Journal of Innovations in Computer Science and Engineering
Shahid Beheshti Unversity

January 2025, Special Volume 2, Issue 2

Comparative Study of Criminal Responsibility of AI in the Legal Framework of Iran and Saudi Arabia

Zahra Meghdadi✉, Code ORCID: 0009-0001-4751-0433
Faculty of Law, Shahid Beheshti University, Tehran, Iran, z_meghdadi@sbu.ac.ir
Mahdi Pourcheriki, Code ORCID: 0009-0006-3240-0553
Faculty of Law and Political Science, University of Tehran, Tehran, Iran, mahdi.pourcheriki@ut.ac.ir

Abstract— This paper examines the legal frameworks governing the criminal liability of artificial intelligence (AI) in Iran and Saudi Arabia, focusing on how both countries address the evolving role of AI in criminal acts. With the rapid advancement of AI technologies—from narrow (weak) AI, which performs specific tasks, to general (strong) AI, capable of autonomous decision-making—complex legal and ethical questions have emerged. Specifically, this paper examines the applicability of three theoretical models of AI criminal liability: Perpetration-By-Another Liability, Natural-Probable-Consequence Liability, and Direct Liability.

The comparative analysis highlights that despite differences in legal traditions and societal contexts, both Iran and Saudi Arabia recognize that AI itself cannot bear criminal responsibility, and instead, liability is attributed to human actors, such as developers, users, and operators. The findings suggest that integrating technological progress with ethical and legal safeguards, grounded in Islamic jurisprudence, is essential for addressing the challenges posed by AI-related crimes in both jurisdictions.

Keywords—artificial intelligence, criminal liability, AI ethics principles, Saudi Arabia, Iran

I. INTRODUCTION

The rapid rise of artificial intelligence (AI) has transformed various aspects of human life, from automated systems in healthcare and finance to autonomous vehicles and smart cities. While these technological advancements promise greater efficiency and convenience, they also raise profound legal and ethical challenges. One pressing issue is how to attribute criminal liability when AI systems commit or facilitate criminal acts. The question of who—or what—should be held responsible when AI is involved in criminal behavior is no longer hypothetical but a reality that legal systems must address.

Existing research has explored various aspects of AI and criminal liability. For instance, a recent research, indicates organizations utilizing AI in Saudi Arabia can be held accountable for actions taken by autonomous systems [1]. However, the research does not address the criminal liability of artificial intelligence in Iran, leaving this aspect unexplored. Another study also conducts a comparative analysis between Iranian criminal law and the laws of the European Union [2]. However, this research and similar studies have not addressed the latest published documents on AI ethics in the Iranian legal system.

Furthermore, Scholars such as Gabriel Hallevy, in works like AI vs. IP: Criminal Liability for Intellectual Property Offences of Artificial Intelligence Entities, have examined potential models of liability, including direct and vicarious responsibility. This study has primarily focused on the theoretical implications of AI's potential to commit crimes independently, though there are some theoretical challenges in accepting certain aspects of these theories. In addition, none of these works offer a comparative analysis between two legal systems with their unique practical challenges. These challenges become even more significant in legal systems governed by distinct socio-legal principles, such as those of Iran and Saudi Arabia, where Islamic law plays a central role.

In this context, the primary research questions of this paper are:

1. What theoretical models of criminal liability for AI are applicable in the legal systems of Iran and Saudi Arabia? And,
2. What challenges and opportunities exist in implementing criminal liability frameworks for AI in these jurisdictions?

This paper first, provides an overview of the theoretical models of criminal liability for AI, including perpetration-by-another liability, natural-probable liability, and direct liability theories. Then offers a comparative analysis of the legal frameworks in Iran and Saudi Arabia. Finally, presents recommendations for refining these frameworks to ensure ethical and legal alignment with the rapid evolution of AI technologies.

Submit Date: 2025-04-30
Accept Date: 2025-05-05
✉ Corresponding author

By addressing these issues, this study aims to contribute to the global discourse on AI and criminal liability while offering insights specific to Iran legal system.

II. AI Criminal Liability models

Currently, three possible models of criminal liability for AI are theoretically conceivable. These models are: (1) Perpetration-By-Another liability, (2) Natural-Probable-Consequence Liability, and (3) direct liability for AI.

A. Perpetration-By-Another Liability

The foundation of this liability rests on the premise that artificial intelligence (AI) lacks any human characteristics. Accordingly, AI is considered as an innocent agent and is primarily viewed as an instrumental entity. While some of AI's capabilities are undeniable, these abilities are analogous to those of a legally incapacitated individual, such as a child, a mentally impaired person, or someone lacking the requisite criminal maturity.

When the physical act of a crime is committed by an innocent agent, the individual who caused the crime through the innocent agent bears criminal liability as the proximate cause superior to the direct perpetrator (causa proxima) [3]. In this context, liability arising from another's act is determined based on the physical conduct of the innocent agent and the mental element of the superior cause.

In such scenarios, the primary question concerning AI is: Who is responsible for the acts of AI? Two candidates are identified in response:

1. The programmer of the AI software, and
2. The end user of the AI system.

Under this model, the programmer and the user are fully criminally liable for the specific crime committed, whereas the AI entity itself bears no criminal liability. This approach, while advantageous in preventing impunity for criminal acts committed through AI, encounters limitations in addressing certain scenarios involving AI-related offenses.

The shortcomings of this model lie in its inability to adequately address the following situations:

1. When AI decides to commit a crime based on its accumulated experience or knowledge, even though its software was not programmed to perform criminal acts.
2. When the AI software was not designed to commit the specific crime in question, yet the AI commits it.
3. When AI acts not as a fully innocent agent but as a semi-autonomous entity, demonstrating a level of awareness or intentionality [4].

To resolve these issues, the natural-probable-consequence liability (Model 2) warrants further consideration. This alternative model acknowledges the evolving capabilities of AI systems and may provide a more comprehensive framework for addressing criminal responsibility in cases involving AI.

B. Natural-Probable-Consequence Liability

This model considers programmers or users deeply involved in the daily activities of artificial intelligence (AI) responsible for the actions of AI, even without any intent to commit a crime through AI. The foundation of this model lies in the idea that although the programmer may not intend to violate any law, others' rights are nonetheless violated as a result of AI's actions. In such cases, programmers or users have no knowledge of the committed offense; they do not program it, nor do they intend to commit a crime using AI. For such scenarios, the second model can provide a suitable legal response. This model is based on the ability of programmers or users to foresee the likelihood of crimes being committed.

According to this model, if a crime is the foreseeable and natural result of a person's behavior, that person can be held responsible for the crime. Originally, the model of responsibility based on the probable natural result was used to impose criminal liability on accomplices when one committed a crime that was neither planned by all parties nor part of a conspiracy. The established rule by courts and commentators is that the liability of an accomplice includes the actions of another accomplice if those actions are the Natural-Probable-Consequence of a criminal scheme encouraged or aided by the first accomplice. This concept has been widely accepted in laws and their amendments regarding accomplice liability [5].

It seems that the Natural-Probable-Consequence Liability model is legally suitable for conditions where AI has committed a violation, while the programmer or user neither had knowledge of the specific act nor intended it nor participated in it. This model requires negligence by the programmer or user, but nothing more. Programmers or users are not required to be aware of subsequent offenses that might occur due to their actions. However, if an reasonable programmer or user knows that such a violation could be the probable and natural result of their actions, they would then be held responsible. programmers or users must reasonably foresee this violation and prevent its occurrence by the AI.

The legal outcomes of applying the Natural-Probable-Consequence Liability model differ for programmers or users in two situations. The first situation is when programmers or users act negligently in programming or using AI, without any criminal intent to commit a crime. The second situation occurs when programmers or users deliberately and knowingly program or use AI to commit a crime but the AI deviates from that plan and commits a different or additional crime.

The first scenario is a pure example of negligence. The second scenario resembles the original idea of the Natural-Probable-Consequence Liability model in cases of accomplice liability. The inherent danger of the group or conspiracy aiming to commit a crime serves as a legal justification for imposing stricter liability on such groups. Consequently, under the Natural-Probable-Consequence Liability model, if programmers or users deliberately and knowingly use AI to commit a specific crime, and the AI

deviates by committing another or additional crime, programmers or users should also be held accountable for the additional crime as if it was knowingly and intentionally committed. However, the liability for the unplanned crime should be based on negligence, not intent [4, p 233].

Moreover, the claim that the AI's functionality could potentially be corrupted through malicious software that manipulates its algorithm and causes its misuse deserves consideration. Such a defense has been successfully employed in the UK, where an individual claimed that child pornography found on their computer was the result of malware operating without their knowledge. The presence of several Trojan programs on their computer led to their acquittal [6].

However, the remaining question is what the criminal liability of the AI itself is when the model of responsibility based on the Natural-Probable-Consequence is applied. Essentially, two possible outcomes exist. If the AI acted as an innocent agent, without any knowledge of the criminal prohibition, it would not be criminally responsible for the crime it committed. In such cases, the actions of the AI would not differ from those under the first model of AI responsibility (the perpetration-by-another model). However, if the AI did not merely act as an innocent agent but as a semi-autonomous one, in addition to the programmer or user's liability under the Natural-Probable-Consequence Liability model, the AI itself should also be directly held criminally responsible for the specific crime committed. This leads to the discussion of the third model of responsibility, namely direct liability.

C. Direct Liability

The premise of direct liability assumes that artificial intelligence (AI) operates independently, without reliance on any specific programmer or user. If an AI system can fulfill the requirements of both the physical (actus reus) and mental (mens rea) elements of a criminal act, there is no inherent barrier to imposing criminal liability on the AI itself. However, it can be argued that, prior to attributing the physical and mental elements to the perpetrator, another condition must first be established: the existence of legal personality in the perpetrator.

In essence, the perpetrator must first be recognized as possessing personality—either as a natural person or as a construct (e.g., legal persons)—before discussing rights, duties, and consequently, criminal liability. This very issue has historically arisen concerning legal persons, leading to the development of four primary theories: the realist theory, the fiction theory, the concession theory and the bracket theory [7].

Accordingly:

1. If personality is considered real, the perpetrator’s criminal liability exists naturally, resulting in direct liability, which requires only the commission of a criminal act by the perpetrator itself.

2. If personality is considered fictional, concessionary or under bracket, the perpetrator’s liability becomes indirect, requiring not only the fulfillment of the physical element by the perpetrator itself, but also additional factors, such as the responsibility of the programmer.

A critical point of distinction, however, emerges between AI and legal persons. While AI can be compared to legal persons in some respects, including deriving its liability from the actions of programmers or users, there is a fundamental difference: a legal person cannot act independently in the absence of a natural person representing it. Its liability must always stem from the actions of a natural person. In contrast, advanced AI systems can independently make decisions and commit physical acts based on those decisions.

This capability makes the acceptance of the realist theory for AI personality significantly more plausible than its application to legal persons.

Nevertheless, the legal personality of AI has not been recognized in either of the two legal systems under discussion. Consequently, the third model of AI criminal liability—based on recognizing AI’s legal personality—has not been adopted in either systems. However, this model remains a topic of theoretical exploration in legal doctrine, assuming the hypothetical acceptance of AI’s natural personality.

In this model, attributing criminal acts to AI is a plausible notion. For instance, in the case of a robot moving its arm to injure a nearby individual, accepting the commission of the physical element (actus reus) of an assault is acceptable. This acceptance is even more straightforward in cases of omission. As long as there is a duty to act, failure to perform the required act constitutes a legal basis for criminal liability.

However, the primary legal challenge in most cases concerns attributing the mental element (mens rea) of crimes to AI. AI does not need to independently conceptualize the commission of a specific crime to be held accountable. It suffices for the AI to knowingly and intentionally act in a manner that fulfills the real elements of a crime. This is because the essential mental state requirements for imposing criminal liability are knowledge and intent, or alternatively, negligence.

Knowledge is defined as the sensory perception of factual data and its understanding. [8] Most AI systems are equipped to acquire such knowledge through data input and sensory mechanisms. Furthermore, the process of analysis in AI systems resembles human cognitive processing.

Regarding specific intent, which is considered the strongest form of mens rea, it is argued that goal-setting is not exclusive to humans. AI systems may be programmed to set and pursue specific objectives or, in the case of advanced AI, autonomously identify goals and take actions to achieve them. In either scenario, such goal-directed behavior could qualify as specific intent.

A counterargument suggests that many crimes result from strong emotions or feelings, such as love, hate, or jealousy, which are inherently human and cannot be replicated by even the most advanced AI. While this observation may hold true for early 21st-century AI technologies, such emotional states are rarely essential elements in most crimes. Only a limited number of offenses, requiring specific emotional states, may not permit attributing mens rea to AI.

For instance, in most jurisdictions, property crimes do not require specific intent but only knowledge and willfulness, both of which are often achievable by AI systems. Advanced algorithms are capable of distinguishing between lawful and unlawful acts, enabling them to recognize whether a particular act constitutes a crime or is permissible.

If criminal liability can be established for programmers and/or users via other legal frameworks, such liability does not exclude or replace the criminal liability of the AI entity itself. However, the criminal liability of an AI entity is not contingent on the liability of its programmer or user.

For example, if one AI system manipulates another, the former AI could be held directly liable, while the initial programmer of the latter system would not necessarily bear responsibility. This distinction underscores the independent potential for attributing direct criminal liability to advanced AI systems.

III. The Legal Framework of Saudi Arabia

Artificial intelligence serves as a cornerstone of Saudi Arabia's Vision 2030 initiative, with 66 out of the 96 strategic objectives in the plan focused on AI and data. The strategy encompasses international investments, fostering domestic AI enterprises, and establishing a regulatory framework aimed at positioning Saudi Arabia as a leader in AI adoption and innovation [9].

To spearhead these efforts, Saudi Arabia established the Saudi Data and Artificial Intelligence Authority (SDAIA), tasked with advancing the national Data & AI agenda and positioning the Kingdom as a global leader in data-driven economies. SDAIA has developed the National Strategy for Data & AI, which aims to encourage AI adoption by cultivating a collaborative ecosystem that promotes the commercialization and industrial application of AI and data [10]. Additionally, SDAIA oversees the National Center for Artificial Intelligence, responsible for conducting AI research, providing strategic guidance to the government, and raising public awareness of AI.

In 2023, two significant developments shaped Saudi Arabia's AI-related legal framework. First, in April, the Saudi Authority for Intellectual Property (SAIP) released a draft of amendments to intellectual property legislation for public consultation. These proposed changes sought to unify existing IP laws and included a dedicated section on intellectual property rules for AI and emerging technologies, aimed at fostering innovation in the AI domain.

But on the subject of AI criminal responsibility, what is more important is the AI ethics principles. In September 2023, SDAIA issued the final version of its AI Ethics Principles (Version 1.0), marking the country’s first AI-focused legal framework. These principles define AI ethics as a set of values, principles, and techniques designed to ensure the ethical development and use of AI technologies [11].

The AI Ethics Principles require entities and individuals to adopt certain standards and ethics when developing and using AI-based systems, These principles are:

1) Fairness, 2) Privacy & Security, 3) Humanity, 4) Social & Environmental Benefits, 5) Reliability & Safety, 6) Transparency & Explainability and 7) Accountability & Responsibility.

However these principles are morally imperative, no specific penalties are set out for non-compliance with the relevant rules. Nevertheless, the legal framework of Saudi Arabia includes rules on liability that may be triggered by the development and use of AI and AI systems through other acts and regulations; below are some examples of how AI Ethics Principles may come to force through these rules:

1) the Personal Data Protection Law (PDPL) includes various penalties for non-compliance, which could be triggered where personal data is processed for AI purposes.

It is worth mentioning that, similar to many data protection laws around the world, the PDPL and its regulations are heavily influenced by a European Union regulation on information privacy in the European Union (EU) and the European Economic Area (EEA), namely, the General Data Protection Regulation (GDPR), especially in terms of fundamental concepts like definitions and data subject rights. [12]

Currently, the Saudi Authority for Data and Artificial Intelligence (SDAIA) serves as the Competent Authority responsible for overseeing the implementation of the PDPL and its regulations. SDAIA has the authority to request documents or information from entities to ensure their compliance. Key enforcement powers under the PDPL include the following:

a. The PDPL designates a distinct category of personal data known as "sensitive data." This category encompasses personal data that reveals racial or ethnic origin, religious, intellectual, or political beliefs, security information, data related to criminal offenses, biometric or genetic information, health data, and information indicating that an individual’s parentage is unknown. The PDPL imposes stricter requirements and limitations on the processing of sensitive data. For instance, organizations cannot rely on “legitimate interest” as a lawful basis for processing sensitive data, nor can sensitive data be used for marketing purposes. [13]

According to Article 35(1) of PDPL: disclosure of sensitive data in breach of the PDPL with the intention to cause harm to the relevant data subject or to gain a personal benefit may result in up to two years' imprisonment or a fine of up to 3 million riyals, or both;

This article may be interpreted as relating to the second principle of AI Ethics Principles, namely, Privacy & Security. The privacy and security principle embodies the core values that AI systems must uphold. These systems should be designed to prioritize safety, safeguard the privacy of collected data, and implement robust data security measures to ensure confidentiality and prevent breaches. [11]

b. Cross-border data transfer (CBDT) is subject to strict regulations through PDPL. As a result, companies are required to establish independent IT facilities or infrastructure in the kingdom of Saudi Arabia to protect and isolate the data from other jurisdictions.

In this regard, one other penalty envisaged through PDPL is a fine of up to 1 million riyals for violation of data transfer provisions (including CBDT). [14] This protection also may be understood under some AI Ethics principles such as Privacy & Security, or Reliability & Safety.

c. There are also some additional penalties and compensations considered in PDPL such as a warning notice or a fine of up to 5 million riyals, for all other matters of non-compliance with PDPL rules (Article 36), compensation claims for material or moral damage for individuals (Article 40), and a confiscation order of funds obtained as a result of a violation (Article 38). All repeat offences may also be doubled.

2) Under the Copyright Law, liability for infringement can result in various penalties, including a warning, a fine of up to 250,000 riyals, closure of the infringing entity for up to two months, confiscation of infringing materials, or imprisonment for up to six months for a first-time offense and these penalties may be doubled for repeat offenses. Such sanctions apply if background content infringes on third-party intellectual property rights or exceeds the scope of permitted use. [15]

This can be understood in relating to the fifth and seventh principles, i.e. Reliability & Safety, and Accountability & Responsibility.

Safety ensures that AI systems do not present a risk of harm or danger to individuals or society. For example, autonomous vehicles could endanger lives if they fail to accurately recognize living beings, are not trained for specific scenarios, or experience system malfunctions.

The Accountability and Responsibility principle assigns ethical responsibility and liability to all stakeholders involved in AI systems, including designers, vendors, procurers, developers, owners, and assessors. These parties are accountable for the decisions and actions of the AI system, particularly when they pose potential risks or cause harm to individuals and communities. To mitigate these risks, effective safeguards and control mechanisms must be implemented to prevent misuse and ensure responsible use of the technology. [11]

3) The Saudi Anti-Cyber Crime Law sets strict penalties for a range of actions categorized as cybercrimes, aiming to protect individuals and organizations from harm caused through digital means. Under this law, offenders may face fines of up to 3 million riyals for engaging in prohibited activities, such as using technology to harm others. This legal framework also recognizes the evolving nature of cyber threats, including those posed by artificial intelligence. If AI systems are employed to commit such offenses, the same stringent penalties may apply, emphasizing the country's commitment to addressing both traditional and emerging cyber risks. By enforcing these measures, Saudi Arabia seeks to ensure a safer digital environment while adapting to the challenges posed by advancing technology.

Accordingly, it can be said that under the current legal system of Saudi Arabia, criminal acts committed through AI or in connection with its development and use may result in criminal liability for individuals or entities that use or develop AI. Therefore, it can be concluded that the only accepted theory regarding criminal liability for AI and related crimes within the Saudi legal framework is the first theory, namely, perpetration-by-another liability.

This idea is also supported by another research mentioned before, exploring the criminal liability of organizations utilizing AI and autonomous systems. Accordingly, in most cases, the manufacturers and the engineers of the autonomous systems are held criminally responsible [1, p 15].

IV. The Legal framework of Iran

Criminal liability in the Iranian legal system, based on Islamic Jurisprudence and Article 140 of the Islamic Penal Code, is contingent upon the presence of three characteristics: intellect, maturity, and free will. Accordingly, only when these three elements exist, and provided that the mental and physical elements of a crime are established, can an individual be held liable for a criminal offense. Furthermore, if the representative of a legal person meets the criteria set forth in Article 140, legal persons may also be held criminally liable under Articles 143 and 747 of the same Code. [16]

Nevertheless, this framework, together with the principle of legality in criminal law, underscores that recognizing any form of legal personality and liability depends on their prior acknowledgment in enacted legislation. Consequently, despite the theoretical possibility of recognizing artificial intelligence (AI) as possessing a form of real personality—and thereby attributing criminal liability to it—the direct attribution of criminal liability to AI is not feasible under the current laws of the Iranian legal system.

However, adopting the first model, namely perpetration-by-another liability, and treating AI as a tool or an entity akin to a child or insane, human actors involved in its conduct can be held responsible. This approach implies that if AI is used as an instrument to commit criminal acts, its user or programmer may be held accountable for the AI's criminal behavior.

At the same time, none of the specific behaviors of AI have, to date, been independently criminalized under Iranian law. The most significant document addressing this subject is the National Artificial Intelligence Document of the Islamic Republic of Iran, approved by the Supreme Council of the Cultural Revolution on August 10, 2024.

Pursuant to Article 1 of this document, AI ethics are defined as "a set of ethical principles guiding the responsible and value-based development and use of AI technologies, consistent with Islamic values, to be observed by experts and other individuals in the design, production, and utilization of AI, thereby establishing mutual rights."

One of the significant issues highlighted in this document is the protection of individuals' privacy. This matter is explicitly mentioned in Article 1 of the document as an example of AI ethical concerns and reiterated in Article 2 under the title "Principles and Value Foundations."

Other examples of ethical issues concerning AI, as outlined in this document, include: respecting individual and social rights, ensuring social security, fairness, explainability, transparency, non-discrimination and impartiality, accountability, alignment with the values and norms of Islamic society, responsibility, trustworthiness, and preventing misuse of technology.

Although no explicit enforcement mechanisms are prescribed in this document (since the issuing authority lacks the jurisdiction for criminalization) or in other laws, a comparative approach to the Saudi legal system could inspire the enactment of criminal laws to protect the values, such as privacy endorsed in this document. As observed, the Saudi legal system, by enacting laws that support the values emphasized in AI ethical principles, has indirectly provided enforcement mechanisms against violations of these values.

In this regard, reference can be made to the approval of the Personal Data Protection Bill by the Iranian Cabinet on July 13, 2024. While this legislation is still in its early stages and lacks a comprehensive framework, its adoption marks a significant step toward AI governance in Iran.

ACKNOWLEDGMENT

Christian Lous Lange, the renowned Norwegian historian and Nobel laureate, aptly remarked that "Technology is a useful servant but a dangerous master" [17]. Given the dual nature of AI as both an enabler of progress and a potential source of harm, it is imperative to consider legal frameworks that address the following challenges:

1. The necessity of defining the legal status and criminal liability of artificial intelligence under the Islamic Penal Code, whether as an autonomous entity or a mere tool.

2. The establishment of robust enforcement mechanisms and regulatory bodies to safeguard individuals' privacy throughout AI operational processes.

3. Considering the rapid advancements in AI, particularly its decision-making and perception capabilities, when drafting legislation to mitigate risks associated with strong AI.

By addressing these legal challenges proactively, societies can harness the benefits of AI while minimizing its risks, ensuring both technological progress and social justice.

At the end, it is suggested that in a separate study, the ethics of artificial intelligence in Iran and Saudi Arabia be compared in detail. Furthermore, the potential regulations that Iran could develop in the future could also serve as a subject for further research.

REFERENCES

[1] M. F. S. Diab, "Criminal Liability for Artificial Intelligence and Autonomous Systems," *American Journal of Society and Law*, vol. 3, no. 1, pp. 14–18, Apr. 2024.

[2] M. H. Kaveh and M. Barani, "Criminal Responsibility of Artificial Intelligence in Iranian Criminal Law with a View to European Union Laws," *Journal of Comparative Criminal Jurisprudence*, vol. 4, no. 3, pp. 51–61, Sep. 2024.

[3] M. Kumar Sahu, "The Rule of Causa Proxima as a Principle of Insurance," *KSL Review*, vol. 4, no. 1, p. 156, 2015.

[4] G. Hallevy, "AI vs. IP, Criminal liability for intellectual property offences of artificial intelligence entities," in *artificial intelligence and the law cybercrime and criminal liability* , D. J. Baker and P. H. Robbinson, Eds., 2021, p. 231.

[5] W. L. Clark, W. L. Marshall, and M. Q. Barnes, *A Treatise on the Law of Crimes*. 1967.

[6] S. W. Brenner, B. Carrier, and J. Henninger, "The Trojan Horse Defense in Cybercrime Cases," *Santa Clara Law Digital Commons*, 2024. https://digitalcommons.law.scu.edu/chtlj/vol21/iss1/1 (accessed Nov. 30, 2024).

[7] "Corporate Personality: Theories of Corporate Personality," *Toppr-guides*, May 29, 2019. https://www.toppr.com/guides/legal-aptitude/jurisprudence/corporate-personality

[8] W. James, The Principles of Psychology. 1890.

[9] Vision 2030, "Overview," *Vision2030.gov.sa*, 2016. https://www.vision2030.gov.sa/en/overview

[10] SaudiPedia, "National Strategy for Data and AI (NSDAI)," *Saudipedia*, Oct. 28, 2024. https://saudipedia.com/en/article/2878/economy-and-business/data-and-ai/national-strategy-for-data-and-ai-nsdai

[11] "Saudi Arabia: Saudi Data and Artificial Intelligence Authority reveals AI Ethics Principles 2.0," *insightplus.bakermckenzie.com*. https://insightplus.bakermckenzie.com/bm/data-technology/saudi-arabia-saudi-data-and-artificial-intelligence-authority-reveals-ai-ethics-principles-20

[12] S. A.-S. Yildiz Hakki Can, "Saudi Arabia's Data Protection Law and Regulations Come Into Effect," *Cleary Cybersecurity and Privacy Watch*, Jan. 17, 2024. https://www.clearycyberwatch.com/2024/01/saudi-arabias-data-protection-law-and-regulations-come-into-effect/

[13] PwC, "KSA Personal Data Protection Law Series: Part 1," PwC Middle East, [Online]. Available: https://www.pwc.com/m1/en/blogs/pdf/ksa-personal-data-protection-law-series-part-1.pdf. Accessed: Nov. 30, 2024.

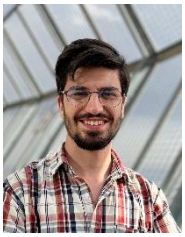
[14] KPMG, "The Path Toward Robust Data Protection Compliance," KPMG Saudi Arabia, 2023. [Online]. Available: https://assets.kpmg.com/content/dam/kpmg/sa/pdf/2023/the-path-toward-robust-data-protection-compliance.pdf. Accessed: Nov. 30, 2024.

[15] K. Silverman, "In Depth: Artificial Intelligence Law," *Lexology*, p. 10, 2024.

[16] *Majlis.ir*, 2024. https://rc.majlis.ir/fa/law/show/845048 (accessed Nov. 30, 2024).

[17] C. Lange, "The Nobel Peace Prize 1921," *NobelPrize.org*, Dec. 13, 1921. https://www.nobelprize.org/prizes/peace/1921/lange/lecture/

زهرا مقدادی:
کد ارکید: https://orcid.org/0009-0001-4751-0433
متولد ۱۳۷۸
مدال طلای المپیاد کشوری ادبی ۱۳۹۶
دانش آموخته کارشناسی دانشگاه تهران (دانشجوی برتر استعدادهای درخشان)
دانش آموخته کارشناسی ارشد حقوق جزا و جرم شناسی دانشگاه تهران
دانشجوی دکتری حقوق کیفری و جرم شناسی دانشگاه شهید بهشتی



مهدی پورچریکی:
کد ارکید: https://orcid.org/0009-0006-3240-0553
متولد ۱۳۷۶
دانش آموخته کارشناسی دانشگاه تهران (رتبهٔ ۲۶ سراسری)
دانش آموخته کارشناسی ارشد حقوق جزا و جرم شناسی دانشگاه تهران (رتبهٔ ۴ سراسری)