ERA Forum (2021) 22:147–158
https://doi.org/10.1007/s12027-020-00648-0

ARTICLE

Liability for AI: public policy considerations

Herbert Zech[1,2]

Accepted: 16 December 2020 / Published online: 7 January 2021

Abstract Liability for AI is the subject of a lively debate. Whether new liability rules should be introduced or not and how these rules should be designed hinges on the function of liability rules. Mainly, they create incentives for risk control, varying with their requirements – especially negligence versus strict liability. In order to do so, they have to take into account who is actually able to exercise control. In scenarios where a clear allocation of risk control is no longer possible, social insurance might step in.

This article discusses public policy considerations concerning liability for artificial intelligence (AI). It first outlines the major risks associated with current developments in information technology (IT) (1.). Second, the implications for liability law are discussed. Liability rules are seen conceptualized as an instrument for risk control (2.). Negligence liability and strict liability serve different purposes making strict liability the rule of choice for novel risks (3.). The key question is, however, who should be held liable (4.). Liability should follow risk control. In future scenarios where individual risk attribution is no longer feasible social insurance might be an alternative (5). Finally, the innovation function of liability rules is stressed, affirming that appropriate liability rules serve as a stimulus for innovation, not as an impediment (6.).

Keywords Artificial Intelligence (AI) · Risks · Negligence · Strict liability

✉ Prof. Dr. jur. Dipl.-Biol. H. Zech
sekretariat.zech@rewi.hu-berlin.de

1 Humboldt-Universität zu Berlin, Lehrstuhl für Bürgerliches Recht, Technik- und IT-Recht, Unter den Linden 9, 10117, Berlin, Germany

2 Weizenbaum-Institut für die vernetzte Gesellschaft, Hardenbergstraße 32, 10623, Berlin, Germany

1 Risks associated with AI

New developments in IT, especially robotics, learning ability (machine learning) and connectivity cause new risks or shifts in the control of existing risks. New value chains imply new actors, like data suppliers or machine trainers, which may cause damages through their input into IT systems.

1.1 Three major technological developments: learning ability, robotics and connectivity

From a liability law perspective, three technological developments can currently be identified which have contributed significantly to the fact that IT, i.e. digital systems which process information, is much more powerful – and thus much more useful, but also sometimes riskier – than it was ten years ago: learning ability, robotics and connectivity.[1]

Learning ability (machine learning) denotes the fact that digital systems no longer have to be completely programmed, but can also constantly learn by themselves, or more precisely can change their behaviour through the input of data from the outside world. First of all, this means that the behaviour of a system no longer has to be completely preconceived by a programmer. Programmers of learning systems no longer need to know all the possible states of the system during operation in advance. At the same time, this implies that the programmer has less influence on the behaviour of the system. The learning ability of digital systems is certainly the aspect that most strongly influences the current discussion about the opportunities and risks of artificial intelligence and the legal responsibility for such risks. The underlying question is the attribution of the consequences of using AI, which can be negative or positive. This attribution plays a role, among others, in contract law, liability law or in intellectual property law. However, the ability to learn is not the only aspect that determines the risks and opportunities of IT systems.

Robotics: In liability law, the legal responsibility for the consequences of the use of IT systems has been discussed even before the spread of learning systems, initially with regard to software. The discussion then gained momentum, however, mainly due to developments in robotics. Robotics can be defined as the coupling of digital systems with physical sensors and actuators. Although software always requires an implementation in some hardware, robotics is more than that. Often digital systems generate as an output information to humans. People then use this information; they react to it with a certain behaviour which might ultimately lead to damages. Robotics, on the other hand, creates a new path of damage, in which digital systems can damage physical legal assets such as life and limb or property without intermediate human intervention. This creates new sources of risk for legally protected interests.

Connectivity (interconnectedness): The third aspect, which so far has been discussed mainly for so-called critical infrastructures and in security law rather than

[1] *Spindler* [10], pp. 125, 126-127; *Zech* [15], pp. A18-A53; cf. *Zech* [16], pp. 187, 191–194. The European Commission Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and Robotics, COM (2020) 64 final, 1.2., now explicitly addresses connectivity and openness, autonomy and data dependency as characteristics of AI, IoT and robotics.

in liability law, is the increasing interconnectedness of digital systems. Whereas in the traditional Internet, connectivity concerned the exchange of information between people, the Internet of Things (IoT) now involves an increasing interconnectedness of devices. Robots, i.e. digital systems with direct hardware control, are now directly connected to each other. The most prominent example is probably the vision of fully automated vehicles. A car can only move independently through traffic if it is connected with a large number of other vehicles at the same time (possibly also via a platform), from which it continuously receives data and only then calculates its concrete behaviour. In addition, more and more everyday objects are equipped with information processing systems. A pioneering role in development of connectivity is assumed by the industrial sector with the concept of "Industry 4.0", i.e. the Internet of Things in industrial production. Increasing connectivity leads to additional new challenges concerning both safety and security.

1.2 Associated risks and changes in risk control

The technological developments outlined above give rise to new risks, especially if they are combined. In order to analyse how risky certain products or services are, two dimensions must be taken into account: first, the applied technologies, second, the sector where they are applied. Accordingly, applications with high risks can be identified.

The use of digital systems for tasks that were previously performed by humans also leads to a shift in risk control. Automation shifts control from the user to the manufacturer. With the advent of learning ability, a part of the control is shifted from the programmer to the trainer (which may be the manufacturer but can also be a separate party). The emergence of new value chains, especially primary and secondary markets[2] for data that is used for training IT systems, which are subsequently used for creating new goods, means that new potential liable parties emerge as well. The manufacturer side, comprising development and production of IT systems, and the user side, comprising operation and use of such systems, are supplemented by the data supply side, comprising the collection and aggregation of training data.

A third and important aspect is that increasing interconnectedness may lead to complex causal processes and, ultimately, to problems of provability.[3] When a physical damage is caused by robots it is always possible to identify the robot being the immediate source of the harm and potential persons responsible for it. However, in an interconnected environment, it will likely be more difficult to identify the many other actors who may have had an influence on the actual damage, for example in cases where faulty data from other vehicles or platforms may be the cause of the damage.

[2] *Schweitzer/Peitz* [6], pp. 275-276.

[3] *Spiecker gen. Döhmann* [9], pp. 700-701; *Teubner* [11], p. 202; *Spindler* [10], p. 125, 139.

2 Liability law and innovation: public policy functions of liability

2.1 Public policy considerations regarding AI

Public policy questions regarding AI start with basic questions like whether it should be applied at all and, if so, in which sectors. This is the realm of regulatory law. Liability law can help to attain an optimum welfare when new technologies are introduced. From an economic perspective, liability rules are an instrument for internalising risks, thereby generating incentives for a beneficial use of IT (outlined under 3.). Liability rules are therefore *one* element of a legal framework for AI.

2.2 The knowledge problem underlying the regulation of new technologies

The background of the discussion about the risks of AI is a considerable knowledge problem: The current developments in information technology are innovative technologies, and different actors (developers, users, affected persons, legislators and judges) have different knowledge about the associated risks. The law has to deal with these information asymmetries. Even more, the available knowledge about these technologies is still in the process of development (for example with regard to the explainability of learning systems). Product liability accepts the development risks defence according to Art. 7 (e) Directive 85/374/EEC when a risk is yet unknowable based on the state of scientific and technical knowledge. In this context, strict liability can be a useful instrument of technology risk control under uncertainty.

The dynamic development of technology and the fact that technological innovations create knowledge asymmetries is a key problem of technology law which can be interpreted as the legal framework for the development, diffusion, and application of specific technologies.[4] Through direct and indirect influences technology law strives to create an optimum of risks (potential damages) and opportunities (potential benefits). Due to the knowledge problem, indirect interventions like liability rules are often more successful than direct ones.

3 Which liability rule should be chosen? Negligence versus strict liability and the role of product liability

Liability law plays an important role as an instrument of indirect risk control with regard to the development and use of artificial intelligence.[5] The aim is to find the optimum level of risk from an economic point of view when using the new technologies. This does not mean avoiding damages at any price. Risks should be accepted where the balance of risks and corresponding opportunities leads to a maximum overall welfare. The following is an overview of two different basic legal principles of risk management, which differ in their incentive effect: negligence liability and strict liability.[6] Product liability is shown to be a de facto negligence liability.

[4] *Zech* [17], pp. 4-6.

[5] *Wagner* [13], pp. 27, 30-31.

[6] A detailed account of these effects can be found in *Shavell* [7], pp. 257-279; *Cooter/Ulen* [2], pp. 175-215; *Wagner* [12].

3.1 Negligence liability

Negligence liability (fault-based liability) is arguably the default principle in all member states.[7] Requiring the breach of a duty besides damage and causation, it acts as an instrument for influencing the level of care. Fault-based liability may be avoided if the necessary level of care is observed. In addition, it creates incentives for potential victims to avoid damages if possible.

Influencing the level of care: Fault-based liability only steps in if the person (or persons) causing damages has (have) not observed the due level of care. This provides an incentive to observe the due level of care, but nothing more. The level of care is set by duties of care which are ultimately determined by the judiciary. The determination is based on an assessment which takes into account the potential social benefits of a conduct as well as its risks. As a result, the judiciary determines which level of risk appears acceptable. An optimal risk level can only be determined in this way, however, if the judiciary has sufficient risk knowledge. Although the judicial determination of the permissible risk level is more flexible than a legal provision could be, the problem remains that state actors are likely to have less technological and thus risk knowledge than developers and manufacturers. For a technology that is still in the course of development, the knowledge of these private actors should therefore be made fruitful in determining where the optimum of opportunities and risks lies. One way of doing this, as will be shown later, is through strict liability. From the point of view of the technology users, a judicial provision ultimately means less legal certainty. This is aggravated by the fact that there is a risk of hindsight bias when deciding on specific cases.

Influencing the behaviour of potential victims: Fault-based liability entails a further incentive effect, namely an incentive for those affected (third parties or even users) to take care of avoiding damage themselves. Where manufacturers and operators behave in accordance with their duties and are therefore not liable, the persons affected bear potential damages themselves (sometimes called general risk of living). Consequently, the persons affected have an incentive to do what they can to avoid such damages, which presupposes, however, that they have the possibility of avoiding the damages. The incentive effect therefore fails in the case of novel technologies about which the average person affected has no risk knowledge. The same applies (or the effect is aggravated) when there are no options for avoidance, as is the case with ubiquitous systems from which one cannot escape in everyday life. As a result, fault-based liability in many new technologies leads to fostering technologies at the expense of those affected. This has notably been the case in the early phase of industrialization. Today, however, it seems unacceptable, not only because of concerns about justice, but also because it can ultimately result in a lack of acceptance of technology. The risks of new technologies are not part of the general risk to life.

Hardships for those affected can be countered by simply setting the duties of care very high. If such a high level of duties of care is assumed, the existing fault-based liability for certain areas, such as new technological risks, approaches strict liability. This, however, raises competence concerns (shift of regulatory competence from the

[7] *Wagner* [13], pp. 27, 33.

legislative to the judicial branch) and leads to legal uncertainty, particularly in the case of new technologies for which there is as yet no established case law. From an incentive point of view, this would be detrimental for innovation. If we do not want to unnecessarily hinder the development and introduction of useful new technologies, the greatest possible legal certainty should be ensured. A second problem is that there are many development risks associated with rapidly evolving new technologies. In the case of development risks which are yet unknowable based on the state of scientific and technical knowledge, fault-based liability fails. There is no duty to avoid the unknowable. However, it would be sensible to hold those liable who are closest to the development and who are best able to foresee the emerging risks, so that an incentive is created to acquire the necessary risk knowledge. This idea is, among others, the basis of strict liability.

3.2 Strict liability

In order to legally cope with the risks associated with artificial intelligence or current digital systems, the introduction of strict liability rules is being discussed, especially for high-risk AI systems.[8] Strict liability not only influences the level of care but also the activity level by fully internalising economic risks of AI, thereby activating private risk knowledge. It also incentivises the further development of existing technologies and, arguably, helps public acceptance. Strict liability may also be used as an instrument for risk-distribution, especially when combined with compulsory liability insurance (third party insurance). However, like any liability rule, it only works when a proof of individual causation is possible.

Additional influence on the level of activity: Strict liability assigns the economic risk to the injurer regardless of whether the injurer behaves in accordance with existing duties or not, i.e., it internalises the risk completely (at least to the extent that the damage is compensable). The risk controller must therefore consider whether the expected benefit of an activity exceeds its risk. If it is not worthwhile, the risky activity will not be carried out. By delegating the assessment to the technology developers and users (i.e. the manufacturers and operators), private risk knowledge is made available.[9] This makes sense especially in the case of new technologies, in respect of which the state – whether as legislator, executive or judiciary – has considerably less risk knowledge than the manufacturers and operators. In the case of private users (consumers) who have no specific risk knowledge, this rationale does not apply.

Incentive for further development: There is also another important incentive effect of strict liability: it provides an incentive to further develop technologies to make them safer. As long as technology users are not able to assess the risk with sufficient reliability, they will refrain from using the technology. At the same time, however, they have an incentive to further develop the existing technology until it is safe

[8] Proposal for a Regulation of the European Parliament and of the Council on liability for the operation of Artificial Intelligence-systems, European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), Annex to the resolution: Detailed recommendations for drawing up a European Parliament and Council Regulation on liability for the operation of Artificial Intelligence-systems.

[9] *Wagner* [12], p. 1444: "Erschließung privater Risikoinformationen".

enough for use. This presupposes that the liable party is able to further develop the technology. Manufacturers are not always identical with developers. However, there will be contractual relations, especially patent licencing agreements, which allow internalisation effects to be passed on.

Societal acceptance of new technologies: A third effect of strict liability regulations is that, with a complete internalisation of risks, the acceptance of the technology by the public might be increased. Liability regulations thus facilitate the introduction of new technologies and contribute to the promotion of technology.

The most important argument *against* the introduction of strict liability is that it could have a deterrent effect and, as a consequence, inhibit innovation. However, the above considerations show that strict liability only requires the technology users to assess whether they want to use the technology or not; it does not prohibit the use of the technology. Compared to a direct intervention by regulatory law, it thus represents the better (less restrictive) alternative, since such an intervention might even have to be a ban – if the state cannot decide otherwise due to a lack of its own risk knowledge and the precautionary principle. Of course, smaller interventions are also conceivable, such as a ban subject to permission, which, however, still requires a certain amount of risk knowledge on the part of the state. Strict liability is thus a regulatory instrument that makes it possible to deal with a situation of uncertain risk assessment and to proceed from the fundamental freedom to apply technology ("freedom-emphasising uncertainty rule"[10]). Strict liability is the liability for actions that are fundamentally desired by society, and for which the appropriate incentives should be provided. It is, of course, important that strict liability is structured in such a way that it can be applied with legal certainty and that there is clarity about the existing liability risks. In particular, clear prerequisites and clear legal consequences must be defined. Maximum liability limits, with which the insurability of the liability risk can be ensured, contribute to a situation where the internalised risk is calculable for technology users.[11] A clear, calculable liability prevents unnecessary deterrent effects.

One problem of strict liability rules from the injured party's point of view is that they – like any liability rule – require causation. Here, the injured party can be helped by shifting the burden of prove and assuming causation for certain high-risk activities. However, due to the increasing connectivity, situations may arise where distant contributors (e.g. by supplying faulty data) cannot be detected. In cases where an immediate causal person acting in accordance with duties of care can be determined (e.g. the operator of a damaging hardware component), while a more distant contributor acting in breach of duty is not held liable, strict liability may result in an incentive for lower levels of care for the distant parties. In such scenarios, consideration must be given to going beyond strict liability.

3.3 Product liability as a de facto negligence liability

Product liability is of special interest for the European legal debate since it is a fully harmonised area of law (Directive 85/374/EEC). Although product liability does not

[10] *Spiecker gen. Döhmann* [8], p. 137, 152: "freiheitsbetonende Unsicherheitenregel".

[11] *Spindler* [10], p. 125, 137.

expressly require negligence, the defect requirement entails negligence of the producer. Product liability, therefore, can be seen as a de facto negligence liability.[12] Moreover, the burden of proof is not shifted completely, since defectiveness has to be proven by the injured party.[13] As a consequence, to the existing product liability the same public policy rationales apply as to negligence liability.

4 Who should be held liable? Liability should follow risk control

4.1 Singling out individuals causing the damage

The effects of liability rules described above depend on clear causation. Only where one or more individuals causing the damage can be determined, liability rules can have an effect on their behaviour. If a person is liable who cannot influence the risk, or, if a person who can influence the risk cannot be determined, liability rules fail. Therefore, it is important to look at how the technological developments described above influence who is in control of the resulting risks.

Admittedly, strict liability combined with a compulsory third party insurance may be used as an instrument for evenly distributing the risk among the liable parties. This does not require full risk control and may be seen as a rationale for strict liability in its own right. As an example, strict liability for car owners which exists in some member states (like Germany) mainly acts as an instrument for risk distribution, not risk mitigation. However, with IT systems such a combination of strict liability and third-party insurance for the owners or operators of certain IT systems might be more difficult to implement due to the sheer number of such systems in the future. Moreover, if it only encompasses immediate causation and not more distant causal systems due to a lack of provability (as described above) it may lead to severe adverse incentive effects. The insurance might become too costly while operators of distantly causative systems or distantly causative agents, like data suppliers, are not affected (hence creating unchecked negative externalities).

4.2 The shift from user to producer, the concept of operator

Looking for the optimum liable party, the shift in risk control has to be taken into account. Risk control is a result of causation, risk knowledge and the ability to change the causative behaviour (choosing the level of activity, choosing the level of care). With regard to IT systems, risk control is increasingly shifted from the user to the producer (e.g., drivers become passengers).[14] This is a result of automation where the end user, apart from the decision to use a system or not, has no further options to influence the risk. In a completely digitalised world, even the decision not to use IT systems becomes increasingly difficult.

[12] *Wagner* [14], p. 726; *Wagner* [13], p. 35-36; cf. *Mazzini* [4], pp. 245, 259-263.

[13] *Mazzini* [4], p. 245, 263-264.

[14] *Wagner* [13], pp. 27, 37-39; *Patti* [5], pp. 190, 198-199.

An important concept in liability law is the definition of an operator or several operators of a system. By definition, an operator is someone who has a certain degree of risk control. With respect to IT systems, a distinction between backend operators and frontend operators has been suggested.[15] This concept was adopted by the European Parliament Resolution.[16] A frontend operator, according to the definition given in the Resolution, is a natural or legal person who exercises a degree of control over a risk connected with the operation and functioning of the AI system and benefits from its operation.[17] A backend operator, in contrast, is a natural or legal person who, on a continuous basis, defines the features of the technology, provides data and essential backend support service and therefore also exercises a degree of control over the risk connected with the operation and functioning of the AI system. As a consequence, the role of producers with an increased amount of risk control may well amount to being a backend operator (if it were not for the exception made with respect to product liability described in the next paragraph).

4.3 Consequence: strict producer liability should at least complement strict operator liability

As a consequence of the increased risk control exercised by producers, strict liability for high-risk IT systems should primarily fall to producers.[18] Operator liability could be assumed for commercial actors, but not for consumers as operators (due to a lack of control).[19]

Quite recently, the European Parliament proposed a "Regulation on liability for the operation of Artificial Intelligence-systems" containing a strict liability for operators but proposed only (arguably) minor amendments to the existing product liability (software as a product, reversal of burden of proof in certain cases).[20] Although it envisages a joint liability for backend and frontend operators, producers might fall outside the scope of the Regulation. This is due to the definition of operators: Art.

[15] European Commission, Report from the Expert Group on Liability and New Technologies – New Technologies Formation, Liability for Artificial Intelligence and other emerging digital technologies, pp. 39-42.

[16] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), para. 12.

[17] The additional requirement of benefiting from the operation reflects well the idea of fully internalising the risks as well as the benefits of a certain activity. However, the question remains if it makes sense to exclude a person fully in control of a risk from liability on the grounds that the person does not benefit. In a situation of full risk control, it is almost unthinkable that the person should not be able to at least indirectly benefit from the activity. In the case of technology-related risks this is also ensured by patent law.

[18] *Wagner* [13], pp. 27, 47; *Wagner* [14], p. 738; *Zech* [15], pp. A100-101.

[19] *Zech* [15], p. A101.

[20] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), para. 8: "[The European Parliament] urges the Commission to assess whether the PLD should be transformed into a regulation, to clarify the definition of 'products' by determining whether digital content and digital services fall under its scope and to consider adapting concepts such as 'damage', 'defect' and 'producer'; is of the opinion that, for the purpose of legal certainty throughout the Union, following the review of the PLD, the concept of 'producer' should incorporate manufacturers, developers, programmers, service providers as well as backend operators; calls on the Commission to consider reversing the rules governing the burden of proof for harm caused by emerging digital technologies in clearly defined cases and after a proper assessment [. . .]".

3 (d) of the proposed Regulation defines: "'operator' means both the frontend and the backend operator as long as the latter's liability is not already covered by Directive 85/374/EEC".[21] Although, in principle, frontend operators encompass producers, due to the exception of frontend operators whose liability "is already covered" by the Product Liability Directive, producers might be excluded. This would be the case if "already covered" is understood in a general sense, namely as regarding the scope of application. If, however, it is understood in a concrete sense, as whether a concrete damage is covered by product liability or not, there would still be room for strict liability.

In contrast, the introduction of a genuine strict liability for producers for clearly defined cases of high-risk systems within the product liability regime should be considered. A strict liability for operators of high-risk AI systems should only be introduced for operators with special expertise (operators whose main business purpose is the operation of digital systems).[22]

5 Beyond individual attribution: (first party) insurance solutions

As already discussed, causation is a necessary prerequisite for liability. An increasing level of interconnectedness ("infrastructure robotics"[23]) might lead to situations where it is no longer possible to prove that *a particular* system is responsible. Even if one hardware component directly causing the physical damage could be singled out, the attribution of responsibility to the manufacturer or operator of this system alone might create the wrong incentives for the persons responsible for other systems (components of the infrastructure) more remote and more difficult to prove being causal. In such situations, a third basic legal principle of risk management might step in, requiring neither breach of duty nor individual causation: first party insurance in the form of compensation funds or a genuine accident insurance for certain types of IT-related accidents.[24]

From the victims' point of view, the decisive difference is that it is no longer necessary to prove that a specific injurer caused the damage. Instead, it is sufficient that the damage was caused by a source covered by the insurance (which could be a catalogue of clearly defined high-risk IT systems). This would have the advantage of ensuring a high level of social acceptance for the new technologies. Such an insurance would be financed by a system of contributions, whereby the circle of contributors could be determined in a similar way to that of strict liability (i.e. according to abstract

[21] Proposal for a Regulation of the European Parliament and of the Council on liability for the operation of Artificial Intelligence-systems, European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), Annex to the resolution: Detailed recommendations for drawing up a European Parliament and Council Regulation on liability for the operation of Artificial Intelligence-systems, B. Text of the proposal requested.

[22] *Zech* [15], p. A101.

[23] *K. Mainzer*, public lecture on 5 October 2015, University of Passau: "Infrastrukturrobotik".

[24] An analysis of the advantages and disadvantages is given by *Borges* [1], p. 159-163. See also *Zech* [15], pp. A105-A110; *Wagner* [14], pp. 740-741.

risk control). A positive effect for contributors would be that the insurance scheme replaces liability, rendering contributors exempt from liability.

However, the idea of a liability-replacing insurance is also subject to objections. If the incentive effects of liability are lost, moral hazards loom. However, an effective incentive structure can also be created through redress and contribution adjustment. Although the challenge then arises again of proving that a particular actor has caused an accident in breach of duty, the insurer (in contrast to a consumer being the victim of an AI-related accident) as a party to the proceedings would be on a par with professional technology users.

6 Final remark: no hinderance – liability and technological innovation

As already pointed out, strict liability rules do not have to be seen as a hinderance for technological innovation but rather as technology friendly instruments of risk control. The same can be said for the briefly mentioned accident insurance, ensuring a level playing field for the providers of IT systems (and especially high-risk AI) in the EU.

As an outlook, three points shall be raised: First, the idea of internalising risks and benefits also points to an interconnection between liability and IP protection: Risk internalisation should be in parallel with the internalisation of positive effects through patent law. This does not only apply to producers and operators of IT systems, but also to suppliers of data.[25] Whereas property and access rights to data have been broadly discussed, liability of data suppliers and the potential need for clarifying or even limiting this liability are still in demand of a thorough examination.

Second, liability is also connected to transparency: Transparency obligations of technology users as an alternative to liability may only affect overall risks if third parties are able to avoid the risks (the same goes for transparency and autonomy of individuals). However, transparency obligations may also help with problems of provability and therefore complement liability rules.[26]

Third, there is a link between transparency and IP which also bears on liability: IP protection may act as a counterbalance for transparency obligations. In this respect, limited disclosure to authorities may also be a solution.[27]

Liability and insurance are important elements for creating a legal framework which ensures an optimal balance of benefits and risks. Safety and security, transparency and IP are other important stones in the mosaic. The EU has assumed a leading role in developing the resulting picture which is still far from being complete.

[25] *De Franceschi/Schulze* [3], p. 1, 13

[26] The same applies to logging obligations, cf. European Commission, Report from the Expert Group on Liability and New Technologies – New Technologies Formation, Liability for Artificial Intelligence and other emerging digital technologies, pp. 47-48.

[27] Cf. European Commission Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and Robotics, COM(2020) 64 final, p. 9: "One way of tackling this challenge would be imposing obligations on developers of the algorithms to disclose the design parameters and metadata of datasets in case accidents occur." Cf. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), para 18.

Funding Note Open Access funding enabled and organized by Projekt DEAL.

References

1. Borges, G.: New Liability Concepts: the potential of insurance and compensation funds. In: Lohsse, S., Schulze, R., Staudenmeyer, D. (eds.) Liability for Artificial Intelligence and the Internet of Things. Nomos, Baden-Baden (2019)
2. Cooter, R.B. Jr., Ulen, T.: Law and Economics, 6th edn. Pearson, Harlow (2014)
3. De Franceschi, A., Schulze, R.: Digital revolution – new challenges for law: introduction. In: De Franceschi, A., Schulze, R. (eds.) Digital Revolution – New Challenges for Law (2019)
4. Mazzini, G.: A system of governance for Artificial Intelligence through the lens of emerging intersections between AI and EU law. In: De Franceschi, A., Schulze, R. (eds.) Digital Revolution – New Challenges for Law (2019)
5. Patti, F.P.: Autonomous vehicles' liability: need for change? In: De Franceschi, A., Schulze, R. (eds.) Digital Revolution – New Challenges for Law (2019)
6. Schweitzer, H., Peitz, M.: Ein neuer europäischer Ordnungsrahmen für Datenmärkte? NJW, Neue Jurist. Wochenschr. **2018**, 275–280 (2018)
7. Shavell, S.: Foundations of Economic Analysis of Law. Belknap Harvard, Cambridge/London (2004)
8. Spiecker gen. Döhmann, I.: Rechtliche Begleitung der Technikentwicklung im Bereich moderner Infrastrukturen und Informationstechnologien. In: Hill, H., Schliesky, U. (eds.) Die Vermessung des virtuellen Raums (2012)
9. Spiecker gen. Döhmann, I.: Zur Zukunft systemischer Digitalisierung – Erste Gedanken zur Haftungs- und Verantwortungszuschreibung bei informationstechnischen Systemen. Computerrecht **2016**, 698–704 (2016)
10. Spindler, G.: User Liability and Strict Liability in the Internet of Things and for Robots. In: Lohsse, S., Schulze, R., Staudenmeyer, D. (eds.) Liability for Artificial Intelligence and the Internet of Things. Nomos, Baden-Baden (2019)
11. Teubner, G.: Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten. Arch. Civ. Prax. **218**, 155–205 (2018)
12. Wagner, G.: Haftung und Versicherung als Instrumente der Technikgesteuerung. Versicher.r., VersR **1999**, 1441–1452 (1999)
13. Wagner, G.: Robot liability. In: Lohsse, S., Schulze, R., Staudenmeyer, D. (eds.) Liability for Artificial Intelligence and the Internet of Things. Nomos, Baden-Baden (2019)
14. Wagner, G.: Verantwortlichkeit im Zeichen digitaler Technologien. Versicher.r., VersR **2020**, 717–741 (2020)
15. Zech, H.: Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung? Gutachten für den 73. Deutschen Juristentag. C.H. Beck, München (2020)
16. Zech, H.: Liability for autonomous systems: tackling specific risks of modern IT. In: Lohsse, S., Schulze, R., Staudenmeyer, D. (eds.) Liability for Artificial Intelligence and the Internet of Things. Nomos, Baden-Baden (2019)
17. Zech, H.: Life sciences and intellectual property: technology law put to the test. Z. Geist. Eigentum/Intellect. Prop. J. **7**, 1–14 (2015)