JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v6i2

Criminal Liability For Ai-Based Cybercrime: Comparative Analysis of Common Law and Civil Law Approaches

Maslihati Nur Hidayati[1*], Agus Surono[2], Ery Pamungkas[3]
[1]Faculty of Law, Pancasila University, maslihati.nh@univpancasila.ac.id.
[2]Faculty of Law, Pancasila University, agussurono@univpancasila.ac.id.
[3]Faculty of Law, Pancasila University, erypamun5224004@univpancasila.ac.id.

[*]Corresponding Author: maslihati.nh@univpancasila.ac.id[1]

Abstract: This study analyzes the fundamental differences between common law and civil law systems in responding to criminal liability for artificial intelligence-based cybercrime. The background of the study covers the significant escalation of crimes utilizing AI, with 87% of global organizations experiencing AI-based attacks in 2024, AI-based fraud losses predicted to reach $40 billion by 2027, and a 223% increase in the trade of deepfake tools on dark web forums. The main problem identified by the research is a critical paradox: as AI technology becomes increasingly sophisticated in facilitating cybercrime, the gap between existing legal regulations and operational realities in the field widens, allowing criminals to exploit ambiguities in accountability to avoid responsibility. The research methodology uses a qualitative comparative legal analysis approach through analysis of primary legal documents from both systems, with case studies in four jurisdictions: the United States and the United Kingdom for common law, and Germany and France for civil law, as well as the supranational framework of the EU AI Act. The results show that the common law system has developed three models of liability—perpetration-via-another, natural-probable-consequence liability, and direct liability—but still faces fundamental difficulties in attributing mens rea to AI systems that lack moral consciousness. In contrast, civil law systems adopt a provider-deployer approach with the mechanisms of Organisationsverschulden in Germany and responsabilité pénale in France, which allow for liability based on organizational negligence, although they often lag behind in responding to technological developments. This study concludes that a hybrid approach is needed that combines the clarity of civil law codification with the adaptive flexibility of common law, as well as cross-jurisdictional harmonization to overcome the challenges of law enforcement in an increasingly autonomous AI era.

Keyword: AI; Comparative ; Criminal Liability; Cybercrime; Mens Rea.

INTRODUCTION

The rapid development of artificial intelligence (AI) technology, particularly in the form of generative AI and large language models, has brought fundamental changes to the global cybercrime landscape. Recent data indicates that in 2024, 87% of global organizations experienced AI-based cyberattacks,(Maundrill, 2025) while 281 of the 500 Fortune companies

(56%) identified AI as a critical risk factor in their annual reports(Ma, 2024). This phenomenon is indicative of a fundamental transformation in criminal methods, whereby perpetrators leverage artificial intelligence's automation, personalization, and scaling capabilities to dramatically increase the effectiveness of their attacks. According to projections by Deloitte, losses from AI-based fraud in the United States are expected to reach $40 billion by 2027, representing a substantial increase from the $12.3 billion recorded in 2023. (Lalchand et al., 2024)

This indicates a notable acceleration, particularly in the financial sector. The broader social impact is evident in the 223% increase in the trade of deepfake tools on dark web forums between the first quarter of 2023 and the first quarter of 2024, as well as the discovery of more than 3,512 AI-generated images of child sexual abuse in one dark web forum. These findings demonstrate that the capabilities of this technology have gone beyond mere financial threats and have crossed the threshold into the realm of crimes against humanity.(Hargreaves, 2024)

In response to this escalation, the international community has initiated significant legal reforms. The European Union passed the AI Act (Regulation (EU) 2024/1689) on June 13, 2024, which came into force on August 1, 2024, becoming the first comprehensive legislative initiative at the supranational level.(Burri, 2022) Concurrently, common law countries such as the United States, the United Kingdom, Canada, and Australia are still developing their approaches, relying on a combination of established common law doctrines and emerging statutory frameworks.

The fundamental differences between common law and civil law systems engender divergent approaches to criminal liability for AI-based crimes. The common law system, originating from the Anglo-Saxon tradition and reliant on judicial precedent, case law, and the flexible interpretation of fundamental principles such as actus reus and mens rea, has developed a more established category of corporate liability. However, this system still faces methodological challenges in attributing liability to autonomous AI entities. In contrast, the civil law system, which is predicated on written codification and systematic interpretation of statutes, provides greater normative clarity.(Sachoulidou, 2024) However, it frequently lags in adapting to technological innovations due to limitations in the formal legislative process. This state of affairs gives rise to a paradox that forms the crux of the research problem: as AI technology becomes more sophisticated in its facilitation of cybercrime, the discrepancy between existing regulations in legal systems and the operational reality on the ground widens, resulting in a scenario where numerous perpetrators enjoy impunity due to the ambiguity of accountability and the challenges in attributing responsibility.(Hutapea et al., 2025)

According to a 2024 global report from the International Committee on Crime Problems (ICPC), 76% of chief information security officers (CISOs) reported that regulatory fragmentation across jurisdictions seriously affects their organizations' ability to maintain compliance.(Jurgens & Cin, 2025) Moreover, UK law enforcement has indicated that the British law enforcement community is not adequately equipped to effectively prevent, disrupt, or investigate AI-based crimes. This scenario poses a significant risk of engendering legal uncertainty, a circumstance that has the potential to be detrimental to both parties with a vested interest in the realm of AI innovation and the protection of crime victims.(Mantili et al., 2025)

An investigation into how countries with common law systems have responded to this challenge reveals a heterogeneous pattern.(Basu & Dave, 2025) In the United States, law enforcement entities depend on the provisions of the Computer Fraud and Abuse Act (CFAA), in addition to various statutes at the federal and state levels.(Lin, 2025) These legal frameworks offer a degree of interpretive flexibility but concomitantly engender ambiguity in their implementation, particularly within the context of AI, which remains in its nascent stages within the domain of jurisprudence. The United Kingdom has endeavored to incorporate AI

considerations through the Computer Misuse Act of 1990 and various regulations. (Abdelaziz, 2025)

The analysis of data enforcement indicates that a discrepancy exists between the regulations in place and the enforcement practices that have been implemented in both systems. This discrepancy is indicative of a significant gap that requires further investigation to ascertain its extent and implications. By the conclusion of 2024, a mere 37% of global organizations reported having a process in place to assess the security of AI tools prior to deployment. Meanwhile, 66% of organizations stated that AI would have the most significant impact on cybersecurity in the coming year. This finding suggests a dissociation between risk awareness and action in the enforcement domain. Moreover, a 2025 report from the Alan Turing Institute indicates that UK law enforcement lacks the necessary resources, coordination, and AI capability deployment to proactively disrupt criminal groups using AI.(Janjeva, 2025) The challenges of attribution and causation are critical bottlenecks in this context. In the context of AI-based crime, the "problem of many hands" becomes exponentially more complex as it involves multiple actors in the developer-manufacturer-user chain, with contributions from designers, programmers, trainers, operators, and third-party users.(Simmler, 2024) The predictability of AI system actions is often negated by the complexity and opacity of machine learning systems.

A comparative analysis reveals that both legal systems possess distinct strengths and weaknesses in their responses to these challenges. The common law system, characterized by its adaptability in interpretation and evolution through case law, enables judicial authorities to respond expeditiously to emerging technologies. However, this also engenders uncertainty in the predictability of legal standards and inconsistency across jurisdictions. Conversely, civil law systems offer clarity and harmonization through explicit codification; however, they frequently exhibit delays in responsiveness to rapid technological change and are constrained by formal legislative processes. The EU AI Act, for instance, delineates between administrative offenses for breaches of substantive requirements (designated as very serious, serious, and minor infractions) and traditional criminal liability, thus establishing a dual-track system that has the potential to address AI misuse at multiple levels.(Basu & Dave, 2025) However, the implementation of these directive-based provisions necessitates transposition into national law, which could result in inconsistency. Concurrently, common law jurisdictions such as the UK and the US are endeavoring to establish a coherent criminal law framework that effectively captures autonomous or semi-autonomous AI behavior without violating fundamental principles, including the principle of guilt and the mens rea doctrine.(Arnal, 2025)

The necessity to establish explicit criminal accountability for AI-related transgressions is bolstered by numerous pivotal considerations. Firstly, the proliferation of criminal activity that incorporates artificial intelligence capabilities results in harm on an unparalleled scale and severity. Financial crimes perpetrated through the use of deepfakes and romance fraud have reached a scale that is estimated to be in the millions of dollars. The generation of child sexual exploitation material has reached volumes that are overwhelming law enforcement agencies.(Davey & Sauerwein, 2023)

Phishing and social engineering attacks have increased by 82% with the augmentation of artificial intelligence. Secondly, criminal groups and even state actors have demonstrated the capability and willingness to weaponize AI tools to achieve criminal objectives. Furthermore, the development trajectory shows that adoption barriers continue to decline. Thirdly, the presence of legal uncertainty and enforcement gaps engenders a scenario in which perpetrators are able to exploit ambiguity in legal frameworks to evade accountability.(Martin, 2025)

Concurrently, corporations and developers operate within an environment characterized by uncertainty, a factor that impedes the responsible development of AI. Fourthly, the transnational nature of cybercrime necessitates enhanced coordination and harmonization

among legal systems. The fragmentation of criminal liability frameworks across jurisdictions enables criminals to exploit regulatory gaps and opt for legal venues that offer the most favorable outcomes, thereby minimizing legal consequences.(Rodrigues, 2020)

This research is significant because it aims to address a critical gap in the academic discourse on the harmonization of criminal liability for AI-enabled cybercrime. Existing literature has explored specific issues such as attribution problems, causation difficulties, and mens rea limitations in an abstract or theoretical manner. However, comparative analysis is limited regarding how the two major legal traditions practically respond to these challenges, where their specific strengths and weaknesses lie, and how lessons learned from one tradition can inform development in the other. Moreover, there has been a paucity of attention paid to the ramifications for civil law countries in the Global South, such as Indonesia, who are confronted with the imperative to adopt AI-related criminal legislation yet frequently possess an inadequate foundation of jurisprudence and institutional capacity to implement sophisticated legal frameworks. By analyzing comparative approaches from common law and civil law countries in regulating criminal liability for AI-based cybercrime, this research can provide practical insights on legislative drafting, enforcement mechanisms, and institutional reforms that can support a more effective and equitable response to emerging threats. At the national level of Indonesia, the findings of this comparative analysis can inform necessary amendments to the ITE Law and the development of specific criminal provisions to address AI developer liability, criteria for fault attribution, and due diligence obligations that are aligned with both international best practices and Indonesian legal principles.

METHOD

This study adopts a comparative legal analysis approach to analyze how common law and civil law systems respond to the challenges of criminal liability in artificial intelligence-based cybercrime. This method was chosen because of its suitability in identifying philosophical differences, implementation mechanisms, and practical effectiveness between the two major legal traditions of the world, which have fundamentally different characteristics in terms of legal sources, normative interpretation, and jurisprudential evolution.

This study applies a qualitative analytical framework involving three main stages. First, the identification stage involves the collection and categorization of primary legal materials from both systems, including statutory provisions from the CFAA in the United States, the Computer Misuse Act in the United Kingdom, the Strafgesetzbuch in Germany, and the French Penal Code in France, combined with the EU AI Act as a supranational framework. Second, the comparative analysis stage involves an in-depth examination of fundamental concepts such as actus reus, mens rea, corporate liability, and related doctrines through the principles in each system to identify material similarities and differences. Third, the synthesis stage involves the formation of a conceptual model that shows how each system handles the three main liability models: perpetration-via-another, natural-probable-consequence liability, and direct liability towards the AI system itself.

The research data sources are secondary and sourced from legal-academic documents covering statutory texts, relevant judicial precedents, documentation of the implementation of the EU AI Act, and peer-reviewed scientific literature from various leading legal journals and research institutions. The research design uses a cross-jurisdictional comparison by selecting two common law countries (the UK and the USA) and two civil law countries (Germany and France) as representative case studies, allowing for the identification of common patterns as well as local variations within each legal tradition. This research also integrates an analysis of enforcement practices by comparing the available regulatory framework with its practical implementation by law enforcement agencies, revealing a significant gap between legal norms and operational realities. This holistic approach enables the study to provide contextual and

relevant recommendations, especially for civil law countries in the Global South such as Indonesia, which need to adopt AI-specific legislation but are constrained by institutional capacity limitations and a developing jurisprudential foundation.

RESULTS AND DISCUSSION

Criminal Liability for AI-Based Crimes in the Common Law System: A Comparative Study of Implementation in the UK and USA

The regulation of criminal liability for crimes committed by artificial intelligence (AI) systems in common law countries such as the United Kingdom (UK) and the United States (USA) faces fundamental challenges in applying traditional criminal principles designed specifically for human agents. The criminal law frameworks of both jurisdictions are predicated on two main constitutive elements that have served as the foundation of criminal liability for centuries. These elements, known as actus reus (criminal act) and mens rea (malicious intent or mental fault), undergird the legal principles that govern criminal liability. The integration of these two elements within the context of increasingly autonomous AI systems gives rise to a substantial discrepancy between the pace of technological advancement and the capacity of prevailing criminal law frameworks to adapt.(Sachoulidou, 2024)

In the UK context, the common law principles governing criminal responsibility have evolved through a process of judicial decisions and subsequent statutory codification. The prevailing English criminal law system is predicated on the notion that criminal liability is exclusively ascribed to human entities or legal persons (e.g., corporations). This is predicated on the premise that these entities possess the cognitive capacity to form criminal intent and commit prohibited acts.(Sarch, 2024) Conversely, in the USA, the criminal liability framework is codified in the Model Penal Code, which has been adopted by various states, although not all. This code also maintains the dual element requirements of actus reus and mens rea for nearly all crimes. Both systems encounter analogous challenges when confronted with autonomous AI systems capable of making decisions and executing actions without direct human intervention.(Hashmi et al., 2025)

The initial element, actus reus or wrongful act, is, by definition, more readily ascribable to an AI system than mens rea. In traditional common law, actus reus is defined as an external or objective act that constitutes the material component of a crime. This encompasses not only physical movements but also omissions (negligence) when there is a legal obligation to act. AI systems, particularly robots or software agents, have the capacity to execute actions that satisfy the technical definition of actus reus, both in the form of commission (the act of doing something) and omission (the failure to act).(R. Abbott, 2020)

To illustrate, if an AI robot programmed to execute operations in a factory were to identify a human worker as a threat to its mission and subsequently attack that worker using its hydraulic arm, this physical action would objectively satisfy the actus reus element of the crime of homicide or assault. In the context of AI-based cybercrimes, software agents that access computer systems without authorization or exceed authorized access fulfill the actus reus component of cybercrime offenses.

However, the primary challenge in applying criminal liability to AI lies in the element of mens rea, which refers to the mental condition or state of mind of the perpetrator when committing a criminal act. According to Model Penal Code Section 2.02 and UK common law principles, various degrees of mens rea are recognized, including knowledge, intent/purpose, recklessness, and negligence. The fundamental challenge is whether AI systems can possess mental states equivalent to the concept of mens rea developed for humans. In the context of traditional common law, the term "mens rea" is understood to denote the state of mind of the perpetrator, encompassing elements such as awareness of the material facts, intention to

achieve a particular outcome, and the presence of recklessness or negligence in the perpetrator's actions.(R. B. Abbott & Sarch, 2019)

In the United Kingdom, the principles of criminal law have been codified through various legislative acts, including the Serious Crime Act of 2015, which establishes the framework for accomplice liability and participatory crimes.(Dyson, 2022) When applying this framework to AI-based crimes, the question that arises is whether machine learning algorithms that process millions of data points and optimize actions based on reward functions can be said to have "knowledge" or "intention" in the legal sense. The latest generation of AI systems have the capacity to collect data from various sources, analyze it, and make probabilistic predictions about the outcomes of their alternative actions. These predictions are superficially reminiscent of how humans form intentions based on their knowledge. However, this similarity is superficial. AI lacks self-awareness, cannot comprehend the moral or legal implications of its actions, and cannot accept the deterrence effect of threatened punishment in the same way that humans do.(Nerantzi & Sartor, 2024)

In the United States, following the Supreme Court's decision in the Van Buren v. United States case in 2021, the criminal liability provisions for computer-based activities under the Computer Fraud and Abuse Act (CFAA, 18 U.S.C. § 1030) underwent substantial elucidation with respect to the elements of mens rea and the interpretation of "authorization." In its decision, the Supreme Court emphasized that "intentionally accessing a computer without authorization or exceeding authorized access" requires a technical understanding of what "access" means in a computing context, namely, entry into a computer system or a specific part of a computer system, rather than simply using the system for unauthorized purposes. This clarification bears significant implications for the criminal liability of AI: the CFAA stipulates the mens rea element of "intentionally," thereby necessitating that the perpetrator deliberately access a computer without authorization or exceed their authorization. The fundamental question pertains to whether an AI system operating autonomously can satisfy this "intentionally" requirement.(Thaw, 2013)

The interpretation of "intentionally" in Model Penal Code section 2.02(2)(a) defines it as an action taken "with conscious object to cause such a result" or "with knowledge that such conduct is substantially certain to cause such result." When applied to autonomous AI systems, the question arises as to whether the reward function or optimization objective programmed into the system can be qualified as a "conscious object" or "intent" in the criminal law sense. It is evident that a programmer who designs artificial intelligence (AI) with the intent to steal data from a computer system by exceeding authorized access privileges undoubtedly possesses the mens rea necessary for criminal liability. However, in a scenario where AI independently and unpredictably learns to optimize its objectives in a way that results in unauthorized access, perhaps because neural networks have identified new strategies that were not designed or anticipated by the programmer, the question of mens rea becomes significantly more complex.(Jani & Rathor, 2024)

In both common law jurisdictions, legal scholars have identified three primary approaches to determining liability. The initial model is the perpetration-via-another model, in which AI systems are regarded as innocent agents or tools. This is analogous to the way in which knives or screwdrivers are treated in criminal law. According to this model, criminal responsibility falls on the programmer or user who utilizes AI instrumentally to perpetrate a crime. In order to be held liable for a crime committed by an AI, a programmer or user must have the necessary mens rea for the crime in question. That is to say, the programmer or user must have the intent to commit the crime in question. The actions of the AI are attributed to the programmer or user as if they had committed the acts themselves. This model is consistently applied in common law in both the UK and the USA when third-party instruments (both human and non-human) are used to commit crimes. In accordance with the tenets of criminal law in

both jurisdictions, an individual who causes another person (or an innocent agent) to commit a crime is considered criminally liable as a principal in the first degree.(Hallevy, 2024)

However, this perpetration-via-another model has significant limitations when applied to autonomous AI systems with a high level of sophistication. This model is not applicable in scenarios where artificial intelligence (AI) perpetrates crimes based on the accumulation of its own experiences and learning, as opposed to being instructed to do so by programmers or users. This leads us to the second model, the natural-probable-consequence liability model. This model is predicated on the premise that programmers or users can be held responsible for crimes committed by AI if those crimes are the natural and probable consequence of their conduct, even if they had no explicit intent to commit those crimes. This approach is predicated on the principle of criminal negligence, a tenet that has long been part of common law in the UK and USA. The principle posits that an individual can be held criminally liable for acts they did not personally commit if those acts are the natural and probable consequence of their conduct that would be foreseeable by a reasonable person.(King et al., 2020)

In the United Kingdom, the principle of accomplice liability, as delineated in the Serious Crime Act of 2015, acknowledges that an individual can be held liable as an accomplice to a crime perpetrated by the principal offender if they provide assistance with the intent that the assistance will be utilized to commit a crime, or with the awareness that a specific crime will be committed.(Horder, 2022) When applied to the programming and deployment of AI systems, this means that programmers or entities that deploy AI with the knowledge that the system may, as a natural and probable consequence, commit certain criminal acts can be held responsible for those crimes through the mechanisms of accomplice liability or criminal negligence. In the United States, a similar principle is applied through aiding-and-abetting liability and the accomplice doctrine, which is recognized in various federal and state courts. This structure of responsibility necessitates that programmers or users possess a reasonable understanding that their actions may result in criminal consequences. (Selbst, 2020)

The third approach is the direct liability model, in which the AI system itself is held criminally liable for crimes committed. The applicability of this model is contingent upon the fulfillment of two constitutive elements of criminal liability by the AI system: actus reus and mens rea. As previously discussed, the actus reus component of the crime in question can be relatively easily attributed to AI. The central question pertains to the capacity of artificial intelligence (AI) to satisfy the mens rea prerequisite as delineated by the prevailing principles of common law criminal jurisprudence. Certain legal theorists posit that the cognition and volition requirements that constitute mens rea in common law, that is, knowledge and intent, can be attributed to AI systems at a certain level of abstraction. The presence of cognition and volition in an AI system can be demonstrated by its capacity to process sensory information, both electronic and physical, analyze it to form a model of its environment, and perform calculations to predict the consequences of alternative actions before choosing the action that optimizes its objective function. At a certain level of abstraction, these cognitive and volitional processes can be said to exist.(Diamantis, 2020)

Nevertheless, the direct implementation of the direct liability model in autonomous AI systems encounters significant challenges in both common law jurisdictions. The United Kingdom and the United States both adhere to the fundamental principle in criminal law that culpability requires not only criminal acts but also moral agency or responsible agency. That is to say, the capacity to understand and respond to morally and legally relevant reasons. The concept of culpability, in this context, is defined as the accountability for choices made within the context of an understanding of applicable norms. While sophisticated AI systems may exhibit computational processes that superficially resemble human reasoning, they are deficient in their comprehension of moral and legal norms, a deficiency that is pertinent to the attribution of culpability.(Osmani, 2020)

In law enforcement practice in both jurisdictions, a more conservative position has been adopted. In the UK, guidance for judicial office holders emphasizes that any use of AI by or on behalf of the judiciary must be consistent with the judiciary's overarching obligation to protect the integrity of the administration of justice. Nevertheless, the present guidance is oriented towards the utilization of AI in judicial and administrative procedures rather than towards criminal liability for AI actions in themselves. The majority of prosecutions for AI-related crimes in the UK have targeted human actors who developed, configured, or used AI for criminal purposes, rather than the AI systems themselves. In the United States, analogous to the United Kingdom, the enforcement of the Computer Fraud and Abuse Act (CFAA) has centered on individuals who utilize computer systems, including those with artificial intelligence components, to obtain unauthorized access or exceed authorized access. The Supreme Court's decision in Van Buren v. United States did not explicitly address criminal liability for autonomous AI systems. However, its interpretation of the terms "intentionally" and "authorization" has important implications for future regulatory frameworks.(Giannini, 2023)

The regulatory framework governing criminal liability for AI-related crimes in common law jurisdictions necessitates a meticulous balancing act among several competing principles and practical considerations. First, the principle of legality must be considered. This principle dictates that criminal liability can only be imposed for conduct that is clearly defined as criminal by pre-existing and specific laws. Secondly, the principle of culpability is invoked, which stipulates that criminal liability can only be attributed to agents who possess moral agency and the capacity to adhere to legal norms. Thirdly, there is the practical consideration that existing criminal statutes in both jurisdictions have been developed to regulate computer crimes, and these statutes generally assume human or corporate perpetrators.(Nerantzi & Sartor, 2024)

In the United Kingdom, the Computer Misuse Act of 1990 establishes legal provisions for addressing three distinct categories of offenses. These categories include unauthorized access, unauthorized access with the intent to commit further offenses, and unauthorized modification. Each provision in this Act, whether implicit or explicit, necessitates an element of knowledge or intent, indicating that access is unauthorized. In the context of AI systems, judicial bodies will be tasked with deliberating on the question of whether autonomous AI systems engaging in unauthorized access can be held liable under the provisions of this Act. In practice, the focus of liability has been on programmers or users. However, as AI systems become increasingly autonomous and unpredictable in their behavior, legislators may consider the potential for direct liability against AI systems.(Soyer & Tettenborn, 2022)

In the United States, the framework for determining criminal liability in cases of computer-related crimes is characterized by fragmentation, with a variety of statutes existing at both the federal and state levels. The Computer Fraud and Abuse Act (CFAA), codified in 18 U.S.C. § 1030, is the prevailing federal statute addressing this issue. However, the CFAA has been subject to substantial criticism due to its extensive scope and ambiguous language. The Van Buren Supreme Court decision established a more limited interpretation of the term "exceeds authorized access," thereby reducing the scope of criminal liability. Under this narrow interpretation, unauthorized access for improper purposes does not necessarily violate the CFAA if the user has authorization to access particular areas of the computer system. The practical effect of this decision is that prosecution for AI-based unauthorized access becomes more difficult, as prosecutors must show that the AI system accessed areas of the computer system to which the AI was not authorized to access, not just that the AI used authorized access for improper purposes.(Villasenor, 2021)

In both jurisdictions, the emerging approach entails the development of specific regulatory frameworks for AI that are distinct from traditional criminal law. In the UK, the

government has identified the governance of artificial intelligence (AI) as a priority area and has issued various guidelines for the responsible development of AI. In the United States, various federal agencies have issued guidance on the regulation of artificial intelligence (AI), including in the criminal context. However, to date, there is no comprehensive federal criminal statute that specifically addresses liability for autonomous AI systems. The question of whether existing criminal law frameworks can adequately address harms from autonomous AI systems, or whether new legislative frameworks are needed, remains the subject of ongoing debate in both jurisdictions.(Makam, 2023)

In the context of corporate criminal liability, as established in both the UK and the US, the principles developed may serve as a model for addressing AI liability. In both jurisdictions, corporations can be held criminally liable even in the absence of traditional human intent. The liability of corporations is typically predicated on the actions of agents operating within the scope of their employment and with the intent to benefit the corporation. This model may be adaptable to autonomous AI systems: if AI systems can be regarded as quasi-legal persons with defined interests and objectives (through algorithms and objective functions), then the corporate liability framework may be extended. However, the implementation of this extension would necessitate a substantial reconceptualization of the foundational principles of criminal law.(Mattia, 2024)

Criminal Liability for AI-Based Crimes in the Civil Law Law System: A Comparative Study of Implementation in the Germany and France

The European Union's Artificial Intelligence Act (AI Act), which is set to take effect in August 2024, establishes that criminal liability cannot be directly attributed to AI, as these systems lack legal personality, moral awareness, or the capacity to comprehend the legal ramifications of their actions. Consequently, the conceptual underpinnings of criminal liability continue to be inextricably linked to conventional legal subjects, namely individuals (natural persons) or legal entities, who find themselves intricately interwoven with the life cycle of AI systems.(de Lemos Campos, 2024)

A foundational principle in the AI Act is the delineation between providers and deployers. According to Article 3(3), the term "providers" encompasses natural persons, legal persons, public authorities, agencies, or bodies that engage in the development of AI systems or general-purpose AI models. Additionally, providers may include entities that have AI systems or models developed and placed on the market or operated under their name or trademark, with or without the provision of compensation. Conversely, deployers are defined in Article 3, paragraph 4 as natural persons, legal persons, public authorities, agencies, or bodies that use AI systems under their authority, with the exception of instances in which AI systems are employed in the context of non-professional personal activities. The allocation of criminal responsibility between these two parties determines who can be held accountable when the use of AI violates the provisions of the law, in particular Article 5 of the AI Act, which prohibits certain AI practices.(Pehlivan, 2024)

Article 5 of the AI Act proscribes a number of AI practices that are considered to violate the fundamental values of the European Union and human rights. The initial proscription pertains to the utilization of subliminal or manipulative techniques that surpass an individual's awareness with the objective of distorting behavior, thereby inflicting or potentially inflicting substantial harm. Secondly, the exploitation of vulnerabilities among specific groups, including those based on factors such as age, disability, or particular social and economic circumstances, is prohibited. Thirdly, the prohibition of social scoring systems that classify individuals or groups based on known, inferred, or predicted social behavior or personal characteristics with detrimental or disproportionate results.(Neuwirth, 2023)

Fourthly, the prohibition encompasses criminal risk assessment systems that predict the likelihood of an individual committing a crime based exclusively on profiling or personality characteristics. The fifth point pertains to the establishment of a prohibition on the creation of facial recognition databases through the unsystematic harvesting of internet images or CCTV footage. Sixthly, a prohibition is to be established on the use of emotion recognition systems in occupational and educational settings, with the exception of instances pertaining to medical or safety concerns. Seventhly, a prohibition is to be established on the use of biometric categorization systems that infer race, political opinion, trade union membership, religious or philosophical beliefs, sexual life, or sexual orientation based on biometric data. The eighth directive stipulates a prohibition on the implementation of real-time remote biometric identification systems in public spaces by law enforcement entities, with limited exceptions granted for the purpose of locating victims of kidnapping, trafficking, child sexual abuse, missing persons, and the prevention of terrorist threats or specific criminal investigations, as detailed in Annex II.(Barkane, 2022)

From a criminal liability perspective, the AI Act establishes a multifaceted framework due to its non-explicit allocation of criminal liability, instead empowering each Member State to establish its own distinct set of criminal regulations. Article 99 of the AI Act stipulates that Member States must formulate rules on penalties and other enforcement measures applicable to violations of the AI Act Regulations by operators. These measures may include warnings and non-monetary penalties. It is imperative that penalties be effective, proportionate, and dissuasive. Failure to comply with the prohibitions on AI practices outlined in Article 5 can result in administrative fines reaching up to €35 million, or, in the case of an enterprise, up to 7% of its total worldwide annual turnover in the previous fiscal year, whichever is higher. However, it is imperative to acknowledge that the AI Act establishes administrative fines, not criminal penalties directly. Nevertheless, this structure provides Member States with the flexibility to allocate criminal liability based on their national criminal laws.(TATARU & CREȚU, 2024)

The criminal liability framework for providers in the context of the AI Act is supported by two articles. The first is Article 16, which regulates the obligations of providers of high-risk AI systems. The second is Article 26, which regulates the obligations of deployers of high-risk AI systems. It is incumbent upon providers to ensure that high-risk AI systems comply with the requirements enumerated in this Regulation prior to their placement on the market. The obligations of providers include the development and maintenance of a quality management system, the provision of technical documentation, the conducting of conformity assessments, the maintenance of automatic logs, the conducting of post-market monitoring, and the reporting of serious incidents. Conversely, deployers are obligated to ensure that high-risk AI systems are utilized in accordance with the provided instructions, appoint competent human oversight, monitor system operations, maintain automatic logs, and report serious incidents to providers and market surveillance authorities.(Schuett, 2024)

Criminal liability may arise when providers or deployers violate these obligations intentionally or through negligence that causes harm. In such cases, the determination of whether negligence or criminal intent (mens rea) can be proven is determined by the national criminal law. In civil law systems such as those in Germany and France, the concept of culpability is formulated through an understanding of intent (dolus) and negligence (culpa). In the context of AI, the critical question is whether the provider or deployer could have known or could have foreseen that their AI system would be used to commit acts that violate Section 5 of the AI Act or cause harm to third parties.(Bertolini, 2025)

In Germany, the legal framework governing criminal liability in the context of artificial intelligence is delineated by the Strafgesetzbuch (StGB), a comprehensive code that serves as the nation's primary legislation. The StGB does not contain specific provisions for AI crimes;

however, general principles can be applied in this context. Section 14 StGB establishes the foundation for this principle, stipulating that an individual who perpetrates an act that results in the occurrence or non-occurrence of a criminal offense based on their own culpability can be held criminally liable. In the context of AI, the pertinent question is whether the provider or deployer can be held liable based on culpa lata or dolus (negligence or intent). Section 15 StGB confirms that criminal liability for acts committed with intent is the prevailing standard, unless criminal law explicitly provides for culpability based on negligence.(Nerantzi & Sartor, 2024)

Within the ambit of AI practices that are proscribed by the AI Act, the evaluation of criminal liability in Germany can be conducted through the lens of several pertinent provisions. First, Section 263 StGB on Betrug (fraud) can be applied if the provider or deployer intentionally uses an AI system that contains manipulative or deceptive elements to deceive the victim and cause material damage. Secondly, Sections 186-187 of the German Criminal Code (StGB) concerning üble Nachrede (libel) and Verleumdung (slander) can be applied if the AI system is used to generate content that attacks a person's honor or reputation. This could be achieved through the use of deepfakes or AI-facilitated content generation. Thirdly, Section 303a StGB concerning Datenveränderung (data manipulation) can be applied if an AI system is manipulated or trained with inaccurate data with the intention of causing errors in decision-making. Fourthly, Section 13 StGB stipulates the regulation of omission liability, which is pertinent when providers or deployers neglect to implement the requisite measures to avert harm through the AI systems under their control or supervision.(Crawford et al., 2025)

In Germany, criminal liability can also arise through the concept of Organisationsverschulden (organizational culpability), a term that applies to legal entities. According to German jurisprudence, legal entities can be held criminally liable if their management or representatives commit criminal acts that benefit the legal entity or if there is negligence in supervision (Aufsichtspflicht). In the context of AI, this responsibility emerges if the leadership or management of an AI system provider or deployer fails to implement adequate safeguards, does not exercise sufficient oversight of their AI systems, or does not report known serious incidents.(Allahverdiyev & Othman, 2022)

The German legal system also acknowledges the concepts of Kausalität (causality) and Vorhersehbarkeit (foreseeability), which are pivotal in evaluating culpability. In the context of AI, the pertinent question is whether the provider or deployer of the AI system could have foreseen that their AI system could potentially cause harm or be utilized to perpetrate a prohibited criminal act. The absence of criminal liability is predicated on the condition that the AI system has been developed in accordance with state-of-the-art standards and best practices, and that the provider or deployer has implemented reasonable safeguards. However, if there is evidence of gross negligence in the development or deployment, or if the provider or deployer knew or should have known about significant risks, then criminal liability may arise.

In France, the criminal liability of AI is governed by the French Penal Code. In contrast to the common law system, the French system, rooted in the civil law tradition, adheres to the principle of responsabilité pénale, as delineated in Article 121-3 of the Penal Code. The article posits that no crime or misdemeanor is committed without intent to commit it. However, when the law provides for it, a misdemeanor is deemed to exist in cases of deliberate endangerment, as well as in cases of fault, imprudence, negligence, or breach of the obligation of prudence or safety determined by law or regulation. This is contingent upon the ability to prove that the perpetrator did not exercise normal diligence by taking into account, where relevant, the nature of the missions or functions, competencies, and powers and means at their disposal.(Ghigheci, 2019)

The question of criminal liability in France is addressed through a variety of mechanisms. First, if a provider or deployer deliberately uses or distributes an AI system that they know is prohibited by Article 5 of the AI Act or applicable French law, they may be held criminally

liable. To illustrate, if a provider or deployer consciously utilizes an AI system designed for subliminal manipulation or exploitation of specific vulnerabilities, they may be subjected to various pertinent offenses under the Code Pénal.(Affagard & Carvès, 2024)

Secondly, criminal liability may arise based on culpa or negligence. According to Article 121-3 of the French Penal Code, criminal liability may arise in circumstances involving fault, imprudence, negligence, or breach of the obligation of prudence or security. This is contingent upon the demonstration that the accused party did not exercise the degree of diligence that would be considered reasonable in light of the nature of their duties, functions, competencies, and authorities. Within the domain of AI, this stipulation signifies that in the event that a provider or deployer neglects to:(Ghigheci, 2019)

1. It is imperative to implement adequate safeguards to prevent AI systems from being used in prohibited or harmful ways.
2. Conduct appropriate conformity assessments or quality management;
3. Subsequent to the deployment of the AI system, it is imperative to undertake a meticulous monitoring of its operational processes.
4. It is imperative that serious incidents be reported as soon as they come to light.
5. It is imperative to adhere to the stipulated obligations, whether they are delineated by the AI Act or by French law.

Failure to comply may result in criminal liability for negligence or culpable omission.

Thirdly, Article 121-3, paragraph three of the Penal Code introduces the concept of criminal liability for individuals who did not directly cause the damage but who created or contributed to creating a situation that allowed the damage to occur or who did not take measures to prevent it. In the context of corporate responsibility, this is particularly salient because the leadership or management of a provider or deployer may be held liable even if they were not directly involved in the development or deployment of the AI system, provided that it is proven that they manifestly and deliberately violated their particular obligations of prudence or security, or committed a grave fault that exposed others to a particularly serious risk that they could not ignore.(Duflot, 2024)

France has established specific criminal provisions that address the perpetration of AI-related crimes. Article 227-23 of the French penal code concerning child sexual abuse material (CSAM) has been broadly interpreted by French courts to include artificial intelligence (AI)-generated or AI-manipulated images of minors, not just real images of actual children. Consequently, if an individual utilizes an AI system to generate, distribute, or proffer deepfakes featuring minors within a pornographic context, they may be subject to prosecution for this offense, irrespective of the absence of any actual child involvement. Furthermore, providers or distributors of platforms that facilitate the sharing of such content may be held accountable under Article 6 of Loi 2004-575 (LCEN - Loi pour la Confiance dans l'Économie Numérique), which stipulates that platforms must monitor and remove any illegal content.(Tual, 2025)

In the Clearview AI case of 2022, the CNIL (French Data Protection Authority) imposed a €20 million fine for the unlawful processing of personal data, including the unauthorized use of facial recognition. While this is an administrative fine under the General Data Protection Regulation (GDPR), it demonstrates France's commitment to leveraging all available mechanisms to ensure compliance with data protection and AI regulations. Furthermore, criminal liability may also arise if intent or gross negligence is proven.(Cortez & Maslej, 2023)

In the broader context of criminal liability for AI-based crimes, both jurisdictions (Germany and France) also consider the concept of liability for creating or enabling infrastructure for criminal activity. This is relevant for “Dark AI” systems, i.e., AI systems specifically engineered for malicious purposes such as hacking, cracking, or cyberattacks. In Germany, Section 202a StGB on Ausspähen von Daten (unauthorized access and spying on data) can be applied if an AI system is used to conduct cyberattacks or data theft. In France,

various provisions in the Code Pénal on unauthorized computer access, data theft, and fraud can also be applied.(Susila & Salim, 2024)

At the European Union level, the Council of Europe (CoE) through the European Committee on Crime Problems (CDPC) has prepared a discussion paper in 2024 on criminal liability related to AI systems. This paper identifies four categories of situations that may require criminal liability(Gless & Peralta, 2024):

First, when AI systems are used as tools to commit established crimes (such as homicide, theft, fraud). In this case, existing criminal laws may be sufficient, although Member States may consider adding AI use as an aggravating circumstance. Second, when AI systems are used to cause harm in novel ways that were not previously predicted. This includes technology-facilitated violence against women and girls (using deepfakes for sexual exploitation), online sexual grooming using AI, and distribution of "Dark AI" systems.

Third, when bona fide use of AI systems results in unforeseeable harm, such as a chatbot slandering someone due to hallucination, a self-driving car causing an accident, or a high-frequency trading system engaging in market manipulation. In these situations, member states may wish to discuss a harmonized approach to establish thresholds for criminal negligence or exemption from liability. Fourth, when AI systems are designed, trained, or deployed in violation of obligations in the AI Act or Framework Convention on AI. This may include violations of transparency, accountability, or non-discrimination requirements.

In the context of enforcement, significant challenges emerge in determining the parties responsible for the complex chain of development, distribution, and deployment of AI systems. This assertion is particularly salient in the context of general-purpose AI models, which have the capacity to be integrated into a myriad of downstream systems. Article 25 of the AI Act acknowledges this complexity by establishing that deployers may be regarded as providers if they make substantial modifications to high-risk AI systems that result in alterations to functionality, safety, or the intended purpose. In such a scenario, the deployer assumes responsibility for ensuring adherence to all provider obligations. Conversely, the original provider may be exonerated from specific responsibilities while maintaining the obligation to cooperate.(van Bekkum, 2025)

In order to establish a framework for criminal liability in the context of AI, it is imperative to consider the fundamental principles of criminal law, including the legality principle (nullum crimen sine lege), proportionality, and due process. In civil law systems, criminal liability can only be invoked if specific criminal provisions clearly establish punishable conduct. In the evolving landscape of AI regulation, Member States must ensure that criminal law provisions are sufficiently clear and precise to allow for fair trials and adequate notice to potential defendants.(Garrett, 2025)

Table 1. Comparison Table of Criminal Liability for Artificial Intelligence-Based Cybercrimes

Dimensions of Analysis	United States	United Kingdom	Germany	France
Legal Basis / Primary Legislation	Computer Fraud and Abuse Act (CFAA) 18 U.S.C. § 1030; Model Penal Code (MPC); Federal Criminal Code	Computer Misuse Act 1990; Criminal Law Act 1977; Fraud Act 2006; Police and Criminal Evidence Act 1984	Strafgesetzbuch (StGB) - Kode Penal; §202a-202d (Unauthorized Computer Access); AI Act EU Implementation	Code Pénal Français - Kode Penal Prancis; Articles 226-16 hingga 226-24 (Computer Crimes); AI Act EU Implementation
Legal System	Common Law (Federal & State level)	Common Law	Civil Law (Codified System)	Civil Law (Codified System)

Dimensions of Analysis	United States	United Kingdom	Germany	France
Primary Criminal Liability Model	Perpetration-via-another model; Natural-probable-consequence liability; Rare direct liability on AI systems	Perpetration-via-another model; Joint enterprise doctrine; Rare individual liability for AI conduct	Provider/Deployer responsibility model; Organisationsverschulden (Corporate culpability); Kausalität & Vorhersehbarkeit principles	Responsabilité pénale model; Culpa/Intent-based liability; Corporate criminal liability for gross negligence
The Concept of Legal Fault (Mens Rea / Culpa)	Strict requirement of mens rea (Intent/Knowledge/ Recklessness); Difficult to establish for AI-mediated crimes; Focuses on programmer/user intent	Strict requirement of mens rea for most crimes; Some strict liability offenses; Emphasis on defendant's subjective knowledge	Vorsatz (Intent) and Fahrlässigkeit (Negligence) distinction; Kulpa dapat berupa omission; Gross negligence sufficient for criminal liability	Intent/Negligence-based culpability; Negligence covers failure to implement safeguards; Lower threshold than gross negligence for some AI-related offenses
Subject of Criminal Liability	Natural persons (programmers, users, executives); Limited corporate criminal liability; AI systems generally not held liable	Natural persons with direct/indirect liability; Corporate entities through directors/managers; AI systems not held liable	Natural persons (developers, users, managers); Legal entities/organizations (Organisationsverschulden); AI systems not held liable	Natural persons (developers, deployers, responsible parties); Legal entities; AI systems not held liable
Provider Accountability (Developer / Provider)	Liability arises from intentional design to facilitate crime; Rare unless explicit criminal intent proven; Limited duty to prevent misuse	Liability based on foreseeable misuse; No duty to prevent all misuse; Liability if design enables crime intentionally	Liability for gross negligence in development; Duty to implement state-of-the-art safeguards; Liability for failure to conduct risk assessments; Organisationsverschulden applies	Liability for culpable failure to implement safeguards; Duty to conduct conformity assessments; Liability for gross negligence; Corporate liability possible
Deployer Accountability (User / Distributor)	Direct liability for intentional misuse; Liability under CFAA if exceeding authorized access; Responsibility for intentional criminal use	Direct liability for misuse; Liability if knowingly using compromised systems; Responsibility for intentional criminal conduct	Liability for failure to implement safeguards post-deployment; Duty to monitor system operation; Liability for using high-risk AI negligently; Duty to report serious incidents	Liability for failure to establish safeguards; Duty to monitor operation; Liability for negligent deployment; Responsibility for incident reporting
Safeguard / Necessary Mitigation	Not explicitly mandated by law; Best practices voluntary; Limited safe harbor protections for reasonable efforts	Reasonable foreseeability standard; No explicit statutory safeguard requirements; Common law duties of care apply	State-of-the-art safeguards required; Conformity assessments mandatory; Risk assessments (DPIA) required; Documentation and auditing required; Monitoring systems required	Adequate safeguards required; Conformity assessments mandatory; DPIA required for high-risk systems; Audit trail documentation required; Incident monitoring systems

Dimensions of Analysis	United States	United Kingdom	Germany	France
Risk Predictability Standard	Foreseeability by reasonable person standard (case-by-case); High threshold for criminal mens rea; Specificity requirement for intended misuse	Natural and probable consequence standard; Foreseeability from skilled operator perspective; Reasonable foresight of risk	Vorhersehbarkeit standard - objective predictability; Reasonable expectation by developer/deployer; Risk assessment output determines liability threshold	Reasonable foresight standard; Predictability based on technical knowledge; Culpability if risks were known or should have been known
Corporate Accountability / Legal Entity	Vicarious liability possible; Depends on respondeat superior doctrine; Limited without explicit authorization	Corporate manslaughter/negligence principles; Director liability; Vicarious liability in limited circumstances	Strong Organisationsverschulden framework; Corporate liability for organizational failures; Culpability through defective decision-making; Collective responsibility possible	Corporate criminal liability under Article 121-2; Liability for organizational defects; Culpability through failure of supervision
Focus of Prosecution	Individuals (programmers, users, executives); Focus on intent and knowledge; AI-enabled fraud cases vs. traditional cybercrime	Individual prosecutions; Focus on direct perpetrators; Executives in severe cases; Traditional cybercrime framework applied	Both individual and corporate prosecution; Focus on failure of safeguards; Prosecution of developers AND deployers possible	Individual and corporate prosecution; Focus on culpable failures; Developer and deployer both targeted when appropriate
Special Regulations on AI Crimes	No specific AI crime statutes; General cybercrime laws applied; CFAA interpretations expanding; AI Fraud Prevention initiatives	No specific AI crime statutes; Computer Misuse Act applied broadly; Case law developing; ICO guidance on GDPR violations	AI Act implementation in StGB underway; Specific penalties for AI-related violations; High-risk system misuse provisions; Strengthened corporate liability	AI Act implementation; Specific criminal provisions for CSAM AI-generated; AI system misuse penalties; Expanded privacy protections

Discussion

The potential for criminal liability in cybercrimes that employ artificial intelligence exemplifies the fundamental tension between two predominant legal traditions worldwide, which are confronted with the challenge of technological innovation at an unprecedented pace. The fundamental differences between common law and civil law systems result in different approaches to criminal accountability mechanisms, the concept of fault, and the allocation of responsibility in the complex AI ecosystem (Ellamey & Elwakad, 2023).

In the common law systems of the United Kingdom and the United States, the framework of criminal liability is predicated on two constitutive elements that have served as the foundation of criminal responsibility for centuries: actus reus (criminal act) and mens rea (criminal intent). The initial element, actus reus, is relatively straightforward to attribute to sophisticated AI systems. AI systems, particularly in the context of cybercrime, can objectively perform acts that meet the technical definition of actus reus, whether in the form of commission or omission. To illustrate, when a software agent accesses a computer system without

authorization or exceeds authorized access, the act clearly fulfills the actus reus component of a cybercrime offense. However, the primary challenge in applying criminal liability to AI lies in the element of mens rea, which refers to the mental state or state of mind of the perpetrator at the time of committing the criminal act (Maskur et al., 2025).

The common law systems in the United Kingdom and the United States have developed three main models for determining criminal liability for AI-based crimes. The initial model is perpetration-via-another, wherein the AI system is regarded as an innocent agent or a mere instrument. In this model, the onus of criminal responsibility falls exclusively upon the programmer or user who utilizes AI to perpetrate the crime. The individual utilizing AI must possess the requisite mens rea for the crime in question, and the AI's actions can be attributed to the programmer or user as if they had committed the act themselves. This model is consistently applied in common law in both jurisdictions when third-party instruments are used to commit crimes (Hallevy, 2010).

However, the perpetration-via-another model has significant limitations when applied to highly sophisticated and autonomous AI systems. This model is not applicable in scenarios where artificial intelligence (AI) commits crimes based on the accumulation of its own experience and learning, rather than explicit instructions from programmers or users. This leads us to the second model, which is the natural-probable-consequence liability model. This approach is predicated on the premise that programmers or users may be held liable for crimes committed by AI if those crimes are the natural and probable consequences of their actions, even if they did not have the explicit intent to commit those crimes. This principle finds its roots in the doctrine of criminal negligence as established within the framework of traditional common law. Under this doctrine, individuals can be held liable for actions they did not personally commit, provided that these actions are the natural and probable consequences of their actions, and that these consequences would have been foreseeable to a reasonable person (King et al., 2020).

The third model is the direct liability model, in which the AI system itself is held criminally liable for crimes committed. The implementation of this model is contingent upon the fulfillment of two fundamental elements of criminal liability by the AI system: actus reus and mens rea. While actus reus can be relatively easily attributed to AI, the central question is whether AI can fulfill the prerequisites of mens rea as outlined by the applicable common law criminal jurisprudence principles. Legal theorists have posited that the requirements of cognition and volition that constitute mens rea in common law, namely knowledge and intent, can be attributed to AI systems at a certain level of abstraction. The capacity of AI to process sensory information, analyze it to form models of its environment, and perform calculations to predict the consequences of alternative actions can be said to demonstrate the presence of cognitive and volitional processes (Baeyaert, 2025).

Nevertheless, the direct implementation of the direct liability model encounters substantial challenges in both common law jurisdictions. The fundamental principle in criminal law that underpins the legal systems of both England and the United States is the requirement of culpability, which demands not only the commission of a criminal act but also the presence of moral agency or responsible agency. In practice, law enforcement agencies in both jurisdictions have adopted a more conservative position. In England, the majority of prosecutions for AI-related crimes target human actors who develop, configure, or use AI for criminal purposes, rather than the AI system itself. In a similar vein, the Computer Fraud and Abuse Act (CFAA) in the United States places a primary emphasis on individuals who utilize computer systems, including those with artificial intelligence components, to gain unauthorized access or exceed authorized access (Panattoni, 2025).

In contrast, the civil law systems implemented in Germany and France, as well as the overarching framework of the EU AI Act, adopt a philosophically distinct approach to criminal

liability for AI-based crimes. The EU AI Act explicitly states that criminal liability cannot be directly attributed to AI because these systems do not have legal personality, moral awareness, or the capacity to understand the legal implications of their actions. Consequently, the conceptual underpinnings of criminal liability continue to be firmly anchored in conventional legal subjects, namely individuals (natural persons) or legal entities (legal entities) implicated in the life cycle of AI systems (Staszkiewicz et al., 2024).

In civil law systems, the principle of distinguishing between providers and deployers plays a crucial role in the allocation of criminal responsibility. As delineated in the AI Act, providers encompass natural persons, legal persons, public authorities, agencies, or bodies engaged in the development of AI systems or general-purpose AI models. Conversely, deployers are entities that utilize AI systems under their authority. The allocation of criminal responsibility between these two parties determines who can be held accountable when the use of AI violates the provisions of the law.

In Germany, the framework for criminal liability is regulated by the Strafgesetzbuch (StGB), a comprehensive penal code that serves as the country's primary legislation. Despite the absence of explicit provisions within the StGB concerning AI crimes, the application of general principles remains a viable course of action in this particular context. The concept of Organisationsverschulden (organizational culpability) enables the imposition of criminal liability on legal entities in instances where their management or representatives engage in criminal activities that benefit the legal entity, or where there is negligence in supervision. In the context of AI, this liability arises if the leadership or management of the provider or deployer fails to implement adequate safeguards, does not exercise sufficient oversight, or does not report known serious incidents (Momsen, 2023).

The German legal system also acknowledges the notions of Kausalität (causality) and Vorhersehbarkeit (foreseeability), which play a pivotal role in determining culpability within the context of AI. The fundamental question pertains to whether the entity providing or implementing an AI system could have foreseen the possibility that its system might result in harm or be utilized for the commission of illicit criminal acts. The absence of criminal liability is predicated on the condition that the AI system has been developed in accordance with current standards and best practices, and that the provider or deployer has implemented reasonable safeguards. However, if there is evidence of gross negligence in the development or deployment, or if the provider or deployer knew or should have known of significant risks, then criminal liability may arise (Rutecka, 2025).

In France, the governance of AI criminal liability is dictated by the French Penal Code, which is principally governed by the principle of responsabilité pénale, as delineated in Article 121-3 of the Penal Code. The French legal system recognizes a form of criminal liability that is not predicated exclusively on intent, but rather encompasses a broader scope of liability that extends to culpa or negligence. Criminal liability may arise in the event that the provider or deployer neglects to implement adequate safeguards, fails to conduct appropriate conformity assessments, fails to monitor system operations after deployment, or fails to report serious incidents. France has established specific criminal provisions addressing AI-related crimes, such as the expanded interpretation of Article 227-23 on child sexual abuse material to include images generated or manipulated by AI (Ghigheci, 2019).

The philosophical distinctions between these two systems mirror a fundamental trade-off between flexibility and legal certainty. The common law system, characterized by its interpretive adaptability and evolution through case law, enables judicial authorities to respond to rapidly emerging technologies. However, this phenomenon engenders a concomitant uncertainty regarding the predictability of legal standards and the existence of inconsistencies across different legal jurisdictions. Conversely, the civil law system offers clarity and harmonization through explicit codification; however, it often exhibits a delayed

responsiveness to rapid technological change and is constrained by formal legislative processes (Paunio, 2009).

CONCLUSION

The philosophical differences between the common law and civil law systems result in contrasting but complementary approaches to regulating criminal liability for artificial intelligence-based cybercrimes. The common law systems in the United Kingdom and the United States rely on the flexibility of judicial interpretation through case precedents and the application of traditional doctrines such as actus reus and mens rea, developing three main models of liability, namely the perpetration-via-another model, the natural-probable-consequence liability model, and the model of direct liability for AI systems. However, practical application has primarily focused on the first and second models due to the fundamental difficulty in attributing mens rea to AI systems that lack moral consciousness or the ability to understand the legal implications of their actions. Meanwhile, the civil law systems in Germany and France, reinforced by the regulatory framework of the EU AI Act, adopt a more structured and codified approach by clearly distinguishing between providers and deployers, and applying the concepts of Organisationsverschulden in Germany and responsabilité pénale in France, which allow for criminal liability based on organizational negligence or failure to implement adequate safeguards.

Although the common law system offers greater adaptability to technological developments through the evolution of case law, it faces uncertainty in the predictability of legal standards and inconsistencies between jurisdictions. Conversely, the civil law system provides greater clarity and harmonization through explicit codification, but often shows a delay in responsiveness to rapid technological change due to the limitations of the formal legislative process. Key challenges faced by both systems include issues of attribution of responsibility in complex development-manufacturing-user chains, difficulties in proving a causal link between AI actions and resulting harm, and complexity in determining the degree of negligence or intent when AI systems act autonomously based on self-learning. The EU AI Act represents the first comprehensive attempt at the supranational level to explicitly regulate the obligations of providers and deployers, including the obligation to conduct risk assessments, maintain quality management systems, carry out post-market surveillance, and report serious incidents, with administrative sanctions of up to €35 million or 7% of global annual turnover for violations of prohibited AI practices.

These findings have significant practical implications for civil law countries in the Global South such as Indonesia, which are facing the need to adopt criminal legislation related to AI but often have limited jurisprudential foundations and institutional capacity. Key recommendations include the need to amend the Electronic Information and Transactions Law to accommodate specific liability for AI developers with clear criteria for attribution of fault, the development of due diligence obligations that are aligned with international best practices while still considering national legal principles, and institutional capacity building for effective law enforcement. This study also identifies the need for cross-jurisdictional harmonization given the transnational nature of cybercrime, where fragmentation of criminal liability frameworks allows perpetrators to exploit regulatory loopholes and engage in favorable forum shopping. Going forward, a hybrid approach is needed that combines the clarity of the civil law system with the adaptive flexibility of the common law system, accompanied by the establishment of stronger international cooperation mechanisms to address the challenges of law enforcement in an increasingly autonomous and complex AI era.

REFERENCE

Abbott, R. (2020). The Reasonable Robot (1st ed.). Cambridge University Press. https://doi.org/10.1017/9781108631761

Abbott, R. B., & Sarch, A. F. (2019). Punishing Artificial Intelligence: Legal Fiction or Science Fiction. UC DAvies Law Review, 53(1). https://doi.org/10.2139/ssrn.3327485

Abdelaziz, D. K. A. (2025). Criminal liability for the misuse and crimes committed by AI: A comparative analysis of legislation and international conventions. Journal of Infrastructure, Policy and Development, 9(1). https://doi.org/10.24294/jipd10722

Affagard, P., & Carvès, M. (2024). Cybersecurity Laws and Regulations France 2025. In ICLG - Cybersecurity Laws and Regulation (1st ed.). ICLG. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/france

Allahverdiyev, S., & Othman, M. (2022). "Verbandssanktionengesetz" — Corporate Liability for Germany? German Law Journal, 23(4), 637–649. https://doi.org/10.1017/glj.2022.37

Arnal, J. (2025). AI at Risk in the EU: It's Not Regulation, It's Implementation. European Journal of Risk Regulation. https://doi.org/10.1017/err.2025.19

Baeyaert, J. (2025). Beyond Personhood. Technology and Regulation, 2025. https://doi.org/10.71265/ssvg8a97

Barkane, I. (2022). Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance1. Information Polity, 27(2). https://doi.org/10.3233/IP-211524

Basu, N., & Dave, R. (2025). Comparative Analysis of Laws in AI. Journal of Lifestyle and SDGs Review, 5(3). https://doi.org/10.47172/2965-730X.SDGsReview.v5.n03.pe05575

Bertolini, A. (2025). Artificial Intelligence and Civil Liability. In Think Tank European Parliament. European Parliament. https://www.europarl.europa.eu/thinktank/en/document/IUST_STU(2025)776426

Burri, T. (2022). The New Regulation of the European Union on Artificial Intelligence. In S. Voeneky, P. Kellmeyer, O. Mueller, & W. Burgard (Eds.), The Cambridge Handbook of Responsible Artificial Intelligence. Cambridge University Press. https://doi.org/10.1017/9781009207898.010

Cortez, E. K., & Maslej, N. (2023). Adjudication of Artificial Intelligence and Automated Decision-Making Cases in Europe and the USA. European Journal of Risk Regulation, 14(3), 457–475. https://doi.org/10.1017/err.2023.61

Crawford, G. E., Juhan, J.-L., Kempe-Müller, S., Maclean, F. M., Rubin, M. H., Saarinen, M., & Wybitul, T. (2025, January 31). Upcoming EU AI Act Obligations: Mandatory Training and Prohibited Practices. Latham & Watkins. https://www.lw.com/en/insights/upcoming-eu-ai-act-obligations-mandatory-training-and-prohibited-practices

Davey, O. M., & Sauerwein, L. (2023). Deepfake In Online Fraud Cases: The Haze Of Artificial Intelligence's Accountability Based On The International Law. Sriwijaya Crimen and Legal Studies, 1(2). https://doi.org/10.28946/scls.v1i2.2654

de Lemos Campos, M. (2024). Comments on the Article Titled "The Regulation of AI Liability in Europe: A Critical Overview of Two Recent Directive Proposals – The (New) AILD and The (Revised) PLD" by Beatriz Garcia. E-Publica, 11(3). https://doi.org/10.47345/v11n3art3

Diamantis, M. E. (2020). The Extended Corporate Mind: When Corporations Use AI to Break the Law. North Carolina Law Review, 98(4). https://scholarship.law.unc.edu/nclr/vol98/iss4/6/

Duflot, A. (2024). Artificial Intelligence in the French Law of 2024. Legal Issues in the Digital Age, 5(1), 37–56. https://doi.org/10.17323/2713-2749.2024.1.37.56

Dyson, M. (2022). The Contribution of Complicity. The Journal of Criminal Law, 86(6). https://doi.org/10.1177/00220183221133439

Ellamey, Y., & Elwakad, A. (2023). The criminal responsibility of artificial intelligence systems: A prospective analytical study. Corporate Law and Governance Review, 5(1), 92–100. https://doi.org/10.22495/clgrv5i1p8

Garrett, B. L. (2025). Artificial Intelligence and Procedural Due Process. Penn Carey Law Journals, 27(5).

Ghigheci, C. (2019). Regulating negligence in French and Italian criminal law. Juridical Tribune, 9. https://www.tribunajuridica.eu/arhiva/An9vS/10.%20Cristinel%20Ghigheci.pdf

Giannini, A. (2023). Criminal behavior and accountability of artificial intelligence systems [Doctoral Thesis, Maastricht University]. https://doi.org/10.26481/dis.20231124ag

Gless, S., & Peralta, A. (2024). Discussion Paper on Criminal Liability Related to AI systems. https://rm.coe.int/cdpc-2024-09-ai-criminal-liability-discussion-paper-final-draft/1680b26f16

Hallevy, G. (2010). The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control. Akron Intellectual Property Journal, 4(2). https://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/1/

Hallevy, G. (2024). The Basic Models of Criminal Liability of AI Systems and Outer Circles. In D. M. Vicente, R. S. Pereira, & A. A. Leal (Eds.), Legal Aspects of Autonomous Systems (Vol. 4, pp. 69–82). CIDP. https://doi.org/10.1007/978-3-031-47946-5_5

Hargreaves, S. (2024). What has changed in the AI CSAM landscape? https://www.iwf.org.uk/media/drufozvi/iwf-ai-csam-report_update-public-jul24v12.pdf

Hashmi, M. A. I., Butt, M. F., Jawad, M., & Sultan, S. (2025). Criminal Liability in the Age of Autonomous Systems: Rethinking Mens Rea and Actus Reus. The Critical Review of Social Sciences Studies, 3(3). https://doi.org/10.59075/szbtkr93

Horder, J. (2022). Ashworth's Principles of Criminal Law. Oxford University Press. https://doi.org/10.1093/he/9780192897381.001.0001

Hutapea, N. M. S., Sitepu, D. K. C., Damanik, J., & Sianipar, S. K. L. (2025). Artificial Intelligence and Criminal Liability: A Preliminary Study within the Indonesian Legal System. JIHK, 7(2). https://doi.org/10.46924/jihk.v7i2.330

Jani, C. C., & Rathor, S. P. (2024). A Legal Framework for Determining The Criminal Liability And Punishment For Artificial Intelligence. Tuijin Jishu Journal of Propulsion Technology, 45(1). https://www.propulsiontechjournal.com/index.php/journal/article/view/4056

Janjeva, A. (2025, March 31). UK law enforcement inadequately equipped to tackle AI-enabled crime. The Alan Turing Institute. https://www.turing.ac.uk/news/uk-law-enforcement-inadequately-equipped-tackle-ai-enabled-crime

Jurgens, J., & Cin, P. D. (2025). Insight Report Global Cybersecurity Outlook 2025 . https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. Science and Engineering Ethics, 26(1), 89–120. https://doi.org/10.1007/s11948-018-00081-0

Lalchand, S., Srinivas, V., Maggiore, B., & Henderson, J. (2024, May 29). Generative AI is expected to magnify the risk of deepfakes and other fraud in banking. Deloitte. https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html

Lin, L. S. F. (2025). Organisational Challenges in US Law Enforcement's Response to AI-Driven Cybercrime and Deepfake Fraud. Laws, 14(4). https://doi.org/10.3390/laws14040046

Ma, J. (2024, August 18). The number of Fortune 500 companies flagging AI risks has soared 473.5%. Fortune.Com. https://fortune.com/2024/08/18/ai-risks-fortune-500-companies-generative-artificial-intelligence-annual-reports/

Makam, G. (2023). Criminal Liability of Robots- A Critical Analysis of the Legal Framework in the US, UK, and Europe. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4649764

Mantili, R., Putri, S. A., & Fakhriah, E. L. (2025). Compensation for Damages Caused by Artificial Intelligence under Indonesian Civil Law. Pena Justisia: Media Komunikasi Dan Kajian Hukum, 24(1). https://doi.org/10.31941/pj.v24i1.5164

Martin, K. (2025, May 27). AI Cyber Attack Statistics 2025. TechAdvisors. https://tech-adv.com/blog/ai-cyber-attack-statistics/

Maskur, M. A., Masyhar, A., Damayanti, R., Ramada, D. P., & Sanyal, S. (2025). Reimagining Criminal Liability in the Age of Artificial Intelligence: Toward a Comparative and Reform-Oriented Legal Framework. Journal of Law and Legal Reform, 6(4), 1805–1838. https://doi.org/10.15294/jllr.v6i4.35540

Mattia, C. (2024). Corporate Criminal Liability and Artificial Intelligence: Doctrinal Overview, Problems and Perspectives. Open Access Journal of Criminology Investigation & Justice, 2(1). https://doi.org/10.23880/oajcij-16000122

Maundrill, B. (2025, March 7). Majority of Orgs Hit by AI Cyber-Attacks as Detection Lags. Infosecurity Magazine.

Momsen, C. (2023). Implications and Limitations of the Use of AI in Criminal Justice in Germany. KriPoz, 1. https://kripoz.de/2023/01/19/implications-and-limitations-of-the-use-of-ai-in-criminal-justice-in-germany/

Nerantzi, E., & Sartor, G. (2024). 'Hard AI Crime': The Deterrence Turn. Oxford Journal of Legal Studies, 44(3). https://doi.org/10.1093/ojls/gqae018

Neuwirth, R. J. (2023). Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA). Computer Law & Security Review, 48. https://doi.org/10.1016/j.clsr.2023.105798

Osmani, N. (2020). The Complexity of Criminal Liability of AI Systems. Masaryk University Journal of Law and Technology, 14(1). https://doi.org/10.5817/MUJLT2020-1-3

Panattoni, B. (2025). Generative AI and Criminal Guilt. In Mimi Zou, C. Poncibò, M. Ebers, & R. Calo (Eds.), The Cambridge Handbook of Generative AI and the Law (1st ed., pp. 392–404). Cambridge University Press. https://doi.org/10.1017/9781009492553.027

Paunio, E. (2009). Beyond Predictability – Reflections on Legal Certainty and the Discourse Theory of Law in the EU Legal Order. German Law Journal, 10(11). https://doi.org/10.1017/S2071832200018332

Pehlivan, C. N. (2024). The EU Artificial Intelligence (AI) Act: An Introduction. Global Privacy Law Review, 5(Issue 1), 31–42. https://doi.org/10.54648/GPLR2024004

Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. Journal of Responsible Technology, 4. https://doi.org/10.1016/j.jrt.2020.100005

Rutecka, D. (2025, February 12). Liability for damages: the missing piece of the AI Act puzzle. Schoenherr. https://schoenherr.eu/content/liability-for-damages-the-missing-piece-of-the-ai-act-puzzle

Sachoulidou, A. (2024). AI Systems and Criminal Liability. Oslo Law Review, 11(1). https://doi.org/10.18261/olr.11.1.3

Sarch, A. (2024). Collective Knowledge and the Limits of the Expanded Identification Doctrine. Oxford Journal of Legal Studies, 44(4), 920–948. https://doi.org/10.1093/ojls/gqae025

Schuett, J. (2024). Risk Management in the Artificial Intelligence Act. European Journal of Risk Regulation, 15(2). https://doi.org/10.1017/err.2023.1

Selbst, A. D. (2020). Negligence and AI's Human Users. Boston University Law Review, 100(4). https://www.bu.edu/bulawreview/files/2020/09/SELBST.pdf

Simmler, M. (2024). Ensuring Accountability for Robots and AI under Criminal Law. In W. Barfield, Y.-H. Weng, & U. Pagallo (Eds.), The Cambridge Handbook of the Law, Policy, and Regulation for Human–Robot Interaction (pp. 798–812). Cambridge University Press. https://doi.org/10.1017/9781009386708.050

Soyer, B., & Tettenborn, A. (2022). Artificial intelligence and civil liability—do we need a new regime? International Journal of Law and Information Technology, 30(4). https://doi.org/10.1093/ijlit/eaad001

Staszkiewicz, P., Horobiowski, J., Szelągowska, A., & Strzelecka, A. M. (2024). Artificial intelligence legal personality and accountability: auditors' accounts of capabilities and challenges for instrument boundary. Meditari Accountancy Research, 32(7). https://doi.org/10.1108/MEDAR-10-2023-2204

Susila, M., & Salim, A. (2024). Cyber Espionage Policy and Regulation: A Comparative Analysis of Indonesia and Germany. PADJADJARAN Jurnal Ilmu Hukum (Journal of Law), 11(1), 122–144. https://doi.org/10.22304/pjih.v11n1.a6

TATARU, Ștefan R., & CREȚU, A.-C. (2024). Decoding The EU Artificial Intelligence Act: An Analysis Of Key Concepts And Provisions. Journal of Public Administration, Finance and Law, 31. https://doi.org/10.47743/jopafl-2024-31-33

Thaw, D. (2013). Criminalizing Hacking, not Dating: Reconstructing the CFAA Intent Requirement. Journal of Criminal Law and Criminology, 103(3). https://scholarship.law.pitt.edu/fac_articles/152/

Tual, M. (2025, July 24). Surge in AI-generated child sexual abuse images alarms advocacy groups and investigators. Lemonde. https://www.lemonde.fr/en/pixels/article/2025/07/24/surge-in-ai-generated-child-sexual-abuse-images-alarms-advocacy-groups-and-investigators_6743661_13.html

van Bekkum, M. (2025). Using sensitive data to de-bias AI systems: Article 10(5) of the EU AI act. Computer Law & Security Review, 56. https://doi.org/10.1016/j.clsr.2025.106115

Villasenor, J. (2021, June 7). Reining in overly broad interpretations of the Computer Fraud and Abuse Act. BVrookings. https://www.brookings.edu/articles/reining-in-overly-broad-interpretations-of-the-computer-fraud-and-abuse-act/