External conformity assessment procedures for high-risk AI-systems: A legal analysis and game theoretical considerations[1]

Mona Winau, Florian Klaus Kaiser, Marcus Wiens, Frank Schultmann, Indra Spiecker gen. Döhmann

Introduction

With its proposal for a Regulation laying down harmonized Rules in Artificial Intelligence (in the following draft AI Act)[2], the EU Commission follows at least to some extent the regulatory concept of the existing unionwide legal framework in product safety law. This concept was implemented with the so-called "New Approach" in 1985, concretized and developed into an overall concept of European conformity assessment procedures and finally put into directly applicable law with the "New Legislative Framework" (NLF), effective in 2010.[3] Existing product safety law that applies to AI systems remains unaffected next to the new regulation.[4]

Due to union product safety law framework the conformity assessment procedure is designed to preventatively ensure compliance of products with the relevant regulations. The procedure can be carried out by officially notified private actors (notified bodies).[5] The concept of shifting the performance of public tasks to private institutions that in turn are supervised by state authorities[6] potentially saves resources and allows the use of the notified bodies' specialized expertise.[7] But at the same time it bears the risk that the public interest of product safety may be overridden by

---

[1] This contribution was written at the KASTEL Institute of Information Security and Dependability at the Karlsruhe Institute of Technology, https://www.kastel.kit.edu/english/index.php.

[2] COM (2021) 106 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206 (22.11.21). All further references are made in regard to the AI Act if not otherwise declared.

[3] In detail to the development of the "New Approach", *Gärtner*, Die Haftung der Benannten Stelle für Medizinprodukte, 2021, 5 pp; cf. for the integration into the NLF-legislation, COM (2021) 206 final, Expl. Mem. 1.2; *Roos/Weitz*, MMR 2021, 844 (848).

[4] COM (2021) 106 final (fn. 1), Expl. Mem. 1. 2.

[5] *Wagner*, JZ 2018, 130 (134).

[6] Cf. in regard to various constellations of organizational or task privatization with a broad understanding of the term, *Burgi*, Funktionale Privtaisierung, 1991, 71 pp.

[7] *Gärtner*, (fn. 3), 2021, S. 10 f.

economic interests.[8] In contrast to public institutions, private stakeholders usually act profit-oriented, which means they depend on an economic line of action even if their tasks serve the purposes of public law. While they perform the conformity assessment procedure in the public interest of product safety, they act as entrepreneurs towards the providers as their costumers, whose interests they want to serve in the best possible way in their own profit interest.

To ensure the effectiveness of the conformity assessment procedure to protect users and other affected individuals from risks due to AI systems, despite expected conflicts of product safety on the one hand and economical objectives on the other hand, there is a need for effective regulation of notified bodies and their action. This may be accomplished by the means of private liability (private enforcement) [9] and administrative fines (public enforcement) for conformity assessment procedures which do not comply with the notified bodies' duties in the sense of a negative incentive regulation. This paper examines the framework of the draft AI Act for notified bodies with regard to their hedging function for securing the public product safety purposes of conformity assessment. Particular attention is paid to the sanctioning of non-compliant conformity assessment procedures. First, it describes the regulatory framework of the external conformity assessment procedure briefly (I.), then it analyses possible union law sanctions for non-compliance of notified bodies with the draft AI Act, taking into account the ECJ jurisprudence on third-party liability under the Medical Device Directive (II.) and the possibility of private third-party liability under German law referring to the relevant decision of the German highest civil court (BGH) and jurisprudential literature due to medical device safety law (III.) A game-theoretical analysis of the ideal strategies of the actors concludes that sanctioning would be a relevant factor a development of the market in the area of conformity assessments taking account of the product safety purposes.

I. The Regulatory Framework of the External Conformity Assessment Procedure

Under the proposed AI Act, prior to placing a high-risk-AI system[10] on the market or putting into service it must pass a conformity assessment procedure (Art. 19). The successful completion of this procedure must be shown by the attachment of an CE marking of conformity attached to the AI system (Art. 49 I)[11]). The conformity assessment procedure may be carried out internally by the providers of an AI system themselves or externally by a notified body, insofar as it does not concern certain products for which a conformity assessment procedure has already been ordered by specific European product safety law (Art. 43 III). According to Art. 43 II, Annex III No. 1 the external procedure is only mandatory for AI systems intended to be used for the real-time and post remote biometric identification of natural persons (remote biometric identification systems).[12] The external

---

[8] Cf. *Wagner*, (fn. 5), 134 f. More generally on possible conflicts of interest in the involvement of private actors, *Nietsch/Osmanovic*, ZIP 2020 (47), 2316 (2326).

[9] Cf. *Rott*, NJW 2017, 1146 (1147); *Gärtner,* (fn.3), 160; *Wagner*, (fn. 5), 132 referring to the ECJ decision on competition law in the Courage case, ECLI:EU:C:2001:465 Rec. 27. See also contributions to instruments of private enforcement in other areas of law, *Schmolke*, NZG 2016, 721; *Purnhagen*, LMuR 2021, 155; *Law/Vincent* (eds.), Public and Private Enforcement of Consumer Law – Insights for Luxembourg, 2021.

[10] High risk AI systems are legally defined pursuant to Art. 5. In more detail on the classification, *Bomhard/Merkle*, RDi 2021, 276 (280); *Ebert/Spiecker gen. Döhmann,* (fn. 10), 1190; *Roos/Weitz*, (fn. 3), 845.

[11] With the CE marking of conformity the provider declares that the AI-system complies with all harmonized legal requirements, Art. 30 III VO (EG) 765/2008, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32008R0765 (29.12.21). In more detail to the CE marking, Schucht, NJW 2019, 1335 (1336).

[12] And only if, in order of prove conformity with the provisions of Title III, Chapter 2, harmonised standards pursuant to Art. 40 or subsidiary common specifications pursuant to Art. 41 have not been (fully) implemented. So too *Ebert/Spiecker gen. Döhmann*, (fn. 10), 1191.

procedure is carried out by conformity assessment bodies notified by notifying authorities, whose organization and form of action are not defined by the regulation. Taking into account considerations of German law, the better arguments speak in favor of assuming a private law activity of the notified body in the public interest of product safety. Although it would be conceivable in principle for notified bodies to act under public law in form of a so-called entrustment, the lack of enforcement powers vis-à-vis providers of AI systems, their subordination to the notifying authority and the obligation under Art. 33 (8) to take out liability insurance, which would not be necessary for public institutions, speak against entrustment.[13]

The external conformity assessment procedure is set out in Annex VII of the draft regulation. The main purpose of the procedure is to examine and assess whether the AI system is in conformity with the requirements set out in Chapter 2 of Title 3 of the regulation. Subject of this examination and the assessment are the quality management system the provider must put in place according to Art. 17 (Annex VII No. 3) and the technical documentation of the system according to Art. 18 (Annex VII No. 4). The procedure also includes the surveillance of the approved quality management system after the AI system has been placed on the market or put into service (Annex VII No. 5).

There are certain procedural and organizational requirements for notified bodies from Chapter 4 of the regulation that shall secure a diligent performance of the notified body in accordance with public safety interests.

Member States are obliged to designate or establish a notifying authority or to designate a national accreditation body according to Regulation (EC) No 765/2008 due to Art. 30 (1). Notifying authorities are competent for notification and long-term surveillance of conformity assessment bodies. Condition for notification is that the applicant conformity assessment body fulfils the requirements set out in Art. 33. Such are for instance a quality management system of the body itself or organizational and procedural warranties for its independence, objectivity, and impartiality of its activities (Sec. 2-4).

Notified bodies must disclose all relevant documents to a competent supervisory authority due to Art. 33 (12). If there are suspicions or information that a notified body no longer fulfils the legal requirements, the competent notifying authority or even the Commission (Art. 37) is obliged to investigate the matter diligently and, if appropriate, to restrict, suspend or withdraw the notification (Art. 36). The possibility of surveillance by the notification authority is further served by the fact that the notified body must inform about certain activities, including the approval of quality management systems and the issuing of certificates (Art. 46).

For carrying out the conformity assessment procedure, Art. 43 (1 lit. b) refers to Annex VII. The latter specifies the assessment program, contents of the EU declaration of conformity and surveillance duties for the notified body. The body is, for instance, obliged to examine every intended change to the quality management system (Annex VII No. 3.4) or to the AI system itself and to carry out period audits (Annex VII No. 4.7) to ensure that the conformity is permanently maintained.

With these procedural safeguards, the Commission has already integrated certain instruments for securing a conformity assessment procedure which meets the public product safety purposes. There are also sufficiently defined concrete legal duties for implementation of the conformity assessment including the surveillance duties in Annex VII. However, because of the economic interests of notified

[13] Cf. the detailed discussion on a souvereign action of notified bodies, *Gärtner*, (fn. 3), S. 118 ff. Agreeing in result, *Beyerbach*, GesR 2015, 522 (525).

bodies the effectiveness of this concrete program of duties will essentially depend on the consequences of their violation as will be shown.

I. Sanctioning of a non-compliant conformity assessment practice

As a consequence of a non-compliant assessment practice, the notified body may be ordered to remedy the breach, or, if appropriate, restrict, suspend or withdraw the notification (Art. 36 (1); 37 (4)). However, a threat of an administrative fine for non-compliance by notified bodies is expressly provided for in the regulation only in case of incorrect, incomplete, or misleading information to authorities pursuant to Art. 71 (5). In any case, the proposal does not explicitly provide for a private law liability.

Sanctions for breaches of the regulation are generally regulated by Art. 71. Pursuant to Section 1, the Member States are obliged to set out effective, appropriate, and dissuasive penalties.[14] The wording of Art. 71 (1) expressively refers to "penalties, including administrative fines". From this it follows the opening clause includes administrative fines as well as private law liability. In contrast to the specific threats of fines in Section 3 and 4, the wording is also not restricted to non-compliance of an AI system, but it applies to all infringements. Therefore, member states can also create sanctions in the event the conformity assessment procedure is not carried out in accordance with the regulation, in particular with the provisions from Annex VII.

Whether a third-party private law liability of notified bodies results from the purpose of the regulation is to be answered on the basis of the ECJ decision referring to the PIP-case[15] and the following debate on individual protection and third-party liability referring to conformity assessment procedures in legal science.[16]

ECJ jurisprudence referring to individual protection in medical product safety law

In a preliminary ruling procedure, the ECJ answered questions about third party liability of notified bodies under private law for breaches of their duties following from the Medical Device Directive and about the presumed individual protection by those legal duties. The reason for the decision was a revision process in the German highest civil court (BGH)[17] concerning a legal dispute between a harmed patient who had received deficient breast implants made of industrial silicone and the TÜV Rheinland as competent conformity assessment body. Because the provider got insolvent, the harmed patient demanded compensation from the notified body due to insufficient surveillance of the implant-provider.[18] The ECJ stated that for notified bodies concrete obligations of product-surveillance follow from the Direction (Rec. 38 ff) and that those also serve the protection of end-users from deficient products (Rec. 51 ff). However, the ECJ did not conclude from this legal setting a liability of notified bodies vis-à-vis harmed third parties for a breach of their surveillance duties (Rn. 55 ff). Instead, such a liability in the opinion of the ECJ could be derived from the applicable national law of the member states, insofar as the liability is based on its own foundations for instance on culpability (Rec. 59). Assuming an union law obligation for the Member States following from the obligation to implement „effective, appropriate and dissuasive penalties" according to the union law

[14] This is a standard clause of European law, Gärtner, (fn. 3) 56.
[15] ECJ C-219/15, ECLI:EU:C:2017:128.
[16] Cf. from the jurisprudential literature *Beyerbach*, (fn. 13), 522; *Wagner*, (fn. 5), 130; *Gärtner*, (fn. 3); *Nietsch/Osmanovic*, (fn. 8), 2316; *Rott*, (fn. 9), 1146; *Brüggemeier*, JZ 2018, 191.
[17] Order for reference, 4 April 2015, VII ZR 36/14 = NJW 2015, 2737. For a summary of the lower court decisions, see *Brüggemeier*, (fn. 16), 192 p.
[18] Summarising the facts, *Beyerbach*, (fn. 13), 523.

principle of effectiveness for Member States to create such liability in national law is also excluded by the decision.[19]

The ECJ's differentiation between the individual protective character of Union law on the one hand and the question of liability for breaches of those norms on the other hand is criticized as incoherent with prior ECJ decisions and in the result inappropriate by numerous jurisprudential authors.[20] Despite this, in substance quite convincing, criticism, according to Art. 267 AEUV the ECJ's interpretation of Union law is binding for national court decisions.[21] For interpretation of a prospective AI Act the ECJ-decision referring the Medical Device Directive has to be observed insofar it is applicable.

The statements regarding the individual protective character of the relevant provisions concerning the conformity assessment procedure specifically relate to the Medical Device Direction so, despite conceptional parallels in European product safety law, they cannot be directly transferred to other legal acts. As individual protective character of union law regulations concerning the conformity assessment procedure is to be examined based on the content and purposes of the legal provisions in question.[22]

Regarding the finding that it does not necessarily follow from the individual protective character of individual provisions of directives that there is a subjective right of the person harmed by the infringement of these provisions, the ECJ refers to its earlier jurisprudence[23] (Rn. 55). From this and from the general expression of the court without any reference to the Medical Device Directive can be deduced that this principle may be applied at least to other legal product safety acts.[24]

Lastly, private third-party liability of notified bodies for the violation of individual protective Union law depends on the conditions of the national legal system.[25] Even if the duty program for notified bodies following from Annex VII is protective, there is no liability under Union law of the notified body vis-à-vis third parties harmed by the non-compliant AI system. The fact that such a liability may result from national law already follows from the regulatory mandate to the Member States due to Art. 71 (1).[26]

II. Third party liability of conformity assessment bodies under German law

If Member States do not create specific liability regimes for notified bodies towards harmed individuals of high-risk AI systems, their liability will depend on general national private law provisions. Depending on the applicable law, this may result in a complex legal situation and the liability may depend on the circumstances of the individual case. An illustrative example of this is the situation under German law.

---

[19] *Gärtner*, (fn. 3), 83; *Wagner*, (fn. 5), 131 p.
[20] *Gärtner*, (fn. 3), 83 ff; *Wagner*, (fn. 5), 133 pp; *Rott*, (fn. 9), 1147; *Brüggemeier*, (fn. 16), 196; dissenting *Nietsch/Osmanovic*, (fn. 8), 2318 f.
[21] *Ehricke, Streiz*, EUV/AEUV, Art. 267 Rn. 6.
[22] *Nietsch/Osmanovic*, (fn. 8), 326.
[23] ECJ, 12 October 2004, C-22/02, ECLI:EU:C:2004:606.
[24] Cf. *Gärtner*, (fn. 3), 84; *Wagner*, (fn. 5), 132; probably also *Brüggemeier*, (fn. 16), 194.
[25] If a claim in tort is asserted, the law of the state where the damage occurred is generally applicable pursuant to Art. 4 I Rome II Regulation. A change in the liability situation for the notified body through a choice of law clause is ruled out due to the lack of a contractual relationship with affected individuals.

[26] Dissenting probably *Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter*, RDi 2021, 528 (536).

For assessment whether the notified body bears liability because of an infringement of individual-protective provisions of the draft AI Act towards third parties harmed by an incompliant AI system, the BGH decision[27] that followed the preliminary decision procedure can be used. In addition, the numerous existing reviews of third-party liability by means of medical device product safety law in the jurisprudential literature[28] can be referred to. In the following, possible bases of claims and still open legal questions will be presented briefly and reviewed for their transferability to third party liability under the draft AI Act.

The injured individual may have a claim based in particular on liability arising from the contract between the notified body and the manufacturer with a protective effect for the benefit of the user and on claims in tort arising from Section 826, 823 (2) of German Civil Code (BGB) in conjunction with Articles 33 (1), 43 (1), Annex VII of the draft AI Act and Section 823 (1) BGB.

1. Liability under the principles of the contract with protective effect in favor of third parties

Liability under the principles of the contract with protective effect in favor of third parties captures constellations of contractual primary or secondary obligations that are also related to a third party. Those obligations also serve to protect a third party that is not party to the contract and is not able to derive any rights from the contract.[29] Whether there are such third party related obligations is to be determined by means of supplementary interpretation of the contract based on the hypothetical intention of the contracting parties.[30] This hypothetical intention is assumed provided that the third party is affected by the contractual service as intended and in a comparable manner to the receiving contracting party (so-called Leistungsnähe).

The recipient in turn must have a legitimate interest for involving the third party into contractual protections (so-called Gläubigernähe). The group of potentially involved third parties must be identifiable for debtors so their risk of liability remains appropriate. Finally, involved third parties be deemed worthy of protection which means they cannot claim damages due to another equivalent basis.[31]

The BGH denied the liability of the conformity assessment body based for an infringement of its contractual duty to conduct the conformity assessment procedure lawfully with a protective effect in favor of the end users because the lacking interest for involving the end users into contractual protection. In addition, the court already questioned an affection of end users comparable to the recipient. In the literature, the denial of the protective effect in favor of end users of the contract between the notified body and the provider is assessed in two ways.[32]

As the consumers themselves do neither intentionally nor factually come directly into contact with the conformity assessment of a product and a breach of duty by the notified body poses a health risk to them while the provider is at risk of pecuniary damages even the proximity to contractual service (Leistungsnähe) is in doubt.[33] In any case, the provider cannot be assumed to be interested to involve the end user into contractual protections. Even though there can be assumed the provider's general interest of protection of the end users, the objective of them conducting the conformity assessment

[27] BGHZ 225, 23.
[28] Cf. fn. 16.
[29] *Gottwald*, in: Säcker/Rixecker/Oetker/Limperg (eds.), MüKo BGB, 8. Ed. 2019, § 328, Rec. 180 p.
[30] BGHZ 225, 23, Rec. 21 f; a.A *Bayer*, JuS 1996, 473; *Gottwald*, (fn. 29), § 823 Rec. 170 pp.
[31] *Gottwald*, (fn. 29), § 328 BGB, Rec. 184 pp; *Janoschek*; in: Hau/Poseck (eds.), BeckOK BGB, 60. Ed. 2021, § 328 Rec. 54 pp.
[32] Summarizing the opinion in Science and with further references *Gärtner*, (fn. 3), 136.
[33] BGHZ 225, 23, Rn. 24, agreeing *Gärtner,* (fn. 3), 139.

is limited to fulfilling the requirements for market access. Thus, there is no hypothetical will of the provider for involving the end users.[34] Also, the interest for involvement cannot result from the principles of expert liability (so-called Expertenhaftung).[35] Those principles cover constellations in which, despite opposing interests of recipient and third, the service is based on a special expertise and is important for both parties recognizably so there is an interest of involving the third party into contractual protection.[36] Such a constellation does not exist regarding the notified body because it only applies its expertise to the assessment of products in contractual relationship with the provider and the assessment does not appear externally to the end[i] consumers.[37]

The relationship between notified body, provider and affected third parties due to the draft AI Regulation is, in accordance with European product safety law, [38] comparable to the constellation in medical device law, so the principles of the court can be transferred substantially. Neither does an affected individual damaged by the AI system come into contact with the conformity assessment procedure directly nor are they at risk of incurring pecuniary damages in case of an unlawful assessment practice by the notified body like the provider does. Accordingly, neither the proximity to contractual service (Leistungsnähe) nor the provider's interest of involvement of affected individuals (Gläubigernähe) can be assumed. Also, the fact that the provider and not the notified body is responsible for the conformity of products (Art. 16) supports this reasoning. The positive outcome of the conformity assessment procedure will also be, if at all, recognizable to users and affected individuals by the placement of the CE marking (Art. 49). When remote biometric identification systems are used, it must be assumed that affected individuals usually cannot see the CE marking. In any case, the service of the notified body itself is not visible for others than the provider. Therefore, in accordance with the observations of BGH there is no basis for involving third parties into the contractual protection between the provider and the notified body. Finally, there is no liability of notified bodies according to the principle of the contract with protectional effect in favor of a third party.

2. Tort Liability of Conformity Assessment Bodies

Tort liability on the basis of § 826 BGB requires intentional immoral damage. Thus, its scope of application is limited to exceptional cases which will not be considered in detail here. Establishing tort liability based on § 823 (1) and § 823 (2) BGB in connection with the infringement of a protective law (so-called Schutzgesetz) is more likely.

As a more specific basis for claims, tort liability based on § 823 (2) BGB in conjunction with the notified bodies' duties from Art. 33 (1), 43 (1), Annex VII draft AI Regulation will be considered first.

For violations of the notified bodies' duties with regards to the conformity assessment procedure of medical devices, such a claim for violation of protective legislation has been affirmed on the merits by the Federal Court of Justice and is also predominantly affirmed with regard to the Medical Devices Ordinance that has since come into force.[39] A first prerequisite for such a liability is the individual protectional character of the violated provisions (so-called Schutzgesetze) regarding the conformity assessment procedure. Regarding medical devices safety law, this could already be taken up with reference to ECJ jurisprudence.

---

[34] BGHZ 225, 23, Rec. 25 p; arguably critical *Gärtner,* (fn. 3), 144.
[35] BGHZ 225, 23, Rec. 27, agreeing *Gärtner*, (fn. 3), 143 p.
[36] With further references *Janoschek*, (fn. 31), § 328 Rec. 67.
[37] BGHZ 225, 23, Rec. 28; different view, but agreeing in the result, *Nietsch/Osmanovic*, (fn. 8), 2320.
[38] so too *Roos/Weitz*, (fn. 3), 848.
[39] BGHZ 225, 2, Rec. 31 pp; summarizing the opinion in Science and with further references, *Gärtner,* (fn. 3), 150 p.

The individual protectional character of the specific obligations of notified bodies arising from Art. 33 (1), 43 (1), Annex VII must be examined on the basis of its regulatory purposes.[40] Individual protectional law is every legal provision which, due to its content and purpose, is also intended to protect individuals from violation of specific rights.[41] There must be an individual protective effect of the provision. The resulting liability must fit in the entire system of liability so it can be assumed that the legislator's intention was at least to also create a liability in case of a culpable infringement of the individual protective legal provision.[42]

The purpose of the AI Regulation is to improve the conditions of the free internal market by laying down harmonized legal provisions as well as the warranty and enforcement of public interest, such as health protection, safety, and free exercise of fundamental rights (Rec. 1). Protection should also be provided against material and immaterial damages and harms that may occur from AI systems to other interests and rights protected by Union law (Rec. 4).[43] While individual protective purposes cannot be derived directly from the improvement of competitive conditions,[44] it is almost evident regarding the designated public interests and individual rights. The intended protection applies to individuals affected by the risks of AI systems. The conformity assessment procedure as a mandatory prerequisite serves the individual protection just of those affected third parties (cf. Rec.27). Even if the provider itself is reliable for product safety,[45] there are the aforementioned specific procedural safeguards and provisions for the assessment process arising from Annex VII just for the purpose of securing a compliant conformity assessment procedure meeting the public product safety interests.[46] The external conformity assessment procedure in particular is intended to guarantee a higher degree of product safety (cf. 64). From this it follows that the specific provisions arising from Annex VII, which the notified body must meet due to Art. 33 (1), 43 (1), are intended to protect individuals affected by the AI system against risks for health, safety, free exercise of fundamental rights and other rights protected by Union law. They are therefore individual protective legal provisions.

A liability based on the culpable violation of the obligations arising from Art. 33 (1), 43 (1), Annex VII by the notified body must fit in the entire system of German liability law so it can be assumed the legislator would have wanted to regulate such liability.

Concerns arise whether the liability risk of the conformity assessment body is compatible with the principle of proportionality. The potentially damaged individuals should be a definable group of persons.[47] The group of potentially affected and damaged persons by an AI system depends on the respective application context. Remote biometric identification systems in particular may affect an undefined number of persons without common features. However, it should be kept in mind that the lawful use of such AI systems in public spaces is limited to exceptional cases due to Art. 5 (1) lit. d.[48]

---

[40] For conformity assessment procedure to be carried out in accordance with another Union legal act (Art. 43 III), the procedure is modified to the effect that the requirements of the AI Act for high-risk systems are to be reviewed in the procedure and specified provisions apply accordingly to it. In this case, it must be examined whether the disregarded obligation resulting from the applicable Union legal act is protective law.

[41] *Förster*; in: Hau/Poseck (eds.), BeckOK BGB, 60. Ed. 2021, § 823 Rn. 276; BGHZ 186, 58, Rec. 18.
[42] *Förster*, (fn. 41), § 823 Rn. 276, 278.
[43] *Grützmacher* therefore assumes the protectice nature of many of the draft's provisions, CR 2021, 433 (438 pp).
[44] Vgl. *Nietsch/Osmanovic*, (fn. 8), 2326.
[45] Cf. with regard to the overall Union law approach to conformity assessment, *Gärtner,* (Fn. 3), 14.
[46] Different view with regard to the protective function of notified bodies under medical device safety law, *Beyerbach*, (fn. 13), 525 p; *Brüggemeier*, (fn. 16), 193.
[47] *Wagner*, in: Säcker/Rixecker/Oetker/Limperg (eds.), MüKo BGB, 8. Ed. 2020, § 823 Rn. 564.
[48] See in more detail on the, however limited, scope of the exemptions, *Ebert/Spiecker gen. Döhmann*, (fn. 10), 1189 p; *Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter*, RDi 2021, 528 (531).

Another argument against compatibility with the German liability system is that according to product liability law the provider is also liable vis-à-vis all affected individuals. Beyond that, the liability based on the infringement of individual protective legal provisions requires the provider's culpability.[49]

The justification for this third party liability with the aid of medical device safety law and the otherwise occurring asymmetric liability[50] also applies, perhaps even especially, with regard to the draft AI Regulation. The conformity assessment body as a private actor is liable under contract law for pecuniary losses including lost profits which may follow from an overly strict assessment practice vis-à-vis the provider. In particular with regard to the conformity assessment procedure on the basis of the abstract and risk-based provisions in the draft AI Regulation and the high complexity of AI systems[51] this poses a real danger to the provider. The conformity assessment body, for instance, must investigate and assess whether the used data for training, validation and testing are "relevant, representative, free of errors and complete" (Art. 10 (3)) so that it must concretize these specifications for each application context in a first step. In any case, as long as there are no harmonized standards (Art. 40) and common specifications (Art. 41) or other sector-specific concretizations available for the respective application context, there will be a great deal of uncertainty for the notified bodies about the interpretation of the requirements with which they have to assess compliance. And even with such specifications notified bodies will still dispose of a wide margin of appreciation,[52] whose judicial review is limited by a proportional interpretation and application of the regulation.

If an AI system is wrongfully assessed as non-compliant with the applicable legal provisions and does not get a conformity certificate, the notified body may be held liable for pecuniary losses the provider suffers, for instance, due to the delayed market entry in case of negligence. If, however, there is no third-party liability for the reverse case, i.e., the notified body unlawfully assesses an AI system as in conformity with the regulation, this results in an asymmetric liability. This leads to incentives for notified bodies to adapt their interpretation of assessment standards in order to favor providers' interests over the public interest of high product safety standards. Such an asymmetric liability situation is therefore contrary to the purpose of the conformity assessment.

Finally, third party liability of notified bodies according to § 823 (2) BGB in conjunction with Art. 33 (1), 43 (1), Annex VII of the draft AI Regulation is possible on the merits. Whether a claim exists in detail depends essentially on whether there has been a culpable infringement of specific individual-protective obligations by the notified body and whether there is a sufficient causal connection between the damaging event and the existence of the damage. Practical enforceability of such a claim in turn depends on the rules on the burden of proof and the factual possibilities of proof for affected individuals. As the analysis of liability issues that arise in this context concerning medical device safety law shows, the third-party liability of notified bodies in German law largely depends on the circumstances of the individual case.[53]

---

[49] Vgl. *Wagner*, (fn. 5), 135; *Gärtner*, (fn.), 159. In contrast *Beyerbach* rejects liability due to the delimited risk, (fn. 13), 525; so too *Brüggemeier*, (fn. 16), 194.

[50] BGHZ 225, 23, Rec. 43; *Gärtner*, (fn. 3), 88; 160; *Wagner*, (fn. 5), 135 p; critical *Nietsch/Osmanovic*, (fn. 8), 2320.

[51] Doubts about the effectiveness of private assessments due to the high complexity of AI-Systems are also expressed by *Ebert/Spiecker gen. Döhmann*, (fn. 10), 1191.

[52] Argue in this direction also *Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter,* RDi 2021, 528 (533).

[53] Vgl. *Gärtner,* (fn. 3), 173 pp; *Nietsch/Osamnovic*, (fn. 8), 2321 ff. With regard to AI Systems additional problems of causality and proof already arise for the provider's liability from the complexity and constant change of the technical processes, *Grützmacher*, CR 2021, 433 (435).

Third party liability of conformity assessment bodies based on § 823 (1) BGB is predominantly recognized as possible if a notified body violates safety duties (so-called Verkehrssicherungspflichten) going beyond the obligations arising from the regulation as guarantor (so-called Garantenstellung). This is, again, a question of the specific individual case which in turn entails the aforementioned problems of causality, enforcement and proof.[54]

III. Sanctioning as an effective Instrument for Safeguarding the Regulatory Purposes

Without specific liability provisions for conformity assessment bodies, as becomes clear from the consideration of the German legal situation, the liability situations depend significantly on terms and valuations of the respective applicable national liability law. In contrast to the opaque and case-by-case liability regime in German tort law the situation in French law is much clearer and easier for affected individuals due to an applicable general liability clause which even comprises pecuniary loss.[55] This results in legal uncertainty for providers of AI systems in the internal market. Also, there is a risk that in situations of asymmetric liability due to national law the effectiveness of the conformity assessment procedure cannot be adequately ensured because of the private liability incentives that conflict with objectives of protection of public law.

How the implementation of private third-party liability in combination with hypothetical administrative fines affects economic incentives for notified bodies is examined using the following game-theoretical model. The players in the game are n companies U (providers), and j private conformity assessment bodies B, as well as a representative user, who only influences the interaction in an indirect way. The objective or profit function of one of the n providers is:

$$G_U = \theta \cdot p - c + (a - k_U)x$$

The variable θ represents the probability that the user uses the product, p is the selling price, and c is the fee for conformity assessment procedure (regardless of the outcome of the test). The variable $x \in \{0,1\}$ is the firms' binary strategy variable, where $x = 1$ represents regulation compliant production and $x = 0$ represents non-compliant production. k_U is a scaling factor representing the production cost of a system that is conform with the regulatory specifications. The parameter a captures the degree of intrinsic motivation of the providers. Providers thereby occur in two types. A proportion α is intrinsically motivated to produce products that are conform to the regulation, for example by a strong sense of duty. For this motivated firm type, $a^H \geq k_U$ holds, consequently this group will always choose $x = 1$. The corresponding complementary share $(1 - \alpha)$ has no intrinsic incentive to produce conform systems ($a^L < k_U$) and will therefore choose $x = 0$. The profit function of the conformity assessment body notified for certification is as follows:

$$G_B = c + (b - k_B)y$$

The notified body receives the fee c for a certification and can then examine conscientiously ($y = 1$) or neglect the examination and issue a "courtesy certificate" instead ($y = 0$). A conscientious assessment incurs a cost according to the scaling factor k_B. The notified body can either be conscientious with probability β ("reliable type") or violate its mandate with the opposite probability $1 - \beta$ ("unreliable type"). The difference between these two types depends on the dutifulness parameter a. For the reliable type, $b^H \geq k_B$ holds, i.e., for this type $y = 1$ is optimal, and for the

[54] Cf. restraining *Nietsch/Osmanovic,* (fn. 8), 2323 pp.
[55] *Gärtner*, (fn. 3) 95 pp.

unreliable type, $b^H \leq k_B$ holds and thus vice versa $y = 0$ is the optimal strategy choice. The two types are a priori indistinguishable neither for the providers nor for the users.

We start the analysis by asking which type of the provider would be willing to have its product assessed (or choose not to enter the market) and at what price. To do this, we first need to determine θ, i.e. the probability that the user will buy and use the offered system from the provider, which in turn varies depending on how much the user trusts the CE marking.[56] Let θ^H be the probability that the user will buy the product, with $\theta^H = \beta + (1-\beta)\alpha$. However, the user also knows that a certificate was issued by either a reliable or an unreliable conformity assessment body. With probability β, the notified body was reliable and the user can trust on the certificate. With probability $1-\beta$, this was an unreliable conformity assessment body that only issues "courtesy certificates", but this is not a problem if the audited provider was nevertheless conscientious (which is the case with probability α). How much would each type of the provider be willing to pay for certification? For the dutiful provider, the critical fee for a certificate is easily determined. Since it always acts in a compliant manner, we need only compare the expected revenue from certification ($\Delta\theta p$ or $\beta(1-\alpha)p$) with the cost (of the fee c): For $\beta(1-\alpha)p \geq c$, the dutiful provider will always vote for certification; however, if the fee were larger than the left-hand side of the inequality, then certification would be too costly even for a dutiful provider (in which case no market would emerge). The opportunistic provider has two choices with respect to certification. It can behave non-compliantly and hope that the notified body will assess the conformity unreliably (certification is worthwhile in this case for $(1-\beta)\Delta\theta p \geq c$) or it accepts the cost of compliant behavior with the advantage that it will then receive the certificate in any case, regardless of the type of authority (certification is worthwhile in this case for $\Delta\theta p \geq c + k_U - a^L$). The opportunistic provider chooses compliant behavior for $\beta \geq \frac{k_U - a^L}{\Delta\theta p}$. Thus, the probability of notifying a dutiful conformity assessment body must exceed the critical threshold on the right-hand side of the inequation.

It can be quickly seen from the inequation derived above that the dutiful provider would always be willing to accept a higher price for the assessment procedure, since it gains more in expected value from the assessment procedure than an opportunistic provider. If we assume a single conformity assessment body, this leaves the conformity assessment body with two options: It can either set a high price at which just all dutiful providers are indifferent or it can set the price so low that the opportunistic providers become indifferent. In the first case, one obtains a so-called *separation equilibrium*, since in this case only dutiful providers let their products be assessed and then receive their certificate in any case. Non-conform products would therefore be efficiently excluded from the market. In a separation equilibrium, the user can therefore always trust a certificate 100%. In the second case, however, there is a so-called *pooling equilibrium*, since the provider types are no longer distinguishable for the user. For the condition $\beta \geq \frac{k_U - a^L}{\Delta\theta p}$ already stated above, the regulation and the assessment practice by the notified body will make all opportunistic providers produce conform products. In this case, all providers have a certificate, but they are also rightfully issued (regardless of whether they receive it from a reliable or unreliable conformity assessment body). For $\beta < \frac{k_U - a^L}{\Delta\theta p}$, there is only one possible assessment price at which the opportunistic providers are non-compliant and try to obtain the certificate by hoping that the notified body is unreliable. In this case, the pooling equilibrium is problematic because, although all providers can show a certificate, only a fraction α offers conform products.

[56] Although, the CE marking does not contain any reliable information about the conformity of the product its absence nevertheless has a comparable factual effect on users, *Schucht*, (fn. 11), 1336.

Yet, in the proposed game, several private conformity assessment bodies are observed. It follows that there will be price competition among these conformity assessment bodies and that they will not be able to freely set the price of certification. In the emerging price competition between conformity assessment bodies, a price for the conformity assessment procedure at marginal cost will thus be established. However, since reliable conformity assessment bodies have higher marginal costs than unreliable conformity assessment bodies, the conformity assessment bodies that operate reliably would be forced out of the market. In this case, certification would lose its signaling effect. The users could now no longer trust the certificate and be unable to distinguish the products of the different providers. In this case, certification under the high-risk-AI would be circumvented.

With the existence of third-party liability under tort law or administrative fines, the calculation of the conformity assessment bodies is adjusted. Thus, in addition to the known profit function, a factor is added that describes the risk of sanctioning an incorrect certification (certification of a non-conform product) as well as the liability claims:

$$G_B = c + (b - k_B)y - (1 - y)(1 - \alpha)(h_B + s_B)\vartheta$$

The risk of certification describes that in the case of issuing a "courtesy certification" $(1 - y)$ and in the case that the certified product is not compliant with the regulation $(1 - \alpha)$ a third party liability claim h_B as well as a administrative fine risk s_B arises. ϑ describes the probability of a notification of the conformity assessment body. For simplicity, it is assumed here that both liability claim and fines are always asserted. The initial price disadvantage of the dutiful notified body can thus be counteracted by the introduction of sanctioning measures and liability measures. Which of the conformity assessment bodies will prevail on the market is a question of the level of sanctions or the level of third-party liability claims. Both conformity assessment bodies could stay in the market if $c \geq (1 - y)(1 - \alpha)(h_B + s_B)\vartheta$ holds. Accordingly, in the case that $c < (1 - y)(1 - \alpha)(h_B + s_B)\vartheta$ holds, only conformity assessment bodies acting dutifully would offer the conformity assessment. The notified body would reject non-conforming products or refuse certification to them if the expected costs (liability claims as well as sanctions) of a " courtesy certification " exceed the equivalent value of the certification. When comparing the effect of liability claims and sanctions, it can be distinguished that these have a different effect in the sense that they influence the probability of notification in different ways. Although the user is obliged to monitor the system pursuant to Art. 29 IV, it must be noted that liability claims only have an influence on the probability of notification if the (affected) users can identify the non-conformity of the AI systems and thus detect false certifications issued by the conformity assessment body. On the other side, administrative fines contribute to the financing of official authorities supervising the conformity assessment bodies (Art. 37) and carrying out the post market monitoring of the AI systems (Art. 63). With low observability of the conformity of the product even after its purchase by the user, administrative fines are more efficient in establishing a market for products that are conform with the regulations. Conversely, liability claims work more effectively when the observability of the product's conformity after purchase by the user is high as each user would have an interest in notifying an unjustified certification.

IV. Conclusion

The legal and economic analysis have shown that sanctioning in the form of a private law liability or administrative fines are an important regulatory instrument to ensure that the procedure is carried out diligently in the public interest of product safety. Both the private and the public law enforcement instruments can be more effective from the perspective of regulation through market incentives for notified bodies depending on the density of official and private post-market monitoring of AI systems. Despite comprehensible criticism on the implementation of private law liability to limit a conflict of interest that follows from the delegation of assessment task to private

actors in general,[57] due to the limited resources of public authorities it should be considered as an additional regulatory instrument. While in view of the new technical changes a broad debate in liability for damages following from the use of AI systems is already taking place[58] and a corresponding unionwide legal framework is still to be enacted,[59] there is a lack of attention to the older discussion on the effectiveness of the conformity assessment procedure without fines and private law liability of notified bodies under Union law which could be important to avoid such damages.

---

[57] *Nietsch/Osmanovic*,(fn. 8), ; similar *Beyerbach*, (fn. 13), 526 p.

[58] cf. *Hofmann*, CR 2020, 282; *Beckers/Teubner,* Three Liability Regimes for Artificial Intelligence: Algorithmic Actants, Hybrids, Crowds, 2022; *Bartneck/Lütge/Wagner/Welsh*, Responsibility and Liability in the Case of AI Systems, in: Bartneck/Lütge/Wagner/Welsh (eds.), An Introduction to Ethics in Robotics and AI, 2021, 39 – 44; *Grützmacher,* (fn. 43), 433.

[59] Cf. The European Parliament resolution with recommendations to the Commission in a civil liability regime for artificial intelligence, (2020/2014(INL)), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html#title1 (29.12.21); to this *Etzkorn*, CR 2020, 764; and the Report from the Commission to the Parliament, COM(2020) 64 final , https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0064 (30.12.21); *Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter,* (fn. 26), 536.