Chapter 2: The Occurrence of Criminal Incidents Involving AI-Driven Autonomous Systems

A. Types of Criminal Offences Likely to Emerge

Autonomous systems driven by AI may lead to harmful outcomes which could constitute offences under criminal law. Although this study primarily examines negligent liability, focusing on the unforeseen consequences that may arise from the use of such systems and the careless conduct of persons behind the machine is important; these systems may also be intentionally utilised in the commission of criminal acts[219]. Therefore, it is essential to identify which crimes are most likely to occur in connection with these systems.

The types of crimes most commonly associated with AI-driven autonomous systems include negligent bodily injury (Section 229 dStGB[220]; Article 89 of Turkish Penal Code (TPC)[221]) and negligent homicide (Section 222 dStGB; Art. 85 of TPC). In addition to those, liability for negligent endangerment of road traffic (Section 315(c)(1), (3) dStGB; Art. 180 of TPC) is conceivable[222]. It should be noted that result-based offences, such as bodily injury and homicide, require proof of causation and the actual occurrence of harm, which can complicate the process of establishing criminal liability[223].

While careless and inattentive violations of data integrity or property damage may also occur, these acts are punishable neither under German

219 SCHUSTER, Strafrechtliche Verantwortlichkeit, 2019, p. 7.

220 Penal Code of Germany, Strafgesetzbuch (StGB), enacted on 15.05.1871, last amended on 07.11.2024, https://www.gesetze-im-internet.de/stgb/BJNR001270871.html. (accessed on 01.08.2025).

221 Turkish Penal Code No. 5237, dated 26.09.2004 (Official Gazette No: 25611, 12.10.2004). For an English translation, see: Council of Europe, European Commission for Democracy through Law (Venice Commission), Penal Code of Turkey, Opinion No. 831/2015, CDL-REF(2016)011, 15 February 2016, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2016)011-e. (accessed on 01.08.2025).

222 STEINERT, Automatisiertes Fahren, 2019, p. 5.

223 SCHUSTER, Künstliche Intelligenz, 2020, p. 390 f.

nor Turkish law[224] due to the absence of provisions for the negligent forms of these offences. Similarly, insult is stipulated as an intentional offence both under Art. 125 of the TPC and Section 185 of the dStGB, and its negligent form is not subject to criminal liability. Should lawmakers in various countries criminalise the negligent form of such acts in the future, the interpretations and applications discussed for current offences would largely apply to these as well. Indeed, the decision to criminalise the negligent forms of various behaviours ultimately reflects a criminal justice policy aimed at protecting societal order; thus, legislators may decide to employ criminal law -the *ultima ratio* instrument- to encourage individuals to exercise greater caution in specific areas. Therefore, as this study aims to provide a general framework, it also includes assessments based on offences such as insult. Indeed, rather than avoiding the examination, addressing such violations is highly effective in clarifying the issue.

For instance, if an individual developed a self-learning computer program that subsequently engaged in the illegal transfer of personal data or unauthorised system access, it is likely that such acts would not fall within the scope of explicitly defined negligent criminal offences. Consequently, no criminal liability would arise in such cases[225]; however, civil liability may still be applicable. An example of this could be the software that "accidentally" purchased illegal drugs from a darknet marketplace in 2014[226]. Moreover, with the anticipated rise in the use of personal drones, concerns regarding privacy are likely to intensify. For example, a partially autonomous drone engaged in an unrelated task could inadvertently capture footage of individuals sunbathing on a private terrace, thereby violating their right to privacy[227]. Additionally, there are frequent instances in which chatbots insult users. In fact, chatbots may be involved in a range of conduct that can be committed through speech, writing, or expressions.

224 Articles 135 et seq. of the Turkish Penal Code (TPC) stipulate crimes involving the intentional infringement of personal data, while Article 151 addresses the intentional form of property damage. According to Article 22(1) of the TPC, crimes committed through negligence are punishable only if explicitly stipulated by law. Although the Venice Commission has adopted the term "recklessness" to refer to negligence in English translation, this usage is inaccurate. In English legal terminology, "recklessness" aligns more closely with the German concept of *Leichtfertigkeit*, which denotes a higher degree of disregard than (conscious or unconscious) negligence.

225 Singapore, Report on Criminal Liability, 2021, pp. 30-31.

226 POWER MIKE, "What happens when a software bot goes on a darknet shopping spree?", 05.12.2014, https://www.theguardian.com/technology/2014/dec/05/software-bot-darknet-shopping-spree-random-shopper. (accessed on 01.08.2025).

227 HILGENDORF, Recht und autonome Maschinen, 2015, p. 17.

However, offences such as insults or threats do not have negligent forms under German or Turkish criminal law. On the other hand, criminal offences such as *causing an atomic explosion via negligence*, as stipulated under Art. 173(2) of the TPC, or *espionage through negligence*, as outlined in Art. 338 of the TPC, may be conceivable in certain contexts.

Finally, it should be noted that AI-driven autonomous systems can be intentionally employed in the commission of various crimes, including financial market fraud, hacking, and other cybercrimes. In this respect, they possess no unique characteristic: any intentional crime can theoretically be committed using these systems as a tool, provided that it aligns with the nature of the crime[228].

B. Categorical Distinction of Crimes Involving Autonomous Systems

1. Various Classifications in Literature

Autonomous systems driven by AI can be involved in a criminal offence in various ways. In scholarly literature, several classifications based on different criteria have been proposed. By focusing on the role of AI systems in committing offences and taking into account different perspectives in literature, this study analyses the matter under three main categories: 1- *crimes committed through AI systems*, 2- *crimes committed against AI systems, 3- crimes caused by (with the involvement of) AI systems*. The first category refers to the utilisation of AI systems to support or increase the effectiveness of committing an offence. The second category refers to offences targeting AI systems themselves, exploiting their vulnerabilities or manipulating them in various ways. The third category, which forms the primary focus of this study, encompasses more complex scenarios in which AI systems exhibit autonomous characteristics and human control is limited or even absent.

In literature, various classifications are proposed based on AI's involvement in criminal activity. One approach categorises the matter as follows: 1- intentional crimes committed by a robot due to specific programming, 2- crimes arising from faulty programming, which bring up issues such as development risk and duty of care, 3- crimes in "dilemma situations" where robots are deliberately programmed to make a specific choice under

228 VOJTUS/KORDIK/DRAZOVA, Artificial Intelligence, 2022, p. 664.

conflicting conditions, and 4- crimes committed by a robot based on its own momentum or autonomous operation[229].

From a criminological perspective, an alternative distinction similar to the one adopted here, categorises the matter as follows: "crimes with AI", "crimes against AI" and "crimes by AI". Accordingly: crimes with AI refers to crimes where AI is used as a tool to commit the crime, crimes against AI refers to crimes targeting AI systems themselves, and crimes by AI indicate more complex scenarios, potentially without direct human instruction or control. It raises important questions about accountability and the autonomous actions of advanced AI systems[230]. Another approach adopts the same categorisation by focusing on the persons behind the machine: cases where users intentionally employ AI as a tool to commit an offence; cases where users act unintentionally but negligently; and cases arising from the AI system's complex structure or learning abilities[231].

A further opinion categorises the subject as follows: AI as an object of criminal law protection, AI as a tool in criminal activity, AI as a perpetrator of criminal activity, and AI as a source of data on criminal activity[232]. Another study makes the distinction as: misconduct of the system, misconduct of the operator, a combination of both, and the non-use of the system[233]. Other approaches also suggest that AI can either be deliberately misused to facilitate crimes or that unintended errors arising from autonomous systems may inadvertently result in criminal outcomes[234].

2. Intentional Use of Autonomous Systems to Commit a Crime

Utilising AI-driven autonomous systems facilitate and enhance the efficiency of committing an offence[235]. Even though AI systems may operate with varying degrees of autonomy and without direct human control, they can nevertheless be employed in criminal activities if their outputs

229 SIMMLER/MARKWALDER, Guilty Robots?, 2019, pp. 7-9.
230 HAYWARD/MAAS, Artificial Intelligence, 2021, pp. 214-219; ZHAO, Principle of Criminal Imputation, 2024, p. 4.
231 MÜSLÜM, Artificial Intelligence, 2023, pp. 135-136.
232 VOJTUS/KORDIK/DRAZOVA, Artificial Intelligence, 2022, p. 664.
233 WIGGER, Automatisiertes Fahren und Strafrecht, 2020, p. 129.
234 MAHMUD, Application and Criminalization, 2023, p. 9; Singapore, Report on Criminal Liability, 2021, p. 23 ff.
235 HAYWARD/MAAS, Artificial Intelligence, 2021, p. 214 ff.

are predictable or foreseeable[236]. Typically, these uses involve intentional behaviour, such as online-phishing, where AI functions similarly to any other instrument[237]. In this sense, AI facilitates new methods for committing traditional offences, such as using high-frequency trading for market manipulation[238] or deploying an autonomous drone to target a specific individual[239]. From the perspective of criminal law, this is not substantially different from using a conventional weapon or an automated system. However, a key point is that sometimes AI systems may be used directly or manipulated to serve as a tool in committing crimes. An example in this context might be instructing a robot to commit arson to an unattended factory[240]. Additionally, images and audio generated through *deepfake* technology can be utilised as tools to commit offences such as fraud[241].

3. Crimes Against Autonomous Systems

Criminal offences committed against AI-driven autonomous systems target these systems directly by exploiting their vulnerabilities or manipulating them in various ways. Such acts include tampering with or sabotaging a system to alter its functioning, causing it to generate faulty outputs, or compromising the data used to train the AI, potentially through the disclosure of confidential information or infringement of intellectual property rights. These attacks directly threaten the integrity, functionality, and security of

236 See: Chapter 4, Section B: "Intentional Liability".
237 GIANNINI/KWIK, Negligence Failures, 2023, p. 48.
238 GLASER, Künstliche Intelligenz, 2024, p. 12.
239 COTOVIO Vasco/SEBASTIAN Clare/GOODWIN Allegra, "Ukraine's AI-enabled drones are trying to disrupt Russia's energy industry. So far, it's working", 02.04.2024, https://edition.cnn.com/2024/04/01/energy/ukrainian-drones-disrupting-russian-energy-industry-intl-cmd/index.html. (accessed on 01.08.2025).
240 HALLEVY, Liability for Crimes Involving AI, 2015, p. 41.
241 Frauds committed using deepfake technology are becoming increasingly widespread. For example, in Hong Kong, an employee was deceived by a deepfake that utilised publicly available images and audio of company executives, resulting in the transfer of $25 million. TAN Huileng, "A company lost $25 million after an employee was tricked by deepfakes of his coworkers on a video call: police", 05.02.2024, https://www.businessinsider.com/deepfake-coworkers-video-call-company-loses-millions-employee-ai-2024-2. (accessed on 01.08.2025).
For a brief assessment of the risks associated with the indistinguishability of deepfake-generated content from authentic ones, see: ÖZBALCI, Ceza Muhakemesi, 2025, p. 165 f.

AI systems[242]. However, if an AI system has been used as an instrument in a crime through manipulation, such cases should be assessed within the scope of the first category (intentional crimes) outlined above.

Such attacks on AI-driven autonomous systems may compromise the system's integrity or exploit its vulnerabilities. For instance, due to the functioning methods of deep neural networks (DNNs), it is relatively easy to deceive them with minor modifications; for example, a slight alteration of a few pixels in an image of a lion could lead the system to misidentify it as a library[243]. In fact, such attacks are generally referred to as *adversarial machine learning attacks*[244] and represent a significant concern; however, they fall outside the scope of this study[245].

4. Crimes Caused by Autonomous Systems

This category, which forms the core of this study, involves more complex scenarios in which AI-driven systems operate at varying degrees of autonomy, often requiring minimal or even no human intervention or control. These cases present challenges in attributing liability to the persons behind the machine, particularly in establishing a causal link between human behaviour and AI outcomes. Such situations may arise from factors like faulty programming, issues within training datasets, or insufficient testing; but they can also result from the AI system's unpredictable interactions

242 HAYWARD/MAAS, Artificial Intelligence, 2021, p. 216 f.
The holder of rights or interests that constitute the core of an offence may be recognised as victim in criminal law. However, in this context, it may initially be more appropriate to consider AI-driven autonomous systems not as victims, but rather as entities that are protected through criminal norms. For a detailed discussion on the scope of the concept of victim in criminal law, see: KATOĞLU, Ceza Hukukunda, 2012, p. 660.

243 DEVILLÉ/SERGEYSSELS/MIDDAG, Basic Concepts of AI, 2021, pp. 9-10.
Among many examples is a project called *Ignotum*, which produced a pancho with a grid pattern designed to deceive AI-driven CCTV systems, preventing the wearer from being recognised as human. "Werteloberfell develops an AI-fooling poncho to confuse CCTV algorithms", 02.02.2021, https://www.designboom.com/design/werteloberfell-ai-fooling-poncho-to-confuse-cctv-algorithms-12-02-2021. (accessed on 01.08.2025).

244 EVTIMOV, et al., Is Tricking a Robot Hacking, 2019, p. 899 ff.

245 For a broad assessment of such attacks and whether they can be evaluated within the current criminal norms, see: KATOĞLU/ALTUNKAŞ/KIZILIRMAK, Yapay Zekâ, 2025, *passim*.

with the external environment relying on its autonomous nature. In this context, issues of foreseeability and the scope of the duty of care become central, often raising questions of potential liability for negligence on the part of the persons behind the machine. An example of this category could be accidents involving autonomous vehicles that result in loss of life[246].

From a terminological perspective, the phrase *crimes caused by autonomous systems* does not imply that AI-driven autonomous systems (despite differing opinions on the matter)[247] directly commit crimes, fulfil the *actus reus*, or serve as the immediate cause of an offence. Rather, it refers to situations where such systems play a role at some point within the causal sequence leading to a crime[248]. Typically, this occurs when the autonomous features of the system contribute as one of several causal factors leading to the offence, often in circumstances where the person behind the machine has acted negligently, such as by failing to anticipate a specific outcome. In such cases, the issue may stem from factors like flawed training data, incorrect programming, or system bugs[249] -or a combination of these factors- making it difficult to pinpoint the precise cause[250].

C. Prominent Cases Highlighting AI-Related Liability

Throughout the study, real-life incidents involving AI-driven autonomous systems are discussed under relevant sections, particularly to analyse the duty of care of the persons behind the machine. In addition, to clarify the classifications outlined above, noteworthy cases will be presented and discussed in this section, with key issues requiring further examination

246 One of the earliest examples pertinent to this issue is the 2016 Tesla accident. The incident took place because the vehicle was unable to distinguish the white sidewall of a truck from the bright sky, resulting in a collision. See: KLEIN Alice, "Tesla driver dies in first fatal autonomous car crash in US", 01.07.2016, https://www.newscientist.com/article/2095740-tesla-driver-dies-in-first-fatal-autonomous-car-crash-in-us. (accessed on 01.08.2025).
FELDLE, Notstandsalgorithmen, 2018, p. 30.

247 SWART, Constructing Electronic Liability, 2023, p. 592.

248 Zhao also uses the term "crimes involving AI" as has been adopted in this study to emphasise the role of AI in criminal activity while deliberately avoiding notions like "committed by AI". See: ZHAO, Principle of Criminal Imputation, 2024, p. 4.

249 Moreover, bugs are frequently inevitable and can sometimes emerge only years after a system's initial deployment. COOPER, et al., Accountability, 2022, p. 869.

250 COOPER, et al., Accountability, 2022, p. 864; NOVELLI/TADDEO/FLORIDI, "Accountability in AI, 2023, p. 5.

being highlighted. This approach not only allows the incidents to be situated within a specified classification but also draws attention to nuances in how these crimes occur, thereby aiding in the concretisation of the theoretical explanations that follow. Beyond the examples discussed here, further concrete cases are discussed under each section to deepen the evaluation. Nonetheless, some incidents that are assessed here will be frequently discussed in the rest of the study, with detailed explanations from this section being cited throughout.

Although numerous incidents involving AI-driven autonomous systems have been covered in the media, scarcely any cases have been brought before the judiciary in Europe that address the specific characteristics of criminal liability; such as the principle of guilt, individual criminal liability, the scope of duty of care, permissible risk, and the principle of reliance[251]. As a developing field, it is understandable and these situations can be explained by the *Collingridge dilemma*, which describes the challenge of regulating emerging technologies: early stages lack sufficient information for potential impacts, effective control and regulation; while later stages make changes difficult due to the technology's wide adaptation and entrenchment[252]. Indeed, it has been stated that despite numerous self-driving vehicle accidents in the U.S., no case has reached the criminal judiciary for a thorough examination of criminal liability[253]. This is largely because manufacturers often reach swift financial settlements with victims, avoiding legal precedents and potential damage to public trust. Additionally, prosecutors have likely refrained from pressing charges due to insufficient

251 For the same observation, see: MILDENBERGER Christian, Promotionsvorhaben an der Rheinischen Friedrich-Wilhelms-Universität Bonn, Strafrechtliche Verantwortung beim Einsatz von Künstlicher Intelligenz in der Diabetes-Therapie, https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Boese/OnlineVorlesung/Expose___KI_Diabetestherapie.pdf, p. 1 f. (accessed on 01.08.2025).

252 COLLINGRIDGE, The Social Control, 1980, p. 19 f.; IBOLD, Künstliche Intelligenz und Strafrecht, 2024, pp. 222-223.

253 As of now, there exists no case law involving a comprehensive analysis of negligence and causation similar to analysis in this study. For the few instances involving more superficial examinations, see: SMILEY Lauren, "The Legal Saga of Uber's Fatal Self-Driving Car Crash Is Over", 28.07.2023, https://www.wired.com/story/ubers-fatal-self-driving-car-crash-saga-over-operator-avoids-prison (accessed on 01.08.2025). BILLEAUD Jacques/SNOW Anita, "The backup driver in the 1st death by a fully autonomous car pleads guilty to endangerment", 28.07.2023, https://apnews.com/article/autonomous-vehicle-death-uber-charge-backup-driver-1c711426a9cf020d3662c47c0dd64e35. (accessed on 01.08.2025).

evidence of criminal wrongdoing, and civil settlements frequently prevent further legal action, given the blurred lines between civil and criminal law in the U.S.[254]. In addition, research conducted by an American legal scholar on case law involving robots indicates that most cases pertain to traditional legal areas such as contract law, criminal law, and tort law. However, the study notes that distinctive characteristics of robots, such as autonomy or emergence, have not been adequately addressed in these cases[255].

Some instances can be particularly fruitful for discussing human-machine interaction and *human in the loop*[256]. For instance, if a medical system, due to flawed training data, misidentifies tumour cells in a cancer patient and leads to misdiagnosis, inadequate treatment, and ultimately, the patient's death[257]; the role of this system in the fatal outcome must be critically examined. In my opinion, in decision-support applications such as these, the physicians who implement the prescribed treatment should, to a certain extent, oversee these results and compare them with traditional diagnostic methods. The outputs of these systems are intended to be evaluated by human professionals (considering the black-box effect), with the final decision resting with them. In this respect, it is distinct from situations involving accidents caused by self-driving vehicles.

Systems driven by AI, whether with low or high autonomy, can be intentionally utilised for criminal conduct such as mass cyberattacks and fraud involving deepfake technology[258]. For example, they can enhance spear phishing by analysing targets' online activities to craft convincing, personalised messages, enabling mass phishing attacks that raise the likelihood of deception[259]. Although cyberattacks using AI-driven autonomous systems

254 WIGGER, Automatisiertes Fahren und Strafrecht, 2020, p. 90 f.
For example, in the case of Uber's Arizona accident in 2018, public prosecutor's office stated that the available evidence did not provide sufficient evidence and therefore, there is "no basis for criminal liability for the Uber corporation". https://s3.documentcloud.org/documents/5759641/UberCrashYavapaiRuling03052019.pdf. (accessed on 01.08.2025).

255 CALO, Robots in American Law, 2016, p. 7, 40.

256 See: Chapter 4, Section C(4)(c): "Human in the Loop".

257 VALERIUS, Strafrechtliche Grenzen, 2022, p. 122 f.

258 ROBINS-EARLY Nick, "CEO of world's biggest ad firm targeted by deepfake scam", 10.05.2024, https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam#:~:text=In%20one%20high%2Dprofile%20example,investing%20%2440m%20in%202021. (accessed on 01.08.2025).

259 OpenAI, The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, Apollo - University of Cambridge Repository, 2018, doi:10.17863/CAM.22520, p. 19.

differ methodologically from fraud involving manually used deepfake contents, both represent instances of intentional crimes.

One of the most frequently cited examples in studies on the matter is Microsoft's *Tay* scandal (2016)[260]. Being a typical example of "crimes caused by AI" category, there is little need to repeat the extensive commentary on this case[261]. Nevertheless, developers' responsibilities in this context can be divided into "pre-Tay" and "post-Tay" phases, because the widespread attention given to the Tay scandal has since made it clear that chatbots with learning capacities which are open to interaction with the public are likely to adopt behaviours and language from users[262]. While this issue may have been more controversial in 2016[263]; by 2025, releasing chatbots to the public without mechanisms, such as guardrails to prevent harmful outputs arising from human interaction would definitely constitute a design flaw[264]. Therefore, it would be inaccurate to equate Grok's insults and threats directed at users in July 2025[265] with the case of Microsoft's Tay.

In a scenario where a Twitter bot was intentionally designed to insult the users interacting with it, the situation would be quite different. A comparable instance has been documented involving a *Reddit* user who configured a similar function[266]. In this case, it could be argued that the developer's actions are intentional rather than merely negligent, as the bot is programmed to insult every single user who interacts with it. The

260 DEVEAU Scott/CAO Jing, "Microsoft Apologizes After Twitter Chat Bot Experiment Goes Awry", 25.03.2016, https://www.bloomberg.com/news/articles/2016-03-25/microsoft-apologizes-after-twitter-chat-bot-experiment-goes-awry. (accessed on 01.08.2025).

261 NEFF/NAGY, Talking to Bots, 2016, pp. 4920-4923.

262 Studies on human interactions with (early) chatbots indicate that users often behave dominantly, rudely or dismissively, viewing chatbots as subordinate tools rather than equal partners. This perception reinforces the chatbot's role as a subordinate, leading to particularly different treatment compared to human counterparts. See: DE ANGELI et al., Proceedings, 2001, p. 474.

263 SINDERS Caroline, "Microsoft's Tay is an Example of Bad Design - or Why Interaction Design Matters, and so does QA-ing.", 24.03.2016, https://medium.com/@carolinesinders/microsoft-s-tay-is-an-example-of-bad-design-d4e65bb2569f#.cr899vm8b. (accessed on 01.08.2025).

264 See: Chapter 4, Section C(4)(a)(2): "Learning from Mistakes and Hindsight Bias".

265 CHAYKA Kyle, "How Elon Musk's Chatbot Turned Evil", 16.07.2025, https://www.newyorker.com/newsletter/the-daily/how-elon-musks-chatbot-turned-evil; SAEEDY Alexander, "Why xAI's Grok Went Rogue", 10.07.2025, https://www.wsj.com/tech/ai/why-xais-grok-went-rogue-a81841b0. (accessed on 01.08.2025).

266 https://www.reddit.com/r/Python/comments/l01yqv/i_made_a_twitter_bot_that_is_rude_to_you_when_you/?rdt=46445. (accessed on 01.08.2025).

developer's lack of liability for intentional insult[267] may be deemed accepted due to the implicit consent of the users involved.

One of the earliest fatal incidents involving autonomous systems is the *Aschaffenburg* case that occurred in 2012[268]. In the incident, the driver suffered a heart attack, yet the vehicle continued driving due to its lane-keeping system. As a result, the car collided with people, killing a mother and child, and injuring the father. Later, the vehicle crashed into a wall. The car was not fully autonomous; rather, it had a lane-keeping system, indicating a partial level of autonomy. Throughout the event, the driver was unconscious. In this case, there is no significant issue regarding civil liability due to the strict liability rule under Section 7 of the StVG[269]. Criminal liability on the other hand is problematic. The driver cannot be held liable, since he was also unconscious during the incident[270]. The key point for discussion on negligent killing or injury lies on the legal expectation of the manufacturer's ability to foresee such outcomes in general. It is also crucial to examine whether, within the technological context at the time, the manufacturer took all necessary measures to mitigate the risk[271]. It is stated that, in this regard, the public prosecutor's office in Aschaffenburg concluded that the manufacturer had not breached its duty of care with respect to negligence, based on the principles of social adequacy and the protective purpose of the norm[272].

In the following sections, the scope of the duty of care for both the manufacturers and the operator involved in this incident will be analysed in detail. However, it is crucial to emphasise that, similar to the *Tay* scandal, significant lessons were drawn from this 2012 event[273]. Since then, both technology and the standard of duty of care have advanced considerably. In 2012, vehicles equipped with low-level autonomous lane-keeping systems lacked the capability to take control if the driver experienced a medical

267 Although insult is not considered a crime in certain legal systems, Article 125 of the Turkish Penal Code classifies it as a criminal offence.

268 HILGENDORF, Automatisiertes Fahren als Herausforderung, 2019, pp. 7-9.

269 HILGENDORF, Autonome Systeme, 2018, p. 104; HILGENDORF, Robotik, Künstliche Intelligenz, Ethik und Recht, 2020, p. 555.

270 HILGENDORF, Robotik, Künstliche Intelligenz, Ethik und Recht, 2020, p. 555.

271 HILGENDORF, Autonome Systeme, 2018, p. 105 f.

272 HILGENDORF, Automatisiertes Fahren als Herausforderung, 2019, pp. 7-9; HILGENDORF, Verantwortung im Straßenverkehr, 2019, p. 156 f.
For the view that it is helpful but vague, see: HILGENDORF, Automatisiertes Fahren und Strafrecht - der Aschaffenburger Fall, 2018, p. 69

273 HILGENDORF, Robotik, Künstliche Intelligenz, Ethik und Recht, 2020, p. 555.

emergency, such as a heart attack[274]. Today, however, vehicles possess technology that enables them to autonomously assume control in such situations, greatly enhancing safety measures[275].

The incidents involving AI-driven autonomous systems are not limited to those discussed here. Throughout the study, numerous other incidents will be examined within the context of relevant discussions. Finally, in this section, it would be pertinent to provide additional examples illustrating the involvement of semi-autonomous vehicles in various minor and major accidents. For instance, during the 2020 Olympic Games in Tokyo, autonomous driving was temporarily halted following an incident in which a vehicle lightly collided with a competitor. In this case, the vehicle's sensors detected the pedestrian crossing and triggered the automatic braking system, while the operator also engaged the emergency brake. However, despite these interventions, the vehicle and the pedestrian made contact before the vehicle could come to a complete stop[276].

Another fatal incident happened with Tesla's semi-autonomous driving in 2016 where the driver has died in a collision with a truck-trailer. In the accident, the system failed to detect the truck, which was crossing the highway, as its white side blended with the bright sky[277]. Therefore, the car failed to apply its brakes and collided with the trailer, passing underneath it, with the underside of the trailer striking the car's windshield[278]. Despite the crash occurring at high speed, the car continued to travel for some distance before stopping. Investigations revealed that the system did not detect the truck in time, and the driver, who was reportedly distracted, did not intervene, despite being instructed to keep their hands on the steering wheel[279]. Following the incident, the National Highway Traffic Safety Administration (NHTSA) conducted an investigation and issued a report. The report found no defects in the design or performance of Tesla's driving assistance system, acknowledging that the system was not intended

274 *Ibid.*

275 NGUYEN, et al., Development, 2017, p. 670.

276 "Tokyo 2020: Toyota restarts driverless vehicles after accident", 31.08.2021, https://www.bbc.com/news/business-58390290. (accessed on 01.08.2025).

277 This issue is examined below in the context of whether it is sufficient for the vehicles to operate solely using cameras. See: Chapter 4, Section C(4)(b)(4): "The Evolution of Duty of Care Through New Techniques".

278 FELDLE, Notstandsalgorithmen, 2018, p. 30.

279 KLEIN Alice, "Tesla driver dies in first fatal autonomous car crash in US", 01.07.2016, https://www.newscientist.com/article/2095740-tesla-driver-dies-in-first-fatal-autonomous-car-crash-in-us/.(accessed on 01.08.2025).

to function reliably in all crash scenarios, such as collisions involving crossing paths. Consequently, the report attributed the accident to human error rather than a failure of the system. It emphasised that the system requires the driver to remain continuously attentive, as it was clearly outlined in the user manual[280].

Finally, in 2018, a similar fatal accident occurred in Arizona, U.S., involving an Uber self-driving test vehicle. Being the first recorded pedestrian fatality involving an autonomous vehicle, this incident involved a pedestrian crossing the road outside of a designated crosswalk. Investigations revealed that the vehicle's system failed to identify the pedestrian correctly and did not activate braking (the system identified the victim 5.6 seconds beforehand but could not classify properly). Furthermore, the human safety driver, distracted by watching videos on a mobile device, failed to intervene in time to prevent the collision[281]. Following the incident, Uber suspended its test-driving operations in Arizona, and the test driver was charged with negligent homicide, while no criminal charges were brought against Uber. In 2023, the case concluded with the driver -reportedly- pleading guilty to endangerment[282]. Similarly, there have been other reported criminal charges in the United States arising from the use of 'autopilot' systems[283]; however, as mentioned above, such cases are exceedingly rare.

280 National Highway Traffic Safety Administration, Preliminary Evaluation Report: Tesla Model S Crash in Williston, Florida (PE16-007) (Washington, D.C.: U.S. Department of Transportation, 2016), https://static.nhtsa.gov/odi/inv/2016/INCLA-PE16007-7876.PDF. (accessed on 01.08.2025).

281 GRIGGS Troy/WAKABAYASHI Daisuke, "How a Self-Driving Uber Killed a Pedestrian in Arizona", 21.03.2018, https://www.nytimes.com/interactive/2018/03/20/us/self-driving-uber-pedestrian-killed.html.

282 SMILEY Lauren, "The Legal Saga of Uber's Fatal Self-Driving Car Crash Is Over", 28.07.2023, https://www.wired.com/story/ubers-fatal-self-driving-car-crash-saga-over-operator-avoids-prison (accessed on 01.08.2025). BILLEAUD Jacques/SNOW Anita, "The backup driver in the 1st death by a fully autonomous car pleads guilty to endangerment", 28.07.2023, https://apnews.com/article/autonomous-vehicle-death-uber-charge-backup-driver-1c711426a9cf020d3662c47c0dd64e35. (accessed on 01.08.2025).

283 KRISCHER Tom/DAZIO Stefanie, "Felony charges are 1st in a fatal crash involving Autopilot", 18.01.2022, https://apnews.com/article/tesla-autopilot-fatal-crash-charges-91b4a0341e07244f3f03051b5c2462ae. (accessed on 01.08.2025).