Chapter 5: Suggestions for De Lege Ferenda

A. Placing Dangerous Products on the Market as an Endangering Offence

The numerous *ex ante* and *ex post* challenges faced in determining liability in crimes involving AI-driven autonomous systems, particularly those arising from the principle of guilt, the establishment of causality, and the identification of the exact cause, have been explored throughout this study. To overcome these issues, prevent liability gaps, and promote the safe development of AI-driven systems, a noteworthy suggestion has been put forward by *Hilgendorf.*

In criminal law, the concept of strict liability (*Gefährdungshaftung*) is incompatible. However, abstract or concrete endangerment offences (*Gefährdungsdelikt*) may be envisaged for the manufacturers of AI-driven autonomous systems' manufacturers. To be specific, as an abstract endangerment offence, criminal provisions could be established for placing dangerous products on the market without adequate safety measures, with the occurrence of harm being an objective condition of punishability (*objektiver Bedingung der Strafbarkeit*). The condition could be an occurrence of bodily harm or significant property damage[1908]. This approach would provide strong motivation for manufacturers to develop AI-driven systems securely and to conduct the necessary safety checks diligently[1909]. *Hilgendorf* also emphasises that it is necessary to debate whether such a regulation is truly required, given that criminal law serves as an *ultima ratio*[1910].

Under such a regulation, the manufacturer of any AI-driven autonomous system causing bodily harm would not automatically be held liable; rather, liability would be limited to those who place such systems on the market without adequate safety measures or without subjecting them to sufficient testing. However, the mere act of placing an inadequately tested product on the market would not, in itself, be sufficient for criminal liability. In addition, there must be a violation of a legal interest, such as bodily harm, significant property damage, or other interests deemed significant by the

[1908] HILGENDORF, Robotik, Künstliche Intelligenz, Ethik und Recht, 2020, p. 555-556.

[1909] HILGENDORF, Autonome Systeme, 2018, p. 111.

[1910] HILGENDORF, Robotik, Künstliche Intelligenz, Ethik und Recht, 2020, p. 556.

legislature, which serve as objective conditions for punishability[1911]. In this context, the challenges in attributing negligence are addressed, as proof of a breach of due care is no longer required. Instead, the mere occurrence of the result is considered sufficient[1912].

A similar regulation was proposed in the 1971 draft of the German Criminal Code. According to this proposal, risks arising from mass production and insufficiently tested products were to be mitigated through the introduction of a certification system. According to the draft provision of the StGB-AE (*Alternativ-Entwurf*)[1913], marketing serially manufactured medicinal products without approval (or a corresponding inspection decision) from the relevant testing agency has been regulated as an abstract endangerment offence. Therefore, it is not required that harm or concrete danger to human health should also occur; not obtaining a certificate from the relevant testing agency is considered sufficient for liability[1914]. In addition to this intentional offence, the provision further stipulates that withholding or failing to report essential information regarding the approval process and violating conditions set by the authority on the labelling, usage instructions, and shelf life of the drug are crimes as well as committing these acts negligently.

This regulation both enables control over the distribution of potentially dangerous products and protects those who comply with it to avoid the risk of criminal prosecution, albeit with certain limitations. Besides, it is stated that this criminal offence structure shows the benefits of abstract endangerment offences, as strict reliance on injury-based offences can be ineffective, as seen in the challenges of the *Contergan* trial[1915]. Products that pass testing are not entirely harmless; however, the risk of mass harm is at least significantly reduced[1916]. Furthermore, compliance with Section

[1911] Indeed, abstractly dangerous behaviour does not always cause a hazardous outcome, and a concrete danger does not always ultimately result in a violation of the protected legal interest. MITSCH, Das erlaubte Risiko, 2018, p. 1163.

[1912] FATEH-MOGHADAM, Innovationsverantwortung, 2020, p. 885.

[1913] Original text of § 155 titled "Vertrieb ungeprüfter Arzneimittel" (Sale of untested medicinal products): "(1) Wer serienmäßig hergestellte Arzneimittel ohne Freigabe durch die Arzneimittelprüfstelle im Rahmen eines Gewerbebetriebes in Verkehr bringt, wird mit Freiheitsstrafe bis zu fünf Jahren bestraft." Alternativ-Entwurf eines Strafgesetzbuches Besonderer Teil: Straftaten gegen die Person, 2. Halbband, Tübingen: Mohr, 1971, p. 11.

[1914] HORN, Erlaubtes Risiko, 1974, p. 719 ff.

[1915] *Ibid*, p. 720 ff.

[1916] *Ibid*, p. 722.

155 of the AE does not absolve the manufacturer of all liability in every circumstance. In line with the explanations regarding permissible risk[1917], fulfilling a specific duty does not automatically equate to satisfying the general duty to refrain from causing harm[1918]. However, if a pharmaceutical manufacturer complies with Section 155 and adheres to the required duty of care, they are exempt from liability for damages that may still arise during the distribution of the drug[1919].

Undoubtedly, *ex-post* evaluations of certain behaviours that lead to specific outcomes can provide statistically empirical data. For example, it is well-documented that driving under the influence of alcohol significantly increases the likelihood of accidents. Building on this, it is worth considering shifting criminal liability from the actual occurrence of harm to the presumed dangerous behaviour itself, particularly for certain actions identified as potential causes of loss or harm, to protect significant legal interests. This approach results in the establishment of endangerment offences[1920]. In particular, emerging technologies such as AI, which can potentially violate legal interests on a large scale and whose risks remain inadequately understood, pose significant dangers when deployed without proper testing, as in the case of self-driving vehicles. Employing the tools of criminal law and the deterrent effect of punishment to discourage such risky behaviours ensures a more effective protection of legal interests[1921].

Abstract endangerment offences are effective in ensuring protection within modern, complex environments without infringing upon constitutional rights or disproportionately impacting individuals. Criminal law can adapt and evolve to stabilise behavioural norms and address the risks posed by new technologies and dangerous products[1922]. Nevertheless, although abstract endangerment offences are regarded as an effective tool serving the preventive function of criminal law, they are criticised for departing from traditional criminal law principles. Therefore, they should be incorporated into criminal law only in exceptional cases where their necessity and pro-

[1917] See: Chapter 4, Section C(5)(c): “The Feasibility of Defining Permissible Risk Through Standards and Other Norms of Conduct”.

[1918] HORN, Erlaubtes Risiko, 1974, p. 725.

[1919] *Ibid*, p. 735 f.

[1920] MITSCH, Das erlaubte Risiko, 2018, p. 1163; SINGELNSTEIN, Preventive Turn Wie Gefahr, 2020, p. 99-102. See also: SCHÖMIG, Gefahren und Risiken, 2023, p. 136.

[1921] KUDLICH, Gefahrbegriffe, 2020, p. 122.

[1922] REUS, Das Recht in der Risikogesellschaft, 2010, p. 186 f.

portionality can be clearly justified[1923]. Certainly, penalising risky behaviour reduces individual freedom within the social sphere[1924].

Indeed, to avoid the challenges of assessing negligence in duty of care violations, lawmakers may criminalise certain behaviours as endangerment offences. Thus, prevention through criminal law involves altering the classic offence structure by introducing abstract endangerment crimes. The elimination of requirements such as actual harm, causality, and objective imputation simplifies proving and increases the likelihood of sanctions, compared to traditional structures[1925]. This approach could be increasingly applied in robotics, even potentially making the mere operation of a robot under certain predefined (adversarial) conditions punishable[1926]. However, a careful balance of interests must be maintained, and in some cases, penalisation may be necessary to uphold social norms. When lesser measures are insufficient to fulfil this duty, the state must employ criminal punishment, particularly for serious violations affecting significant legal interests such as human life, in order to fulfil its constitutional duty of protection[1927].

Nevertheless, it must be remembered that criminal law serves as *ultima ratio*. Civil or administrative law solutions, or self-regulation obligations, often better achieve legislative goals. However, due to its perceived efficiency; criminal law is frequently treated as a master key and rapidly applied to regulate technology[1928]. It should be borne in mind that this principle emphasises that criminalisation should be a last resort, used only when no other means can achieve the intended goal. It also highlights the risk of over-regulation driven by populist demands or media pressure[1929].

In this regard, one perspective advocates for the introduction of a special criminal product liability, broadly defined, through the imposition of administrative offences for violations of the technical standards outlined in the EU AI Regulation (AI Act). Similar to European antitrust law, the adoption of a framework based on the collective responsibility of companies is suggested. This would prevent companies from evading liability by refer-

[1923] HASSEMER, Sicherheit, 2006, p. 137; IBOLD, Künstliche Intelligenz und Strafrecht, 2024, p. 151, 430.

[1924] MITSCH, Das erlaubte Risiko, 2018, p. 1164.

[1925] IBOLD, Künstliche Intelligenz und Strafrecht, 2024, p. 153, 425.

[1926] MARKWALDER/SIMMLER, Roboterstrafrecht, 2017, p. 177 f.

[1927] REUS, Das Recht in der Risikogesellschaft, 2010, p. 102; Singapore, Report on Criminal Liability, 2021, p. 16, [para. 2.11].

[1928] HILGENDORF, Digitalisierung, Virtualisierung und das Recht, 2020, p. 411.

[1929] HILGENDORF, Modern Technology, 2017, p. 24.

ring to factual uncertainties. However, such measures should not be classified as punishments (*Strafen*), as this would conflict with the fundamental principles of criminal law, such as action and guilt. Moreover, it is argued that a system of fines under this approach would have a sufficient deterrent effect[1930].

On the other hand, *Hilgendorf*'s suggestion can serve as an example of the application of preventive criminal law aimed at mitigating certain significant risk factors. Thus, similar to the regulation under Section 316 of the StGB, which criminalises operating a vehicle in traffic while not being in a condition to drive safely; the marketing of AI-driven systems that do not conform to established technical standards could be addressed through this suggestion[1931]. However, the question arises as to what constitutes adequate safety measures and who will be responsible for determining and confirming them. For instance, it has been suggested that establishing an entity similar to the *Technischer Überwachungsverein* (TÜV) with a special approval procedure to monitor the technical standards and market release of such systems could be a practical solution. This entity could function as a state authority, with its operations subject to democratic oversight[1932]. However, the aforementioned concerns about such a mechanism being reduced to a mere *box-ticking* exercise must be kept in mind[1933].

Hilgendorf's proposal, which envisions placing dangerous products on the market as an endangerment offence, with the occurrence of harm serving as an objective condition of punishability, thus offers highly pragmatic and significant solutions. However, it is important to note certain reservations. It could initially be argued that having adequately tested products and implementing safety measures should be tied to objective criteria. However, this approach risks turning into a mere checklist system. Such a system may encourage companies to focus solely on fulfilling formal requirements rather than actively pursuing measures that genuinely enhance product safety and reduce dangers in specific cases. Moreover, companies might mitigate their own research efforts by over-relying on government inspections and shifting responsibility to the state. This reliance could create safety gaps, as governmental oversight cannot comprehensively address all

[1930] IBOLD, Künstliche Intelligenz und Strafrecht, 2024, p. 430.

[1931] *Ibid*, p. 144.

[1932] HILGENDORF, Autonomes Fahren im Dilemma, 2017, pp. 171-172.

[1933] See: Chapter 4, Section C(5)(c): "The Feasibility of Defining Permissible Risk Through Standards and Other Norms of Conduct".

potential risks or substitute for the proactive diligence of manufacturers in ensuring product safety[1934].

Another concern with this approach is that it would apply exclusively to AI-driven autonomous systems classified as products that are put into circulation. In this context, liability is focused solely on manufacturers, without any determination regarding the responsibility of other persons behind the machine, interacting with such machines. The fundamental issue in this context lies in the capacity of AI (-driven) systems to be produced in countless variations, facilitated by the possibilities of digital technology. Without being affiliated with any organisation, even an individual can create numerous distinct AI (-driven) systems in a short period and distribute them over the internet. Indeed, such internet bots driven by AI can be easily created and programmed to operate autonomously within social networks, offering a cost-effective and efficient alternative to traditional forms of online activity[1935]. Consequently, criminal offences involving such systems would remain unaddressed.

A further issue relates to the objective conditions of punishability. All scholarly criticisms directed at this institution are likely to extend to this regulation as well. This is because objective conditions for criminal liability refer to factual circumstances that must exist for a crime to be punishable, where the existence of such conditions suffices to establish liability irrespective of the perpetrator's knowledge or intent[1936]. These conditions are not influenced by errors concerning the factual circumstances and make criminal liability contingent upon external, non-criminal political or legal interests[1937]. Additionally, it is essential to determine which legal interests should constitute the basis for objective conditions of criminal liability. For example, will legal interests such as *privacy* be included, or, as *Hilgendorf* suggests, should the focus instead be on bodily harm or significant property damage?

Another point, which can also be directed at other criminal offences involving AI-driven systems, is that imposing liability through such endangerment offences may hinder innovation due to its restrictive nature[1938].

[1934] HORN, Erlaubtes Risiko, 1974, p. 730 f.

[1935] REINBACHER, Social Bots, 2020, p. 458.

[1936] HILGENDORF/VALERIUS, Strafrecht AT, 2022, p. 75 Rn. 114.

[1937] VOGEL/BÜLTE, § 15 Vorsätzliches fahrlässiges Handeln in LK, 2020, p. 1199 f., Rn. 313 ff.

[1938] LOHMANN, Liability Issues, 2016, p. 338 f.; OSMANI, The Complexity of Criminal Liability, 2020, p. 75.

However, it is essential that the threat of criminal sanctions serves not only to deter individuals but also to prevent corporations (individuals within), which have the potential to create far greater risks, from engaging in harmful practices. Furthermore, this presents an opportunity for legislators to clarify human responsibility by prohibiting the delegation of critical decisions (such as matters of life and death) to AI (-driven) systems or by restricting the deployment of high-risk AI technologies[1939].

B. Certain Jurisdictions Concretising Criminal (Non-)Liability For AI-Driven Autonomous Systems

Criminal liability in offences involving AI-driven autonomous systems presents significant challenges, particularly in attributing liability to a specific individual. These difficulties necessitate solutions that align with the fundamental principles of criminal law. In this context, this study sought to propose concrete solutions within the framework of negligent liability, focusing on the boundaries of the duty of care and the permissible risk doctrine. Similarly, many jurisdictions aim to address such issues using existing criminal law norms rather than enacting entirely new legislation; primarily because newly introduced laws may conflict with established legal principles and frameworks.

In this section, a brief overview of prominent laws and legislative proposals worldwide that offer alternative perspectives on the issue will be provided. However, the analysis is not conducted through a comparative law methodology and is limited to a superficial overview. These examples could serve as the basis for more specific academic studies in the future.

Singapore:

Comprehensive legislative efforts have been underway in **Singapore** since 2018 to address the potential dangers posed by AI-driven systems, both in the digital realm as software and in the physical world as hardware. To begin with the existing norm, the Singapore Penal Code of 1871, Article 287(1)[1940], titled "*Rash or negligent conduct with respect to any machinery*

For a critical assessment of endangerment offences, see: YETKIN, Cezalandırılabilirliğin Öne Alınması, 2024, p. 116 f.

[1939] FATEH-MOGHADAM, Innovationsverantwortung, 2020, p. 883.

[1940] Singapore Penal Code 1871, 2020 revised edition, 16.09.1872, https://sso.agc.gov.sg/act/pc1871?ProvIds=P414_267A-#pr287-. (accessed on 01.08.2025).

in possession or under charge of offender" is as follows: "A person shall be guilty of an offence who does, with any machinery in the person's possession or under the person's care, any act so rashly or negligently (...) [endanger human life, cause injury or death]". Nonetheless, it is noted that the term "machinery" does not encompass AI software, therefore would not be applicable for AI-driven autonomous systems[1941].

Nevertheless, noting that AI-driven systems operate not only in physical spaces, such as autonomous driving, but also in various critical digital fields, including the financial sector, electronic communication, and social media postings; and as they continue to develop, they will be employed in increasingly dynamic and unpredictable ways. Considering these potential future threats, emphasising that "no legislative amendments are immediately necessary", two criminal norm provisions were proposed in 2018 by the Singapore Penal Code Review Committee (PCRC)[1942].

Firstly, similar to Article 287, it was proposed to establish a negligent offence that also addresses computer programmes. Accordingly: *Whoever makes, alters or uses a computer program so rashly or negligently as to endanger human life, or to be likely to cause hurt or injury to any other person, or knowingly or negligently omits to take such order with any computer program under his care as is sufficient to guard against any probable danger to human life from such computer program, shall be punished (…)*"[1943] In this way, the aim is to prevent the creation of risk by developers or operators of computer programmes through negligent behaviour and to encourage greater caution[1944].

The provision further includes determinations regarding when a computer program is considered to be under human control: "(2) For the purposes of this section, a person uses a computer program if he causes a computer holding the computer program to perform any function that - (a) causes the computer program to be executed; or (b) is itself a function of the computer program. (3) For the purposes of this section, a computer program is under a person's care if he has the lawful authority to use it, cease or prevent its use, or direct the manner in which it is used or the purpose for which it is used"[1945].

[1941] Singapore, Report on Criminal Liability, 2021, p. 30 [para. 4.24].

[1942] Singapore Penal Code Review Committee (PCRC), "Report", 2018, p. 29 ff.

[1943] *Ibid*, p. 30.

[1944] Singapore, Report on Criminal Liability, 2021, p. 39, [para. 4.49].

[1945] Singapore Penal Code Review Committee (PCRC), "Report", 2018, p. 30.

Another proposed offence seeks to impose a duty on individuals who have control over a computer program to take reasonable steps to prevent or mitigate harms caused by the program[1946] is as follows: "(1) Where a computer program - (a) produces any output, or (b) performs any function, that is likely to cause any hurt or injury to any other person, or any danger or annoyance to the public, and the computer program is under a person's care, if that person knowingly omits to take reasonable steps to prevent such hurt, injury, danger or annoyance, he shall be punished. (2) For the purposes of this section, a computer program is under a person's care if he has the lawful authority to use it, cease or prevent its use, or direct the manner in which it is used or the purpose for which it is used"[1947]. In this way, the legislator imposes an obligation on individuals exercising control over computer programmes to take reasonable measures to mitigate any harm that may arise from these programmes once such harms become apparent[1948].

Regarding the recommendations of the PCRC, it has been suggested that any new legal offences should be specifically tailored to high-risk scenarios. Moreover, the laws should clearly define the responsibilities and standards expected in such situations. This approach would be more effective than introducing broad criminal negligence laws applicable to all industries and uses of AI (-driven) systems[1949].

France:

The French Road Act explicitly introduces a provision on exemption from liability. Specifically, under Article 121-1 of the French Road Traffic Act, the driver of a vehicle is ordinarily held criminally liable for offences committed while operating the vehicle. However, according to the Article L123-1[1950] (as amended on 16.04.2021), with reference to Article L121-1 the driver of a vehicle will not be criminally liable for offences committed while driving the vehicle if: the driving functions have been delegated to an automated driving system, when this system exercises dynamic control of the vehicle at the time of the offence and under the conditions set out

[1946] Singapore, Report on Criminal Liability, 2021, pp. 5-6, [para. 26].

[1947] Singapore Penal Code Review Committee (PCRC), "Report", 2018, p. 31 f.

[1948] Singapore, Report on Criminal Liability, 2021, p. 39, [para. 4.49].

[1949] *Ibid*, p. 41, [para. 4.56].

[1950] France, Code de la Route, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043371835. (accessed on 01.08.2025).

in Article L319-3[1951]. According to Article L123-1(2), the driver must always be in a position to respond to a request to take control of the automated driving system. Additionally, Article L123-2 stipulates that the manufacturer shall bear criminal liability for offenses of unintentional harm to the life or integrity of an individual caused by the vehicle when the automated driving system is exercising dynamic control, and when fault is established.

The UK:

Another suggestion was put forward by **the UK** Law Commission in 2022. They proposed that, where authorised vehicles comply with all requisite standards and the self-driving function is properly activated and operational, the individual occupying the driver's seat should no longer bear criminal liability for the dynamic driving task[1952]. Thus, a distinction in the classification of AI systems emerges between those requiring real-time human oversight and those capable of operating autonomously without such intervention[1953].

[1951] **Article L319-3**: "**I**. The decision to activate an automated driving system is taken by the driver, who has been previously informed by the system that it is capable of exercising dynamic control of the vehicle in accordance with its using conditions. **II**. When its state of operation no longer allows it to exercise dynamic control of the vehicle or when the conditions of use are no longer fulfilled or when it anticipates that its conditions of use will probably no longer be fulfilled during the execution of the manoeuvre, the automated driving system must: **1-** Alert the driver; **2-** Make a request to take control back; **3-** Initiate and execute a manoeuvre with minimal risk in the absence of takeover at the end of the transition period or in the event of a serious failure." (Translated by the author). https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043371914. (accessed on 01.08.2025).

[1952] Law Commission of England and Wales Report, Automated Vehicles: Joint Report, London: Law Commission of England and Wales (Law Commission No 404), Scottish Law Commission (Scottish Law Commission No 258), 2022, p. 77, [para. 5.46], https://lawcom.gov.uk/project/automated-vehicles. (accessed on 01.08.2025).

[1953] GIANNINI/KWIK, Negligence Failures, 2023, p. 76 f.