, for example if damage is caused by a particular AI application, but it cannot be identified precisely by which. In those cases, a victim compensation guarantee fund may have to intervene.
- Sometimes it is held that the introduction of a duty to purchase financial security should also lead to a financial limit (a so-called cap) on the amount of a liability. That is, however, not necessarily the case. A financial cap on liability may have negative effects both for victim compensation as well as for deterrence. Moreover, the liability of the injurer could remain unlimited, but the duty to purchase financial security could be limited to a particular amount. Mandating financial security should therefore not necessarily be combined with a financial limit on liability.

---

70 See *Bertolini/Episcopo* (2021) 12 EJRR 644.

71 See eg EP Resolution (fn 6) Recital 21.

72 *Bertolini/Episcopo* (2021) 12 EJRR 644.

73 Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability (The Motor Insurance Directive 2009, Article 13(1)) [2009] OJ L 263/11.

- In the European policy debate, one can detect a mention of a reversal of the burden of proof.[74] Some literature equally welcomes such a reversal of the burden of proof to facilitate victim compensation.[75] It is not so clear for which particular element of liability the burden of proof would be reversed. If it concerned the burden of proving negligence (in case a fault rule would apply), this could still be understood, although it might amount to a strict liability rule, as it may be difficult for developers or operators to show that they were not at fault. More problematic can be the case where the burden of proving causation is equally reversed. That would amount to a situation where a potentially liable party would have to show that its application did not cause the damage to the victim. In the context of AI, considering the opacity of an AI system, such proof could often be very difficult or even impossible to obtain, not only for victims but also for developers or operators. There is therefore a risk that developers or operators would be held liable for losses which have not been caused by their AI technology, even if they have actually optimised their activities in every possible manner. This may not only lead to over-deterrence (thus stifling innovation), but could also lead to uninsurability.[76]

# VII Allocation of the duty to provide financial security

If a duty to provide financial security were to be introduced for particular AI applications, on whom or on what should that duty then be imposed? The logical answer would be that it should be imposed on the liable party. After reading the EU policy documents, it is not immediately clear who that party would be as they distinguish between developers and operators and within operators there are still further distinctions. As a result, there is a wide variety of different parties that could potentially be held liable for AI-related damage, but does that necessarily mean that the duty to seek financial security (to which, for example, the EP resolution equally refers) would also apply to all those parties that could potentially be held liable? That would obviously make things needlessly complicated. And the EP Resolution even adds another complication by suggesting joint and several liability between all parties potentially liable; this is endorsed by the literature.[77] It may be clear that, within such a framework, where a wide variety of different parties could be held potentially liable, it makes no sense to allocate a duty to seek financial security to all of them, as it would lead to an unnecessary accumulation of costs.

If one examines the way in which mandatory financial security is regulated, for example in the international conventions that have introduced mandatory financial security, it is striking that the duty to provide financial security is usually channelled to one particular actor who controls the activity. The major advantage of allocating the duty to provide financial security to the entity that controls the activity is that the duty to provide financial security is allocated directly to the activity. The perfect example of this is obviously the mandatory liability insurance for motor vehicles.[78] The rule is simple: one cannot bring a European vehicle into circulation if there is no liability insurance to cover the particular vehicle. If an accident happens, the victim has a direct

---

74 See inter alia EG-NTF (fn 4) 47 ff.
75 *Bertolini/Episcopo* (2021) 12 EJRR 644.
76 *Faure/Hartlief* (2003) OECD 125 ff.
77 EP Resolution (fn 6) art 11; see also *Bertolini/Episcopo* (2021) 12 EJRR 644.
78 Art 3 Motor Insurance Directive 2009 (fn 73).

right of action on the liability insurance of the car and defences that the liability insurer would hold against the insured cannot be invoked against the victim. Moreover, if the liability insurer judges that another party has contributed to the accident, they can exercise a right of recourse against that third party, but the victim is in principle fully compensated.

That same model applies today as well in most legal systems if an autonomous vehicle were to be brought into circulation. It is in that respect striking that some see important questions concerning the potential liability of producers, operators or road managers in the case of an accident with an autonomous vehicle.[79] But, in fact, if today such a vehicle were to be brought into circulation, the rules concerning the mandatory liability insurance for the vehicle would still apply, as a result of which there is, at least from the victim's perspective, no problem. The role AI can play in a vehicle can, again, be at many levels, varying from simple support with, for example, speed control or parking to (in the future) fully autonomous driving. If such an autonomous vehicle were to be brought into circulation, this would (also on the basis of the current legislation) only be possible if it could be proven that the liability of the vehicle is mandatorily insured. Again, this facilitates the claim of a potential victim. The victim does not need to worry about the question of whether they would have to bring a liability suit against, for example, the developer, the smart road manager or the person that owned the car. The victim can simply exercise a direct right of action against the insurer of the vehicle who has the obligation to directly compensate the victim. Obviously, the insurer may take recourse to recover damages, for example, if the insurer judged that it was a mistake in the software of the developer that caused the accident. But those liability questions do not affect the compensation to the victim, who is protected via the mandatory liability insurance attached to the specific vehicle.

Although this model may generally work, there could still be problems in practice. Insurers may, for example, refuse cover for fully autonomous cars, which would imply that those vehicles could then not be brought into circulation or they may charge prohibitively high premiums. But it is important to learn from the positive experiences (acquired during many decennia now) of the mandatory liability insurance for motor vehicles, which precisely shows that it is important to allocate the duty to seek financial security to one particular activity rather than suggesting a general duty to insure for all potentially liable parties (as the EP Resolution currently does). It is important to channel the duty to provide financial security to one particular activity. Other parties who contribute to the risk could still remain liable, but at least the victim could call directly on the insurer of the activity. If other parties have contributed to the risk, it would be up to the insurer to eventually exercise recourse.

## VIII Concluding remarks

AI can create risks of losses, but it also can bring many benefits to society. As a result, it is important to carefully balance a liability and insurance regime for AI-related risks. To the extent that AI could lead to potentially grave damage, there may be a need for financial security in case of risk aversion. An operator may have a need for first-party cover of its own losses. Developers and/or operators may have a demand for third-party cover to the extent that they are held liable for the losses of the victim.

[79] *Bertolini/Episcopo* (2021) 12 EJRR 644.

The current EU proposals referring to mandatory insurance seem to do this in a much too loose manner, without fully realising the consequences. An initial problem is that (in contrast with other policy documents) the EP Resolution only refers to mandatory insurance rather than formulating a duty to provide solvency guarantees more broadly, insurance just being one of the options. Another problem is that the EP Resolution generally suggests mandatory liability insurance, apparently for all types of so-called high-risk AI applications. While there are some good reasons for differentiating between high risk and low risk for the purpose of deciding whether some risk should be deterred by strict liability, such a category might not help us to precisely decide whether a risk could lead to insolvency or not. From a theoretical perspective, mandatory financial security would only be indicated for risks where there may be potentially serious damage and insolvency. The introduction of mandatory financial security should therefore not be generalised, but technology-specific. It is in that respect striking that, for AI-related risks, the EP Resolution has no problems loosely mandating liability insurance, whereas there is hardly any information yet on the potential scope of the risks related to AI and the corresponding losses. It is striking as, for many other domains of EU law (for example environmental liability), there are today often spectacular incidents with extensive damage, leading to the insolvency of the operator and no adequate victim compensation as in that domain no generalised solvency guarantees exist. One can therefore not escape the impression that the EP Resolution wants to show a strong desire to adequately deal with AI-related risks, without being fully informed about those risks and the potential corresponding losses. We therefore call for a balanced, cautious approach, issuing regulations mandating financial security in an evidence-based manner. Only when the evidence points to the fact that in particular AI sectors risks of extensive damage may emerge, potentially leading to the insolvency of the parties involved, would there be an argument for a carefully designed mandatory solvency guarantee framework. Such a balanced approach may allow society to continue enjoying the benefits of AI and equally control the risks where and when they might emerge via appropriate prevention and compensation mechanisms.