TTLF Working Papers

No. 112

Artificial Intelligence & Civil Liability in Light of the EU’s AI Act and President Biden’s Executive Order

Stefan Heiss

2024
About the TTLF Working Papers

TTLF’s Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF’s Working Paper Series is to share “work in progress”. The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF’s mission and activities.

If you should have any questions regarding the TTLF’s Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria
About the Author

Stefan Heiss is a research associate and Ph.D. law student at the University of Bremen, Germany. He obtained his law degree (Mag. iur., J.D. equivalent) from the Karl-Franzens-University of Graz, Austria, in 2019, where he was awarded the Law Faculty Award. During his studies, he completed a study visit in San Marcos, USA, and worked at the Institute for Civil Law, Foreign and Private International Law. As an associated member of an interdisciplinary research network, he also gained experience in interdisciplinary work. Most recently, he held a research fellowship at the University of California, Berkeley. Stefan’s research focuses on liability issues of new technologies (especially artificial intelligence), national and international commercial and corporate law, comparative law, and the economic analysis of law. In this context, his academic work has been published by academic and peer reviewed journals, e.g. by the Hastings Sci. & Tech. L.J. He received several awards in recognition of his research. He has been a TTLF Fellow since 2022.

General Note about the Content

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:

Copyright

© 2024 Stefan Heiss
Abstract

Most recent EU and US proposals on the governance of artificial intelligence (AI) focus on ex ante regulation to reduce the risks of AI and enhance AI’s innovation. President Biden’s Executive Order from October 30, 2023 builds upon a principles-based approach in which federal agencies should establish AI policies. On December 8, 2023, the EU took pioneering steps to regulate AI applications with a provisional agreement about the AI Act. One of the most pressing concerns to keep in mind is that it may still be too early for regulators to determine exactly how AI will be used. From a civil liability perspective, the effects of such conventional regulatory ex ante requirements for the civil liability standard of AI are particularly relevant. In other words, the impact of current regulatory AI initiatives on civil liability ought to be assessed. In general, the standards of liability law shall not be tied to ex ante regulatory standards initiated by governments such as the AI Act. Civil liability may require a standard for an AI application that is higher than that of a safety regulation, or it may require a standard that is lower.
# Table of contents

I. Introduction ..................................................................................................................... 1

II. EU & US Landscape on AI Governance ................................................................. 4
   A. EU Initiatives ............................................................................................................. 5
      1. AI Act (Dec. 8, 2023) ......................................................................................... 6
      2. Legislative Proposals on Civil Liability for AI ............................................... 10
   B. President Biden’s Executive Order on AI (Oct. 30, 2023) ..................... 15

III. Regulatory Implications for AI Civil Liability Standards ....................... 18
   A. Who should be liable for AI? ................................................................................. 19
   B. Regulatory AI Initiatives and Civil Liability ...................................................... 22
      1. Standards from the AI Act ................................................................................. 23
      2. Principles from the US Executive Order .......................................................... 30

IV. Lessons & Conclusion ............................................................................................... 32
   A. Banning unacceptable AI applications ................................................................. 32
   B. Regulatory Standards ≠ Civil Liability Standards ............................................... 34
   C. International Regulatory Cooperation? ................................................................. 37
I. Introduction

In recent years, the EU and the US have begun to respond to the emerging technology of artificial intelligence (AI) by claiming their regulatory power. On December 8, 2023, a provisional agreement was reached about the AI Act by both European co-legislators, Council and Parliament.\(^1\) This emphasizes that the EU is especially keen to keep its leading position as a global pioneer and guiding light for regulation. But also, on October 30, a, the US President initiated new principles for federal agencies to govern AI.\(^2\) With all the ambition and ability to shape the AI world in the interests of public regulators and amidst the hype for holistic regulation, Hayek’s words ought to be stressed: “The fact of our irremediable ignorance of most of the particular facts which determine the processes of society”.\(^3\) This aspect describes the natural limits of governments to precisely regulate activities ex ante, which is particularly important for the regulation of AI.

To regulate AI, the first question – simply defining AI – seems already doomed to fail since the subject matter is anything but clear.\(^4\) So far, not even computer scientists have agreed on a future-proof definition of AI.\(^5\) Whereas the US defines AI in general


\(^{4}\) AI is also referred to as autonomous systems or robots, see, e.g., Bryan Casey & Mark A. Lemley, *You Might Be a Robot*, 105 CORNELL L. REV. 287 (2020); Sofia Samoili et al., *AI Watch: Defining Artificial Intelligence*, JRC TECHNICAL REPORTS 1, 6-86 (2020) (analyzing 55 key documents of definitions on AI).

terms, the EU first listed techniques and approaches that qualify as AI in an annex. Nevertheless, the AI Act Trilogue has led to the adoption of the revised OECD definition of AI. The AI Act’s scope of application is therefore very broad. For the purpose of civil liability, the distinctive characteristic of AI is its ability to act under uncertainty. Autonomy, connectivity, and opacity are also characteristics that describe AI systems.

From a comparative perspective, it is interesting to note that the EU is the regulator that provides the most precise rules on how to develop and deploy AI systems, even though most of them are built in the US. Since the information on the newest AI developments is mainly condensed outside of Europe, it is – at the very least – questionable whether the EU institutions are in a position to obtain sufficient data in a timely manner. The most prominent examples are foundation models like ChatGPT, which caught the EU regulators by surprise. Of course, the EU is aiming for the so-called Brussels Effect to set European standards for the rest of the world, but is this outcome worth pursuing at all costs?

When it comes to the regulation of AI, the longstanding debate about regulatory impediments to innovation must be taken into consideration. Moreover, the idea that

---

6 Proposal for a Regulation laying down harmonised rules on artificial intelligence, EUROPEAN COMMISSION (Apr. 21, 2021), Art. 3(1) and annex I (e.g. machine learning approaches, logic- and knowledge-based approaches, statistical approaches or bayesian estimation).
7 See Stuart Russell et al., Updates to the OECD’s definition of an AI system explained, OECD (Nov. 29, 2023).
9 See, e.g., Gian Volpicelli, ChatGPT broke the EU plan to regulate AI, POLITICO (March 3, 2023).
civil liability law might be an obstacle to the development of AI has been known for many years. It has been demonstrated that the interplay between safety regulation, liability, and innovation is more sophisticated than simply discouraging one over the other. However, many companies indicated that they have not yet incorporated AI into their daily operations due to the risk of liability. Therefore, the impact of new regulatory initiatives on liability standards appears to be of particular importance. The economic analysis of law and its social cost-benefit comparisons can serve as baseline to compare different instruments of AI governance.

In light of the recent ex ante regulations in the EU and the US, questions of the impact on liability law emerge. AI developers and operators are already governed by civil liability law, and its implications are crucial in the time before regulatory standards would enter into force. For instance, if human oversight is mentioned as a necessary requirement for the usage of AI, one might argue that a failure to comply with this rule would also result in an infringement of the concrete liability standard. This could clarify many issues that deal with the difficulty of the standard of care for AI. In contrast, such a rule may dilute the benefit of the case-by-case approach of liability standards. Certainly, the interaction between tort law doctrines and AI will shape the future concerning AI’s safety level, frequency of use, and cost of development, among other things.

14 European enterprise survey on the use of technologies based on artificial intelligence, IPSOS BELGIUM & ICT, at 58 (2020).
The effects of conventional regulatory ex ante requirements for the civil liability standard can be summarized in two questions: (i) Should a party’s \textit{compliance} with the rules regarding AI relieve the person (manufacturer/operator) of liability if harm occurs? (ii) Should a party’s \textit{non-compliance} with the rules regarding AI result necessarily in the person’s (manufacturer/operator) liability?\(^{17}\)

The following, divided into three sections, answers questions about the impact of current regulatory AI initiatives on civil liability. Section II. provides an overview on the current EU and US initiatives on AI. In particular, this section focuses on the provisional agreement of the AI Act from December 8, 2023 and President Biden’s Executive Order from October 30, 2023. Section III. argues that the standard of civil liability should be based neither on the rules of the AI Act nor on the principles of the Executive Order. Section IV. highlights some lessons that can be learned for the governance of AI.

\section*{II. EU & US Landscape on AI Governance}
Legislators and policymakers in Europe and the US have been ramping up their efforts to regulate AI. Within the EU, the most prominent approach to govern AI is the AI Act, which emphasizes several ex ante approaches on how to develop and use high-risk AI applications.\(^{18}\) Most recently, the US initiated an Executive Order on how to


\(^{18}\) \textit{Proposal for a Regulation laying down harmonised rules on artificial intelligence}, \textit{EUROPEAN COMMISSION} (Apr. 21, 2021); \textit{Proposal for a Regulation laying down harmonised rules on artificial intelligence, Council’s General Approach}, \textit{EUROPEAN COUNCIL} (Nov. 25, 2022); \textit{Proposal for a
deal with emerging risks from AI. The common denominator underlying these efforts is that the existing legal framework is insufficient to deal with the challenges concerning AI. The AI Act as well as the Executive Order ought to overcome some AI hurdles and set global standards for the development and application of AI. These initiatives may have some implications for liability law and in particular the necessary standards of care within one jurisdiction. Liability law differs between European member states as well as between US states. Therefore, the standardization of regulatory approaches appears to be particularly relevant in order to achieve a level playing field for the safety of AI.

A. EU Initiatives

On December 8, 2023 the negotiators of the European Council and the European Parliament reached a provisional agreement on the AI Act. The AI Act focuses on regulatory standards and will become the first far-reaching AI legislation within the EU. Since 2017, the EU institutions have initiated a large number of recommendations and draft regulations. With regard to civil liability, the European Commission and Parliament set out different proposals on what measures need to be taken. Yet these initiatives on civil liability are still in the legislative process and their further course is


\[\text{WHITE HOUSE, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, (Oct. 30, 2023).}\]


\[\text{Resolution on Civil Law Rules on Robotics, EUROPEAN PARLIAMENT (Feb. 16, 2017).}\]
unclear. For the time being, it is particularly important to consider how the AI Act will affect civil liability law.

1. AI Act (Dec. 8, 2023)

The die for regulating AI is cast. From 6 to 8 December 2023, an agreement on the AI Act acceptable to both co-legislators within the EU was reached in the so-called Trilogue\(^\text{22}\) between the European Council and the European Parliament.\(^\text{23}\) Now, the AI Act only needs to be formally adopted by both of them to become official EU law. Before the formal adoption, the provisional agreement just needs some polishing, such as a legal-linguistic revision.

In April 2021, the European Commission initiated the first regulatory framework on AI, known as the AI Act.\(^\text{24}\) By the time the Council and the Parliament reached a preliminary agreement on December 8, 2023, the proposal had undergone several changes.\(^\text{25}\) Since the previous aspects have already been outlined in great detail several times,\(^\text{26}\) the following comments address the most recent AI Act Trilogue deal of December 8, 2023.

There has been no shortage of criticism along the AI Act’s journey. Most recently, the statement of France, Germany, and Italy on a concept of self-regulation for foundation

\(^{22}\) See the glossary of summary: https://eur-lex.europa.eu/EN/legal-content/glossary/trilogue.html.

\(^{23}\) See supra note 20.

\(^{24}\) Proposal for a Regulation laying down harmonised rules on artificial intelligence, EUROPEAN COMMISSION (Apr. 21, 2021).


\(^{26}\) See Heiss, supra note 8 (providing an overview).
models like ChatGPT has once again called into question the European attempt to regulate AI. The agreement between the Council and the Parliament is therefore an important signal to the world that Europe is at the forefront of AI regulation. Consequently, it ensures that different rules on a national level would not become an obstacle to intra-European trade and that no legal fragmentation would occur when it comes to regulating AI across the 27 member states. The EU aims to set a global standard for AI regulation and to promote European interests and values.

The Trilogue’s results include several new elements, ranging from the definition of AI to law enforcement. Five aspects should be of particular note:

First, AI systems are classified by risk, and the necessary requirements of an AI system go hand in hand with its risks. Not all AI systems have the same risk profile. For instance, physical, purely economic, or social risks may be affected to different degrees of severity by different AI systems. The EU prohibits the use of some AI applications due to the fact that their associated risks are unacceptable. For example, social scoring and some cases of predictive policing for individuals are banned from the European market. The major part of the AI Act focuses on high-risk AI systems. They are obliged to various requirements and obligations to gain access to the EU market. There has been criticism of the sectoral approach used to identify high-risk

---

27 See Luca Bertuzzi, France, Germany, Italy push for ‘mandatory self-regulation’ for foundation models in EU’s AI law, EURACTIV (Nov. 19, 2023).
28 The following is based on: supra note 20.
30 See below sec. IV.1.
31 For example, establishing a risk management system, validating and testing data sets, documentation, record-keeping, human oversight and post-market surveillance, see European Commission, supra note 18, at art. 8–15, 17, 19, 21, 62.
applications and the associated strict regulatory provisions. However, the requirements reached in the Trilogue are supposed to be more technically feasible and less burdensome for stakeholders to comply with. For an ultimate conclusion, it is necessary to wait for the final text. Finally, when AI systems are not classified as high-risk, but are intended to interact with natural persons, e.g., chatbots, these systems are subject to very light transparency obligations (so-called limited risk).

Second, the provisional agreement has led to the establishment of minimum standards for all AI systems that can be used for different purposes (general purpose AI). Apart from that, a further distinction was established between two types of foundation models, such as ChatGPT, which are capable of performing a wide range of distinctive tasks. For the first group of foundation models that do not reach the threshold of $10^{25}$ FLOPs, such as ChatGPT-3.5 or Bard, transparency obligations were introduced. Additional regulations apply to the second group of foundation models that reach $10^{25}$ FLOPs, such as ChatGPT-4. Overall, the main concern appears to be the threshold of $10^{25}$ FLOPs, which only covers a small portion of foundation models.

Third, a new governance architecture has been set up to oversee general purpose AI across the EU. This so-called AI Office will be advised by a scientific panel of independent experts to ensure the best possible enforcement. In terms of gathering information on the capabilities and impact of foundation models, this appears to be particularly important. Moreover, an AI Board, which shall include member states’ representatives, will remain as a coordination platform and an advisory body to the

---

Commission. The establishment of a code of practice for foundation models is mentioned as a central task in this context. The development of codes of conduct is particularly welcome, as it serves as a mechanism for the use of information by multiple stakeholders.

Fourth, regulatory sandboxes are the main focus of interest in creating innovation-friendly measures. The allowance for real-world testing of AI systems is also critical in several respects. For AI developers, it may be difficult to assess how risky it is to operate an AI system in public. Testing provides an essential opportunity to do so. From a civil liability perspective, an appropriate level of testing is an important factor in determining the standard of care.

Fifth, in the event of non-compliance, companies face fines of up to 7% of their annual global turnover or €35 million, whichever is greater. Three different categories result from the Trilogue. The first one is the violations of the banned AI applications, which would be penalized with 7% or €35 million. The second category would be a fine of 3% or €15 million for violations of the AI Act’s obligations. The third one would be 1.5% or €7.5 million resulting from the supply of incorrect information. With regard to SMEs, however, further fine caps may apply.

Overall, the provisional agreement of the AI Act is another milestone in establishing Europe as the furthest ahead in regulating AI. Of course, the progress and amendments of the AI Act have demonstrated the difficulties in keeping up when technological breakthroughs emerge. For any further judgement, the final version will have to be awaited. However, the provisions of the AI Act already raise crucial questions for AI
manufacturers and operators regarding civil liability law. The AI Act should apply two years after its entry into force, but questions are already being asked today about the implications for the liability law standards.

2. Legislative Proposals on Civil Liability for AI

It has been argued that the harms caused by AI systems do not always fit neatly into the existing structure of civil liability regimes.\(^{34}\) In this context, several amendments to liability law for a more comprehensive approach were proposed.\(^{35}\) At the European level, a distinction must be made between the Parliament’s proposal and the Commission’s proposal.

In October 2020, the *European Parliament* published a draft regulation on new extra-contractual liability rules for AI.\(^{36}\) The major aspect in the initiative is the proposal of different liability rules for different risks, which is similar to the aforementioned risk classification within the AI Act. High-risk AI systems face strict liability with contributory negligence, whereas non-high-risk AI shall be subject to negligence. Distinguishing between the two sectors of risk is, however, the crux of the matter. The

---


\(^{36}\) *Resolution on a civil liability regime for artificial intelligence*, EUROPEAN PARLIAMENT (Oct. 20, 2020).
attempt to provide legal certainty by establishing a definitive list of high-risk applications has backfired.\textsuperscript{37}

In general, when risks are significantly large and cannot be controlled easily, strict liability seems adequate, as proposed by the initiative for high-risk AI. However, the mere implementation of a sectoral approach similar to the AI Act would lead to frictions in the law of civil liability. For example, the health care sector provides a manifold on different AI applications from surgery robots to spam filters.\textsuperscript{38} It is evident that the spam filter is not associated with a lot of risks, but it would still be subject to strict liability under the sector-specific approach. For the AI developers, this could lead to high barriers to enter the market.\textsuperscript{39} Moreover, finding specific AI cases for an enumerated list of risky applications is inherently difficult. While these concerns about defining and assessing risk are not unheard of,\textsuperscript{40} the wide range of AI activities leads to several applications that have the potential to cause significant harm to the general public.\textsuperscript{41} The risk of operating a particular technology is independent of whether the system is conventionally controlled or AI-controlled. For instance, the

\textsuperscript{37} See, e.g., Gerhard Wagner, Liability for Artificial Intelligence: A Proposal of the European Parliament, in LAW BY ALGORITHM 127, 142 (Horst Eidenmüller & Gerhard Wagner eds., 2021) ("An Enumeration Principle without Enumeration").

\textsuperscript{38} See, e.g., Corindus’ Technology Successfully Used in World’s First in Human Telerobotic Coronary Intervention, BUSINESS WIRE (Dec. 6, 2018); see also AI And Healthcare: A Giant Opportunity, FORBES (Feb. 11, 2019).

\textsuperscript{39} See, e.g., Yavar Bathaee, The Artificial Intelligence Black Box and the Failure of Intent and Causation, 31 HARV. J.L. & TECH. 889, 931–932 (2018) ("Finally, strict liability may impose significant barriers to entry. It may simply be too costly, unpredictable, or difficult to produce and deploy AI without risking potentially ruinous liability.").


risks associated with a conventional lawnmower and an AI-based lawnmower are the same.\textsuperscript{42}

At first glance, an alternative approach to the situation would be to omit the exhaustive list and concentrate on the essential feature of strict liability as a general clause, which would be applied on a case-by-case basis. In scenarios where the risks associated with AI cannot be controlled in a desirable manner, strict liability leads to equality at the compensation level. Nevertheless, this approach would lead to fundamental questions among the legal system of member states that are independent of AI. In jurisdictions like Germany, courts cannot simply impose strict liability on activities that cause abnormal hazards.\textsuperscript{43} It is exclusively the responsibility of the legislator to determine which activity or technology qualifies for strict liability. This aspect is referred to as the principle of enumeration.\textsuperscript{44} Any deviation from this principle would cause disruption in the legal system of countries like Germany, the extent of which is extremely difficult to evaluate with regard to AI.

To conclude, the Achilles’ heel of the Parliament’s initiative is its disruption of national law and its sheer novelty.\textsuperscript{45} In the recent drafts by the European Commission, a different path was chosen.

\textsuperscript{42} Wagner, supra note 37, at 147.
\textsuperscript{43} Gerhard Wagner, \textit{Strict Liability}, in MAX PLANCK ENCYCLOPEDIA OF EUROPEAN PRIVATE LAW (Jürgen Basedow et al. eds. 2012).
\textsuperscript{44} Wagner, supra note 37, at 142.
In September 2022, the *European Commission* proposed two approaches to cope with AI’s liability: on the one hand, concerning adjustments to the producer’s liability for defective products and, on the other hand, initiating a new directive exclusively on the liability of AI.46

First, the current Product Liability Directive 85/374/EEC dates back to 1985. Considering the impact of emerging digital technologies, it has been argued for many years that the existing directive needs to be updated. Although AI was one consideration in adopting the directive, it can still be referred to as a technology-neutral law. At this point, only the amendments to the criterion of a defective product should be highlighted below.47

Several of the extended criteria in art. 6(1) of the proposed directive for the defectiveness assessment are related to AI. In particular, the amendments with regard to the relevant time for placing a product on the market are adjusted to AI. Defects arising after being put onto the market are explicitly included into the defectiveness test according to art. 6(1)(c) and (e) of the proposed directive.48 For example, Microsoft’s chatbot Tay had the potential ability to learn after deployment.49 Furthermore, art. 6(1)(d) considers the connectivity of products.

---


47 See, e.g., Hacker, *supra* note 35; Wagner, *supra* note 35 (both providing further deliberations); Heiss, *supra* note 45 (providing an overview).


Second, the novel draft AI Liability Directive applies to fault-based non-contractual civil law claims for damages caused by an AI system.\(^{50}\) Contrary to the product liability directive, the proposed AI Liability Directive focuses solely on AI and nothing else.\(^{51}\) One important aspect is that the draft is closely intertwined with the aforementioned AI Act.

Art. 2(1) and (2) of the draft directive import the definition of AI and of high-risk AI systems from the AI Act. As mentioned above, the risk-based classification in the AI Act has drawn criticism since its first initiation.\(^{52}\) The AI Act is attempting to provide predictability for the distinction by means of an exhaustive list. Of course, such an ex ante approach seems questionable due to the inherent nature of AI. For example, foundation models like ChatGPT, which operate in a variety of tasks, were not explicitly mentioned as high-risk; some have called for these systems to be included in the list.\(^{53}\)

Contrary to the draft bill by the European Parliament, the proposed AI Liability Directive does not establish or define any rules of liability; rather, it focuses on the law of evidence.\(^{54}\) However, for the intersection between regulation and civil liability one aspect seems of special interest. Recital 23 states that “fault can be established in respect of non-compliance with Union rules which specifically regulate high-risk AI systems like the requirements introduced for certain high-risk AI systems by [the AI

---

\(^{50}\) See *supra* note 46.


\(^{53}\) See Patrick Grady, *ChatGPT Amendment Shows the EU is Regulating by Outrage*, CENTER FOR DATA INNOVATION (Feb. 13, 2023).

Act], requirements which may be introduced by future sectoral legislation for other high-risk AI systems according to [Article 2(2) of the AI Act]”. 55 This might be an implicit gateway to determine the standard of care at the European level, which has to be examined in greater detail below.56

B. President Biden’s Executive Order on AI (Oct. 30, 2023)

Major federal and state regulatory initiatives on AI have been initiated in the US legal landscape. Contrary to the EU, US Congress has not taken comprehensive legislative actions to regulate AI so far. Rather, the focus in the US is on the regulatory policies of federal agencies.57 For example, in 2021, the National AI Initiative Act set forth a framework to strengthen and coordinate AI research, development, demonstration, and education activities.58 In 2022, the White House Office of Science and Technology Policy issued a blueprint for an AI Bill of Rights.59 In 2023, the National Institute of Standards and Technology (NIST), as the federal AI standards coordinator, published a final version of its AI risk management framework.60 Most recently, an Executive Order was published by the White House.

56 See below sec. III.B.1.
57 For a comprehensive overview, see Milanesi, supra note 25, at 49–59.
On October 30, 2023 US President Joe Biden initiated an Executive Order regarding “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence”\textsuperscript{61}. The purpose of the order is to provide the necessary baseline for a coordinated, federal government-wide approach to safely and responsibly govern the development and use of AI. The next step for these authorities is to draft guidelines for responsible AI and policies for the regulation and oversight of AI. The Executive Order thus relies heavily on administrative rule making.

The Executive Order outlines eight guiding principles and priorities to promote and steward AI development and deployment. First and foremost, it is stressed that AI must be safe and secure. Second, the promotion of innovation and competition is mentioned particularly in the context of intellectual property questions to protect inventors and creators, as well as a fair, open, and competitive ecosystem and marketplace. Third, the support for American workers is yet another principle of the Executive Order. Fourth, the advancement of equity and civil rights in the context of AI seems evidential. Fifth, preventing AI from exploiting consumers is essential when AI interacts with them. Sixth, data protection is another important principle in dealing with AI. Seventh, the US federal government has to use AI responsibly. Eighth, the final principle concerns the achievement of a global leadership role for the US in AI policy and AI regulation.

Overall, the Executive Order provides a pathway for federal agencies to address issues concerning AI. It is referred to as the most comprehensive and far-reaching US

\textsuperscript{61} See supra note 19.
While there is the saying that law should leave emerging technologies alone, tech giants like Google, Microsoft, and OpenAI have already stressed the need for AI regulation within the US. Accordingly, the initiative is the result of a lengthy discussion between multiple stakeholders. The values and norms laid out in the initiative may also indicate the US approach for new legislation. Of course, whether Congress will put its teeth into AI legislation is anything but clear.

Some of the principles in the Executive Order are also at the heart of civil liability, especially when it comes to safe and secure AI applications. In these aspects, civil liability is an important cornerstone, as it aims to strike a balance between efficiently protecting potential victims of harm and providing enough leeway for enterprises to develop new technologies. With regard to consumer protection, the mechanism of product liability seems of special relevance to achieve a socially desirable level of protection.

From a bird’s eye view, the order issued by President Biden has a strong influence on federal government using AI, whereas it lacks power to directly address the private sector. To achieve some of the aforementioned principles, civil liability, and especially tort law, seems an appropriate mechanism to do so. In general, however, a common liability regime for AI is not yet on the horizon due to the differences in tort law

---


63 See Brian Fung, Microsoft leaps into the AI regulation debate, calling for a new US agency and executive order, CNN BUSINESS (May 25, 2023); Cecilia Kang, OpenAI’s Sam Altman Urges A.I. Regulation in Senate Hearing, THE NEW YORK TIMES (May 16, 2023); Cristiano Lima, Google bucks calls for a new AI regulator, THE WASHINGTON POST (Jun. 13, 2023).

64 See, e.g., WHITE HOUSE, Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI (July 21, 2023).

among the various states. The more pressing question, then, seems to be whether standards emerge from the Executive Order for liability law. This could be one way in which the initiative has an indirect impact on the private sector.

III. Regulatory Implications for AI Civil Liability Standards

By legal standards, two basic distinctions are necessary, which influence the behavior of AI actors. First, standards of precaution to avoid liability for negligence. Second, regulatory standards to participate in regulated activities and avoid fines and sanctions. The aforementioned overview between the EU and the US regulatory approaches emphasizes that questions on the political agenda are primarily concerned with regulatory standards for AI. The question, thus, emerges: how do the regulatory standards for AI affect civil liability standards?

To answer the question, it is important to understand the function of the two mechanisms. Civil liability law does not operate through social command, but rather indirectly through the deterrent effect when harm occurs and compensation is claimed. In contrast, standards, prohibitions, and other forms of safety regulation directly modify behavior through requirements that are in place before or independent of the actual event.

---

68 See Shavell, supra note 17, at 357–58.
In many ways, civil liability and regulatory standards are intertwined and have a complementary effect. For the approaches by the EU and the US regarding AI, the scope and magnitude need to be clarified. It has been argued that the rules provided in the AI Act determine the critical relationship for civil liability between the amount of damage and the probability of occurrence in a binding manner for courts. In other words, this argument signifies that the AI Act lays down mandatory requirements for the liability standard. However, such an extreme position must be firmly opposed.

First, it is still necessary to ask which actors are involved in the governance of AI. In the past years, several actors – including AI itself – were identified as the least cost avoider for the harm caused by AI systems. A brief glance reveals that several players might be liable, but in any case, AI should not be promoted to a legal entity.

**A. Who should be liable for AI?**

Characteristics of AI systems like autonomy and opacity lead to scenarios with similar outcomes to the well-known Principal-Agent-Problem in corporate governance. But the essential difference between humans and AI agents is that AI lacks incentives to comply with legal mandates. Unlike the principal, there are no monetary or ethical reasons for an AI agent to obey a particular set of standards. Therefore, the objective in the development and use of AI agents can only be that the principal specifies appropriate parameters. So far, three main centers of interest for liability schemes were named: the AI system, the manufacturer (developer), and the operator (user).

---


First and foremost, in 2017, the European Parliament considered the promotion of AI to the status of a person (a so-called ePerson). Since then, the legislators have examined the legal implications of such an ePerson in detail, and neither the EU nor the US have touched it again. Despite the aspects of minimum asset requirement or mandatory insurance, the main obstacle is that AI systems are unreceptive to financial incentives to avoid harm generated by the liability system. Whether or not an AI system complies with the standard of care relies on aspects such as software development, training data, application area, etc. All of these factors can be influenced by the principal, who delegates tasks to the AI system and responds to the incentives of liability. The principal as a financially motivated rational actor will reduce potentially harmful activities to the point where accident costs exceed activity benefits. Therefore, the main focus of civil liability law has to lie on the manufacturer and operator of an AI system.

Secondly, the manufacturer of an AI system seems to be the primary target. Over the course of many decades, a multi-layered edifice of case law has evolved in the US. Since 1985, the directive on product liability provides a common basis for EU member states that closely resembles its US equivalent. In the case of autonomous cars, when drivers become passengers, only the manufacturer has the capability to influence the safety of the car. The manufacturer thus ought to bear the costs of a collision caused by

---

71 See supra note 21, at para. 59 (f).
73 United States v Carroll Towing Co. 159 F.2d 169, 173 (2d Cir. 1947).
a defect.\textsuperscript{76} But not everything is as straightforward as autonomous vehicles. For instance, it seems questionable whether the training of an AI system might already promote someone to the manufacturer of a new AI system. In Europe, the proposed directive on liability for defective products now clarifies that stand-alone software must be viewed as a product.\textsuperscript{77} Accordingly, the scope of application of product liability and therefore the accountability of the manufacturer is going to be broad.\textsuperscript{78}

Thirdly, for example, the output by foundation models like ChatGPT is influenced by its manufacturer (OpenAI) as well as its user. Hence, proper incentives for both seem to be a desirable solution. Regarding unbundled products or open systems, the user is also liable for any software that has been installed after the user obtained the original system and for any modifications that have been made to the original product.\textsuperscript{79} In 2020, the European Parliament initiated a liability framework focusing on the operator who exercises control over the system.\textsuperscript{80} As mentioned above, the introduction of a scheme of strict liability for high-risk AI systems appears to be difficult to realize at present.\textsuperscript{81} According to current tort law doctrines in the US or Germany, users are still subject to conventional civil liability law. In most of these cases, the decisive aspect is the standard of care.

\textsuperscript{76} See Heiss, supra note 45, at 22.
\textsuperscript{77} See Product Liability Directive, supra note 46, at art. 4(1).
\textsuperscript{78} So far, it has been argued that the scope of product liability might appear greater in the US than in other EU countries, see, e.g., Konrad Zweigert & Hein Kötz, Introduction to Comparative Law 671-78 (3d. ed. 1998).
\textsuperscript{79} See Wagner, supra note 72, at 607.
\textsuperscript{80} See supra note 36.
\textsuperscript{81} See supra sec. II.B.
To conclude, both the manufacturer (developer) and the operator (user) are important risk bearers, but they have different levels of influence depending on the AI system. This must be taken into account in liability law.

**B. Regulatory AI Initiatives and Civil Liability**

In a product liability case, the establishment of a product defect is the decisive factor. Two different doctrines have emerged to determine the standards of design defects: on the European side, the consumer expectations test and on the US side, the risk utility test. In the era of AI, to simply base the question of whether a product is defectively designed according to consumers appears to be inadequate. Consumers may irrationally expect 100% accuracy or safety by AI systems, which is impossible to achieve in most cases. As a consequence, socially desirable activities may not be accomplished. Therefore, at least for AI systems, the concept of reasonable consumer expectations is desirable because the expected safety standards are equivalent to a cost-benefit analysis.

In a negligence case, the ascertainment of the appropriate standard of care is necessary. Specifically, the standard to be applied is that of a breach of duty by a reasonable person. From a European perspective, it is important to note that the tort of negligence is based on the jurisdictions of the member states. Of course, tort law in the US also differs within the states. Generally, the standard of care can be explained by using Judge Learned Hand’s formula, who developed three elements of measurement:

---

84 Restatement (Second) of Torts § 283 (1979); see also David G. Owen, The Five Elements of Negligence, 35 Hofstra L. Rev. 1671, 1672 (2007).
the magnitude of the specific loss, the probability of the accident’s occurring, and the burden of taking precautions that would prevent it.\textsuperscript{85}

For the ascertainment of design defects under product liability or standards of care under the negligence doctrine, the impact on non-compliance with regulatory standards for AI seems especially fruitful. If the proposed EU or US initiatives on AI have a decisive impact on the liability standard, then the difficulties in determining a defective product or the standard of care for courts would be mitigated. Further, it has been argued in the context of the AI Act that the decisive aspects of civil liability, namely the amount of damage and the probability of occurrence, are determined in a manner that is binding for courts.\textsuperscript{86}

Two questions emerge from the joint use of liability and regulation: (i) Should a party’s \textit{compliance} with the rules regarding AI relieve the person (manufacturer/operator) of liability if harm occurs? (ii) Should a party’s \textit{non-compliance} with the rules regarding AI result necessarily in the person’s (manufacturer/operator) liability?\textsuperscript{87}

1. Standards from the AI Act
The AI Act provides a manifold number of precise requirements for the development and usage of AI. Now, possible effects from the AI Act on the standard of care for


\textsuperscript{86} See Deng, supra note 69.

\textsuperscript{87} See generally Shavell, supra note 17, at 365.
liability law should be examined with regard to human oversight in art. 14 of the AI Act. This requirement provides a direct way to control the risks associated with AI, mitigating them by the necessity of human intervention.

Art. 14(4)(d) of the AI Act states that a human shall be able “to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system”.88 From a civil liability perspective, the two questions above should be answered with regard to the requirement for human intervention of the AI system in any given situation.

Before answering both questions, it must be noted that most of the strict rules within the AI Act apply solely to high-risk applications.89 The current risk classification for AI has been strongly criticized, especially with regard to civil liability.90 In short, according to art. 6 two criteria are relevant for the high-risk classification.91 The first criterion includes AI systems that are used as safety components of products subject to ex ante conformity assessment by a third party, such as the machinery directive. The second criterion designates AI systems that are explicitly listed in an annex, such as recruitment area. According to art. 7 of the AI Act, the European Commission as public authority is empowered to define the high-risk sectors before those systems operate in public. Due to the fast-moving nature of AI, the effectiveness of such an ex ante approach appears to be highly questionable.

88 See supra note 18.
89 See generally Milanesi, supra note 25, at 14–18.
90 See Heiss, supra note 41, at 194–200.
One major challenge is that the method of evaluating risk (probability x magnitude) differs between the approach within the AI Act and the method for evaluating the standard of care. Contrary to the AI Act’s sectoral determination of high-risk, the riskiness of an activity for the standard of care depends on the specific circumstances of a given situation. Furthermore, risk associated with tort law is based on the rewardable damages, whereas the AI Act may base its risk assessment on other aspects. For example, the provisional agreement provides for a fundamental rights impact assessment before a high-risk AI system is put on the market.⁹² A coherent concept of risk between regulation and civil liability appears very difficult for these reasons.

Apart from these obstacles, it is important to consider the implications of requiring human oversight for AI systems that are not classified as high-risk under the AI Act. Since the majority of AI applications may not fall into the high-risk sector, this observation is of paramount importance. To meet the standard of care for civil liability, it could be argued that non-high-risk AI applications not listed, but still posing some risk, ought to be subject to the same requirements as high-risk systems.⁹³ Conversely, there may be an implicit rejection of any standard of human oversight for non-high-risk AI. In the end, both extreme positions have to be rejected.

(i) Starting with the first question: should a party's compliance with the rules regarding AI relieve the person (manufacturer/operator) of liability if harm occurs?

⁹² See supra note 20.
⁹³ See Deng, supra note 69.
Assuming that governments have less than perfect knowledge of situations and behavior regarding AI, there will undoubtedly be some AI applications that ought to do even more than meet the requirements within the AI Act. The reason might be that they represent a particularly high risk of harm, can take additional precautions at lower costs than others, or can take precautions that are not addressed by regulation.

Situations may arise where autonomy is not desirable. This results in the requirement of automation, which follows pre-determined rules, rather than acting under uncertainty. For example, Annex III of the AI Act refers to the management and operation of critical infrastructure as a high-risk application. More specifically, AI systems that operate in the area of road traffic and the supply of water, gas, heating and electricity would be considered high-risk applications. However, critical infrastructure encompasses a wide range of applications from nuclear power plants to dams and water management. In the case of nuclear power plants, a deterministic control might be the socially desirable way for safety reasons, and stricter requirements seem necessary. Thus, if someone uses an autonomous system in circumstances where a deterministic system would be safer and more cost-effective, that person would not meet the standard of care and could be held liable. Since in the necessary scenarios civil liability will induce AI manufacturer and operators to take socially beneficial precautions beyond those requirements in the AI Act, the application of civil liability as an independent complement to regulation will be beneficial for society.

94 See, e.g., Daniel Malan, The law can't keep up with new tech: Here's How to Close the Gap, WORLD ECONOMIC FORUM (Jun. 21, 2018).
95 See Shavell, supra note 17, at 359–360.
96 But see Jonghyun Kim et al., AUTONOMOUS NUCLEAR POWER PLANTS WITH ARTIFICIAL INTELLIGENCE, 2023 (providing examples on how to apply AI techniques to various areas of nuclear power plants).
97 See Shavell, supra note 17, at 359–360 (providing an example).
The same applies to non-high-risk systems. First, art. 14 of the AI Act does not apply to non-high-risk AI, but the AI Act stresses that an AI developer may voluntarily comply with the AI Act. Even if this were the case, the liability standard would still need to be based on the above criteria. Otherwise, private actors could determine the standard of care by complying with the AI Act if they were relieved of all liability.

Second, shielding AI actors from liability may also amplify irrational behavior through over-investment in AI compliance when it is not necessary.

In some cases, greater care may also be necessary for both high-risk and non-high-risk AI to meet the standard of care in civil law. To simply comply with art. 14 of the AI Act, thus, does not per se satisfy the civil liability standard. For both high-risk and non-high-risk AI systems, the answer to the first question (i) is no. Of course, this finding also supports the legislator in not imposing the strictest rules, as liability law can create additional incentives for precaution to control the risks regarding AI.¹⁹⁸

(ii) The second question is as follows: should a party’s non-compliance with the rules regarding AI result necessarily in the person’s (manufacturer/operator) liability?

If the answer to this question is yes, one must be aware that this would have a wide-ranging effect on the way the liability standard for AI is defined in the diverse national legal systems of the European member states. In recital 22 of the proposed liability directive for AI, it is explicitly stressed that “this Directive does not harmonise the

¹⁹⁸ See Shavell, supra note 17, at 359–360.
conditions under which national courts establish fault.\textsuperscript{99} However, the following recital 23 emphasizes that non-compliance with EU rules, such as the forthcoming AI Act, can amount to a breach of the standard of care.\textsuperscript{100} This aspect demonstrates how intertwined the EU initiatives are and how important it is to address this intersection.

Due to the rigorous fines of up to 7\% of company’s annual global turnover or €35 Million for non-compliance, it seems that high-risk AI operators have strong incentives for compliance. Thus, it is of particular relevance to answer the question of the failure to satisfy the requirements in art. 14 of the AI Act for non-high-risk AI systems. However, the correct answer is no for both of them.

Empirical data show that human oversight, i.e., to override or reverse the output of the AI system, leads to a suboptimal outcome in some scenarios.\textsuperscript{101} For example, if 90\% of human-altered decisions in disease detection worsen the outcome of the AI system, then parties would be undesirably led to comply with human oversight. Consequently, if human oversight diminishes the quality of a particular AI system, the requirement in art. 14 of the AI Act would add unnecessary costs to development, degrade safety, and dilute the advantage of the case-by-case approach of liability standards.

Furthermore, one needs to be aware that technical restraints in the AI development may make it impossible for AI developers to fulfil the requirement of human oversight.

\textsuperscript{101} See Victoria Angelova et al., \textit{Algorithmic Recommendations and Human Discretion}, HARVARD KENNEDY SCHOOL (Oct. 25, 2022), (demonstrating that 90\% of judges underperform the algorithm when making a discretionary override).
according to art. 14. In fact, this could create steep barriers for some technical implications – though socially beneficial – to enter the market. For example, to examine the decision path of an AI system for humans, the documentation of weights of the individual features is extremely important.\textsuperscript{102} However, the representability of these weights varies substantially based on the particular type of AI technique. It has been argued that it is significantly difficult or even impossible for humans to interpret AI models based on sophisticated technology, like random forests or deep neuronal networks.\textsuperscript{103}

Especially in terms of non-high-risk AI applications it seems necessary to stress that the requirements within the AI Act do not always fit for each application. There might also be AI actors who should not be subject to requirements by the AI Act because they have higher costs of care than typical, or they have a lower than typical risk.\textsuperscript{104} This conclusion may also apply to high-risk AI, where the civil liability standards are not based on the provisions of the AI Act.\textsuperscript{105} The failure of an AI manufacturer or operator to satisfy the regulatory requirements within the AI Act does not result per se in their liability.

There is a common understanding among lawmakers and the private sector that there should be no one-size-fits-all approach to AI. If civil liability takes the regulatory standards of the AI Act as its benchmark, the effect of a one-size-fits-all approach is

\begin{itemize}
\item \textsuperscript{103} See Hacker, \textit{supra} note 102; Zachary C. Lipton, \textit{The Mythos of Model Interpretability}, 61 COMMUNICATIONS OF THE ACM, 36 (2018).
\item \textsuperscript{104} See Shavell, \textit{supra} note 17, at 365–366.
\item \textsuperscript{105} Contrary Deng, \textit{supra} note 69.
\end{itemize}
likely to materialize. Overall, it is clear that different standards apply to civil liability, which is also true in the US.

2. Principles from the US Executive Order

The big difference between the EU AI Act and the US Executive Order is that the latter does not have the status of a legislation and addresses federal agencies rather than private actors. The guidelines presented in the Executive Order thus have some similarities with the European Commission’s White Paper on AI from 2020, upon which the AI Act is based.106

Federal agencies are now responsible for identifying appropriate guidance in the relevant sectors. To determine the standard of care for civil liability, this may provide some navigation concerning the relationship between the amount of damages and the probability of occurrence. Similar to the aforementioned conclusion on the AI Act, a mandatory requirement for courts to determine the standard of care in liability law cannot be imposed. The AI operator and developer still might be liable for damages that occur despite compliance with the guidelines resulting from the Executive Order and may be relieved of liability even if they fail to comply.

Unlike the AI Act, the Executive Order alone is too imprecise to provide any further guidance on the standard of conduct for any particular AI application. Given the Executive Order’s principle-based approach, measures for the use of complex AI systems need to be specified. As a result, the current US approach provides little

guidance for establishing specific rules for the development and use of AI. For example, sec. 8(b)(i)(A) of the Executive Order emphasizes, with regard to the health sector, that appropriate human oversight of the application of AI-generated output shall be taken into consideration.\footnote{See also Michelle M. Mello et al., President Biden’s Executive Order on Artificial Intelligence—Implications for Health Care Organizations, JAMA (Nov. 30, 2023).} In contrast to the approach taken at the European level, there are no precise requirements for human supervision. Instead, the need for human intervention must be assessed.

Even if the competent authority defines more detailed measures for the conditions under which AI ought to be used in the medical field, separate standards must be applied for liability law. A recent example from the US, where a similar approach has proven challenging, was the introduction of drone rules. The FAA continued to drag its feet on drone rules: e.g. deadlines set by Congress and self-imposed deadlines were postponed.\footnote{See Larry Downes, America Can’t Lead the World in Innovation if the FAA Keeps Dragging Its Feet on Drone Rules, WASHINGTON POST (Oct. 8, 2014).} Again, this demonstrates the difficulties for agencies to gain information about fast-moving technologies and to keep up with them.\footnote{Cf. Emily S. Bremer, Private Complements to Public Governance, 81 Mo. L. REV. 1115, 1123 (2016) (arguing that “private institutions may be able to respond more nimbly, efficiently, and cost-effectively than administrative agencies to changes in technology, industry practice, or other circumstances”).} The case-by-case approach in civil law can compensate for some of these shortcomings if the standard is not tied to the regulatory requirements.

One final point should be addressed regarding the intersection of liability and regulation: neither liability law nor ex ante rule-based regulation alone will govern AI systems in a socially desirable manner. However, it is important to note that the intervention of ex ante safety regulation is only necessary where liability law fails to
provide the necessary incentives for private actors. On the other hand, courts shall not rely on the regulator’s measures to determine safety standards. Civil liability and ex ante safety regulation are designed to be complementary and mutually reinforcing.\textsuperscript{110} Regardless of what guidelines are finally promulgated by the public authorities, a flexible approach applies to liability law on a case-by-case basis.

IV. Lessons & Conclusion

A. Banning unacceptable AI applications

To ban AI systems that are considered a clear threat to the safety, livelihoods and rights of people is an essential function of ex ante regulation. Manipulative techniques can exploit dark patterns to circumvent users’ free will.\textsuperscript{111} For example, the provisional agreement of the AI Act prohibits biometric categorization to infer sensitive data and some cases of predictive policing for individuals.\textsuperscript{112} Some US Congress members have initiated a bill which would prohibit AI from firing nuclear weapons without final human approval.\textsuperscript{113} In the case of prohibited practices, the conclusion is that the associated risks for society are generally too high to permit the systems – despite the benefits they offer.\textsuperscript{114}

Contrary to a nuanced approach of prohibiting AI, leading scholars like Professor Stuart Russell and entrepreneurs like Elon Musk signed a letter which emphasizes to

\textsuperscript{110} See Daria Kim, Artificial Intelligence Should Not Become a “Black Hole” for Human Agency in Tort Law, 29 TORT L. REV. 152, 165 (2023); Heiss, supra note 8, at 256–257.

\textsuperscript{111} Jamie Luguri & Lior Jacob Strahilevitz, Shining a light on dark patterns, 13 J. LEGAL ANALYSIS 43 (2021).

\textsuperscript{112} See supra note 20.

\textsuperscript{113} Adi Robertson, Lawmakers propose banning AI from singlehandedly launching nuclear weapons, THE VERGE (Apr. 28, 2023).

\textsuperscript{114} See Chamberlain, supra note 91, at 8.
stop the AI development for six months until robust regulations would be initiated. First, the long-lasting EU legislative process demonstrates that a holistic AI policy seems impossible, in a short period of six months. Second, the stop of the development of AI have effects similar to the prohibitions in general. This, however, does not equal the associated risks of AI and thus should not be pursued any further.

The prohibition of certain AI applications illustrates the importance of ex ante regulation. On the other hand, it also demonstrates that it is a walk on a tightrope to determine unacceptable risky AI systems for regulators. Art. 5(1)(a) and (b) concern AI systems that use “subliminal techniques”, but the wording might also be applicable to personalized advertising techniques, which has been a well-established business model for many years. Hence, being clear and precise enough to list only unacceptable AI risks is critical.

Foundation models such as ChatGPT, with its wide range of application and general purpose, make it extremely difficult to adequately manage the associated risks. One might raise the question whether ChatGPT could be considered to pose unacceptable risks and subsequently be prohibited under the AI Act? While the answer to this question seems to be no under the AI Act Trilogue rules, models like ChatGPT emphasize the complexity of regulating AI.

---

117 See, e.g., Ckauidia Novelli et al., Taking AI risks seriously: a new assessment model for the AI Act, AI & Soc (July 12, 2023) (proposing a different method to assess the risk of general-purpose AI like ChatGPT) https://doi.org/10.1007/s00146-023-01723-z.
In sum, there are AI applications that pose threats of harm that are unacceptable in a democratic society. In these scenarios, regulatory intervention by the government appears to be necessary and thus the socially desirable solution, instead of a joint use between regulation and civil liability. However, only a small number of AI scenarios pose an unacceptable level of risk. The AI Act Trilogue agreement mentions, for example, cognitive behavioral manipulation, the untargeted scraping of facial images from the internet or CCTV footage, emotion recognition in the workplace and educational institutions, social scoring, biometric categorization to infer sensitive data, and some cases of predictive policing for individuals.119 A flexible approach, which also relies on the incentivization of liability law, is therefore necessary for the vast majority of AI applications.

**B. Regulatory Standards ≠ Civil Liability Standards**

Civil liability and regulation should not be viewed as mutually exclusive solutions. The key concern to bear in mind is that it might be too early for regulators to precisely determine the usage of AI.120 An example of an unexpected negative effect of a well-intentioned public policy is that young people stopped cycling due to the mandatory wearing of bicycle helmets in several US states.121 If regulators are not sure about ex ante direct safety rules, civil liability may provide the best opportunity to achieve socially desirable outcomes.

119 See supra note 20.
First, the principles in President Biden’s Executive Order can only be understood as a first indicator for civil liability standards. But even after federal agencies initiate new policies, it is up to the courts to designate the applicable AI standards on a case-by-case basis. The failure to comply with regulatory requirements does not, by itself, constitute an infringement of the relevant liability standard. Especially when it comes to more general initiatives, the application and deployment of socially desirable AI systems rely heavily on the incentives generated by the liability system.¹²²

Second, contrary to the general principles by the US Executive Order, the EU put forth a vast amount of specific ex ante safety requirements for AI. From a civil liability perspective, the greatest difficulty may still be a comprehensive risk classification. The approaches in the proposals for a new liability directive or regulation demonstrate that the risk assessment and categorization in the AI Act is not suitable for civil liability law.¹²³ Proposals to be bound by regulatory standards, such as those in recital 23 of the AI Liability Directive, must be strongly criticized as they would cause considerable consequences for the liability law of EU member states and do not appear to be beneficial from a welfare perspective.

The joint use of liability and regulatory strategies can go a long way toward improving the overall safety and efficiency of AI implementation.¹²⁴ It is evident that ex ante regulation is needed when the use of AI shall be avoided altogether. Similarly, it is clear that restrictive rules may create path dependencies and make it hard to change the

¹²² See supra sec. III.B.
regulatory course later. Most recently, France, Germany, and Italy reached an agreement on how to regulate foundation models of AI, such as ChatGPT. Due to its focus on mandatory self-regulation through codes of conduct rather than regulatory rules, the Franco-German-Italian document can be interpreted as a backlash against the restrictive AI Act. The public response to the agreement is divided: on the one hand, it is emphasized that these governments undermine the AI Act and are bowing to the tech industry’s claims; on the other hand, a more balanced approach should be reached. This confirms the regulatory difficulties of a rule-based approach in this early stage of the technology. The lesson to be learned from this ongoing discussion is that civil liability’s aim – to strike a balance between fairly protecting people from AI while also ensuring that companies have enough leeway to develop technologies – often provides a less restrictive approach than ex ante requirements to enter the market.

Enforceability is an aspect that has not yet been mentioned. Of course, the most appropriate rules or liability standards will not cause desirable incentives if AI manufacturers and operators do not face a credible threat of being held liable. It has been argued that the US is especially keen on private enforcement, whereas the EU favors public enforcement. This may also be indicated by the different approaches concerning AI governance. However, new ground is being broken at the European level in terms of public enforcement. The AI Act seeks to establish AI authorities in the EU as well as member states that are still being set up. These new agencies ought

126 See supra note 27.
127 See EU: France, Germany and Italy risk unravelling landmark AI Act negotiations, AMNESTY INTERNATIONAL (Nov. 27, 2023); Germany, France and Italy reach agreement on future AI regulation, THE BUSINESS STANDARD (Nov. 19, 2023).
to deal with the various applications of AI. For this reason alone, it makes sense to consider civil liability as the second pillar and to avoid making AI governance dependent on ex ante regulation. Whether an AI strategy works within a jurisdiction will thus depend much on the regulatory environment and traditions, particularly when international intervention becomes involved.

C. International Regulatory Cooperation?

In November 2023, all of the key AI players attended the AI Safety Summit in the UK. The agreed-upon declaration focuses heavily on risks associated with the most advanced foundation models.129 To rely on a global regulatory cohesion still seems naive, even though the regulation of AI is a supranational issue, and coordination is desirable from a global perspective.

For the sake of international cohesion, especially between the three dominant digital powers – China, the EU, and the US – have the authority to shape the standards for AI governance. But with so many different interests involved, finding a common denominator seems far from easy. In the race to become the digital leader, the EU is especially known for its regulation, the US for its big tech companies, and China for its infrastructure.130 In order to expand its influence on the global market, for the US it might be counterproductive to strictly regulate its AI companies because it might lead to a decline of its power.131 The comparison of the EU and US approaches above

129 See AI SAFETY SUMMIT, The Bletchley Declaration by Countries Attending the AI Safety Summit, (Nov. 1-2, 2023); Derek Robertson, The AI safety summit, and its critics, POLITICO (Nov. 8, 2023).
131 BRADFORD, supra note 130, at 15–16.
reveals some overlap. However, their different interests do not allow for more than an international declaration.

From a European perspective, in consideration of the so-called Brussels-effect,\textsuperscript{132} one might argue that the EU has the power to set global standards worldwide even without an international agreement. For example, the European Council mentions the GDPR as an example of how the EU imposed their standards on other jurisdictions.\textsuperscript{133} But this effect is not as straightforward as the EU would like.\textsuperscript{134} For example, companies cannot simply reduce their compliance costs by choosing the GDPR as the presumed most stringent regulation. With regard to data protection laws, comparative analysis of multiple jurisdictions reveals that no law is the strictest on all measures and some laws go beyond the GDPR’s standards.\textsuperscript{135} In any case, relying solely on the regulatory impact of the EU for international AI standards will not be sufficient.

Beyond regulatory cooperation, international standards reflecting best practices could be achieved through organizations such as UNCITRAL or UNIDROIT.\textsuperscript{136} For example, the section of electronic commerce by UNCITRAL puts forth a “[t]axonomy of legal issues related to the digital economy” also addressing liability issues regarding

\textsuperscript{132} BRADFORD, supra note 10.
\textsuperscript{133} See supra note 20.
\textsuperscript{134} See, e.g., Jens Frankenreiter, Cost-Based California Effects, 39 YALE J. REG. 1155 (2022) (providing an empirical study that the Cost-Based California Effects in data privacy law might be less important than is commonly assumed).
\textsuperscript{135} See Anupam Chander & Paul Schwartz, Privacy and/or Trade, 90 CHICAGO L. REV. 49, 70–80 (2023).
\textsuperscript{136} See John Armour & Horst Eidenmüller, Self-Driving Corporations?, 10 HARV. BUS. L. REV. 87, 114 (2020).
AI. As a result, at least in the long term, a certain degree of international convergence and a level playing field can be expected at the international level.

---

137 Taxonomy of legal issues related to the digital economy, PREPARED BY THE SECRETARIAT OF THE UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (2023).