Journal of Human Security | 2025 | Volume 21 | Issue 2 | Pages 14-18
DOI: https://doi.org/10.12924/johs2025.210203
ISSN: 1835–3800

Journal of Human Security

Research Article

The Basis of Civil Liability for Damages Caused by Artificial Intelligence in Light of General Legal Theory: Comparative Study

Yasar Alhiniti[1], Hanae Sadrati[2], Omar Almakhzoumi[3], Majed Falah Alsarhan[4], Hani Aljahdali[5]

[1]Faculty of Law- Zarqa University, Zarqa, jordan. Email: valhunieti@zu.edu.jo
[2]Faculty of Law- University of Sidi Mohamed Ben Abdellah – Morocco. Email: Hanaesadrati1996@gmail.com
[3]Faculty of Law- Zarqa University, Zarqa, jordan. Email: omakhzoumi@zu.edu.jo
[4]Faculty of Law- Zarqa University, Zarqa, jordan. Email: Malsarhan@zu.edu.jo
[5]College of Law, University of Business & Technology, Jeddah, Saudi Arabia. Email: h.aljahdali@ubt.edu.sa

***Correspondence:** valhunieti@zu.edu.jo

Submitted: 25 August 2025 | Revised: 30 October 2025 | Accepted: 25 November 2025 | Published: 23 December 2025

Abstract: The progressive incorporation of artificial intelligence (AI) into information and communication technologies (ICT) has significantly reshaped contemporary social and professional life. In the current digital environment, computers, internet infrastructures, and AI-driven systems are extensively deployed across multiple sectors. However, alongside the accelerated expansion of AI and information technologies, cybercrime has become an increasingly prominent phenomenon, posing serious risks to the privacy and security of individuals, communities, institutions, and states. Despite its substantial advantages, AI has generated considerable legal and regulatory challenges, particularly in relation to cybercrime and civil liability. This study explores the function of AI within ICT and analyses the ways in which technological advancement contributes to cyber-related threats. It further examines the conceptual foundations of civil liability and assesses how responsibility for harm caused by AI systems is addressed within Moroccan, British, and French legal frameworks. Through a comparative approach, the research evaluates traditional, contractual, and objective civil liability models as they apply to AI-induced damage. Particular attention is given to the Moroccan Civil Obligations Code (MOCC), which establishes the basis for liability, and its comparison with corresponding provisions in British and French law, highlighting their principal strengths and legal implications. The findings indicate that existing civil liability regimes remain capable of offering lawful and equitable compensation mechanisms when adapted to the complex characteristics of AI technologies. The study ultimately underscores the pressing need for Morocco to align its legislative framework with international cooperation initiatives and comparative legal models in order to effectively address the emerging challenges associated with artificial intelligence.

Keywords: Artificial Intelligence, Civil Liability, Contractual Fault, Tort Law, Objective Liability, Legal Theory

1. Introduction

The field of information technology has progressively broadened its scope, exerting substantial influence across social, economic, legal, and intellectual domains [1]. A central and defining component of this evolution is artificial intelligence (AI), which has profoundly reshaped human perspectives by redefining rational decision-making processes [2]. Machine-driven AI has generated notable advantages through developments in robotics, social engineering applications, and automated decision-making mechanisms [3; 4]. Similarly, the convergence of AI technologies with internet-based services represents a transformative force within contemporary society [5]. Nonetheless, the widespread adoption of AI-driven systems has intensified concerns related to security risks and liability for harm, particularly where accountability for damage remains uncertain [6]. The absence of a coherent and systematic legal framework presents serious difficulties in attributing responsibility and ensuring adequate remedies for individuals adversely affected by AI-related damage [7; 8].

Despite the extensive innovations introduced by AI, its application has also produced significant adverse implications across multiple aspects of human life. The integration of AI into cyberspace has altered the nature and scale of its use, creating heightened threats to social security through the proliferation of cybercrime [9]. Cybercrime extends beyond attacks on isolated information systems and has a broader detrimental impact on the digital environment as a whole [2]. Cyberattacks typically involve intrusions into software systems, computer networks, and websites, thereby undermining individual security within society [10; 11]. The growing prevalence of such attacks has led to their recognition as forms of organised crime, encompassing cyber espionage, cyberterrorism, and financially motivated offences such as electronic money laundering through online banking platforms [2]. Unlike conventional criminal activities, these technologically enabled offences are inherently transnational and closely linked to automated data-processing infrastructures [4]. They are frequently perpetrated by highly skilled technical specialists, commonly referred to as cybercriminals. Research by Romagna and Leukfeldt [5] indicates that cybercriminals increasingly rely on AI-based tools to enhance malware deployment and generate deceptive digital content for extortion purposes. Such practices substantially reduce operational costs while increasing both efficiency Tarrad [6] and precision in cyberattacks [12], thereby adversely affecting individuals, communities, institutions, and corporate entities.

Given the rapid escalation of transnational cybercrime, the establishment of structured and effective mechanisms to deter cybercriminal activity has become essential for safeguarding societal well-being [13]. In the context of AI, cybercrime is often executed through autonomous algorithms that operate without direct human involvement, creating complex challenges in ensuring justice and fair compensation for injured parties. Within general legal theory, civil liability is understood as a mechanism designed to protect fundamental rights by securing justice for aggrieved individuals and providing appropriate compensation from responsible actors [14]. Consequently, international agreements play a crucial role in limiting and combating cybercrime, and states that develop effective regulatory frameworks benefit significantly from international cooperation in this domain.

As AI-based tools continue to pose serious risks to civil security, both technical and legal challenges associated with AI systems, cybercrime, and internet governance have intensified [8]. The expanding threat of cybercrime, fuelled by rapid advancements in communication technologies, has contributed to the globalisation of criminal activity. New categories of offences have emerged, including defamation, cyberstalking, cyberterrorism, malware dissemination, phishing, and social engineering, many of which are conducted remotely and, in some cases, without direct human intervention [15]. Although these crimes constitute a global threat, no single state possesses the capacity to comprehensively detect, monitor, and suppress cybercrime independently [13]. The inherently transnational

© 2025 By the Authors. This Open Access Article Was Published Under a Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/).

character of cybercrime necessitates international cooperation at the operational level as the primary means of effective enforcement and prevention [1]. Accordingly, cybercrime represents an urgent global challenge that requires coordinated cross-border communication and shared responsibility in identifying and prosecuting offenders.

This study examines the significance of international cooperation and analyses how states respond through regulatory frameworks aimed at mitigating cybercrime. It further seeks to investigate civil liability for damage caused by AI systems within the context of general legal theory. To achieve this objective, a comparative analysis is undertaken between the Moroccan, British, and French legal frameworks.

2. Literature Review

2.1 Historical Context

From the 1960s onwards, cybercrime has developed in parallel with the expanding use of computers, internet technologies, and later smartphones [9]. During the period between 1960 and 1970, the protection of computer systems and personal data primarily relied on physical safeguards, including restricted access and secured facilities. However, the subsequent decade introduced far more complex challenges in securing personal and financial information [1]. The emergence of ARPANET provided practical exposure that enabled hackers to exploit system vulnerabilities and extract sensitive data. In 1975, the publication entitled “The protection of information in computer systems” underscored the growing importance of cybersecurity measures, particularly user authentication and access control mechanisms [13]. The formal development of the internet in 1983 further intensified security risks, enabling state-level cyber intrusions, including attacks on confidential military records in the United States.

By 1988, cybercrime had assumed an international dimension when hackers succeeded in stealing approximately $70 million from the National Bank of Chicago. In the same year, Carnegie Mellon University established the first Computer Emergency Response Team (CERT) to mitigate cyber threats and respond to incidents more effectively [16]. Between 1989 and 1990, cyber threats remained relatively limited; nevertheless, the Council of Europe’s ministerial committee committed to adopting Recommendation No. 9, aimed at addressing emerging computer and internet-related crimes [17].

The 1990s marked a significant escalation in cybersecurity risks with the appearance of malware and computer viruses, alongside unauthorised intrusions into systems belonging to NASA and the United States government [14]. In 1998, a Russian hacker group orchestrated the transfer of approximately $10 million from Citibank into overseas accounts, highlighting the vulnerabilities of international financial systems. In response, governments across multiple jurisdictions initiated substantial legislative reforms and amendments to counter cybercrime more effectively [16]. The early 2000s witnessed accelerated globalisation, particularly within the banking sector, which coincided with a surge in cyberattacks targeting online financial data and credit card information [8]. This period was characterised by frequent attacks on multinational corporations and international organisations, revealing serious weaknesses in security infrastructures. Consequently, states implemented enhanced protective measures, including two-factor authentication, encryption protocols, fraud detection systems, and firewalls to safeguard financial transactions and sensitive official records [9]. Although the Council of Europe adopted the Convention on Cybercrime in 2001, inconsistent implementation across jurisdictions contributed to continued cyber incidents and substantial financial losses.

In 2007, large-scale cyberattacks on Estonia’s governmental and institutional systems exposed the destructive potential of cybercrime and prompted states worldwide to prioritise cybersecurity policies. This decade experienced increasingly sophisticated and aggressive state-sponsored attacks, accompanied by the expansion of cyber weapons and supporting infrastructures. Notable ransomware incidents, such as WannaCry and NotPetya, caused extensive global disruption and economic damage [18]. In response, advanced security strategies, including intrusion detection systems (IDS), intrusion prevention systems (IPS), zero-trust architectures, and intelligence-sharing frameworks, were introduced to strengthen national security and improve incident response capabilities. During the 2020s, cybercrime has intensified further with the integration of AI-based technologies [19]. Generative AI has amplified cyber threats by enabling sophisticated social engineering tactics and fully automated attacks, leading to supply chain compromises and an increase in financial fraud. These developments have reinforced the imperative to secure digital infrastructures, prompting Morocco to ratify bilateral and international judicial cooperation agreements aimed at combating cybercrime [18]. Additionally, Article 713 of the Moroccan Code of Criminal Procedure explicitly addresses the protection of individual privacy against cyber-related offences.

As technological advancements continue to transform the world into an increasingly interconnected environment, cybersecurity risks and threats are correspondingly expanding. In the later stages of the 2020s, developments in quantum computing and cloud-based platforms have further intensified cyber threats by facilitating more efficient fraud, extortion, and malware dissemination [20]. Addressing these evolving risks requires the integration of robust regulatory mechanisms, widespread public awareness initiatives, and sustained international cooperation. Accordingly, states must adopt a comprehensive multidisciplinary approach to effectively confront and mitigate cybercrime.

2.2 2.2 Concept and Categorization of Cybercrime

Cybercrime can be understood as conduct that causes harm through the use of computer systems or digital technologies [13]. As technological innovation continues to advance, cybercrime increasingly manifests in novel forms that often fall outside rigid or traditional legal classifications. Marelino [20] characterises cybercrime as unlawful computer-related activities facilitated through electronic networks and influenced by third-party actors. Despite extensive international discourse, no single, universally accepted definition of cybercrime or cybersecurity has been formally adopted. The United Nations, while addressing cybersecurity within its manuals and policy instruments, has similarly refrained from establishing a definitive and uniform conceptualisation [9]. In analytical and regulatory contexts, cybercrime is commonly categorised according to both its target and its method of execution. From the perspective of targets, such offences may be directed at individuals, property, organisations, or society at large. In terms of methods, cybercrime encompasses practices such as malware deployment, social engineering techniques, and network-based attacks.

2.3 Civil Liability and Its Type to Damages

Civil liability is commonly understood as a legal obligation imposed on a wrongdoer to bear the consequences arising from unlawful conduct. Such an obligation is typically enforced through a judicial decision requiring an individual to provide compensation for harm caused by their actions or omissions [21]. Within the framework of general legal theory, civil liability is established when three cumulative elements are present: the existence of misconduct or a wrongful act, such as fraud or breach of an agreement; the occurrence of damage; and a causal link connecting the wrongful conduct to the resulting harm [22]. In the context of cybercrime involving artificial intelligence technologies, multiple forms of civil liability may arise in response to damage caused by technologically mediated conduct. Civil liability is generally invoked where a legal duty has not been fulfilled in a manner that ensures justice and fairness.

Civil liability may be categorised according to its legal source, most notably into contractual, tortious, and objective liability regimes [23]. Contractual civil liability arises where parties fail to discharge obligations established under a valid contract, either through non-performance or defective performance. This form of liability is typically confined to compensating damages linked to fraud or moral obligations arising from the contractual relationship [14]. Tortious civil liability, by contrast, is triggered when one party causes harm to another through unlawful conduct or the violation of legal norms, independent of any contractual relationship [24]. It encompasses both intentional and unintentional acts and extends to moral as well as material damage. Objective liability, finally, is imposed without the need to demonstrate fault or negligence, focusing instead on the existence of legally attributable harm. This form of liability is commonly associated with activities involving defective products, hazardous machinery, or inherently dangerous substances [17]. Accordingly, civil liability within general legal theory operates as a structured mechanism for the allocation of risk and the determination of legal accountability.

2.4 Civil Liability for Damages Caused by Artificial Intelligence

Artificial intelligence has undeniably transformed nearly every sphere of human activity; however, this rapid development has also intensified concerns regarding the protection of individual privacy. The deployment of AI systems has generated significant public liability for harm, necessitating regulatory responses from states at both national and international levels. Within the Moroccan legal framework, Article 77 of the Moroccan Code of Obligations establishes a general principle of civil liability, providing that any act committed by an individual, whether intentional or unintentional, which causes harm to another, gives rise to an obligation to repair the resulting damage [25]. This provision further extends to situations in which harm is inflicted through the use of AI-based technologies, thereby

requiring the responsible party to provide compensation for the damage incurred [26].

Similarly, under French law, Article 1242 of the French Civil Code affirms that individuals are legally responsible for compensating damage arising from their personal conduct, moral fault, or fraudulent actions [13]. This responsibility equally applies where harm is caused through the deployment or operation of AI technologies, obliging the relevant actor to redress the loss suffered. The increasing reliance on artificial intelligence therefore presents substantial challenges in the domain of civil liability, particularly as it contributes to the escalation of cybercrime affecting individuals, social structures, and organisational entities [27].

3. Methodology

A descriptive-analytical methodology was adopted to achieve the objectives of this research. The study is exploratory in character, which justified the application of an interpretivist philosophical stance combined with an inductive research approach [28]. In addition, a comparative legal method was employed to examine the foundations of civil liability for damage arising from artificial intelligence within the Moroccan, French, and British legal systems [3]. This methodological combination facilitated a detailed assessment of the current Moroccan legal framework as it relates to civil liability. The descriptive-analytical approach was further utilised to examine and interpret relevant legal texts, statutes, and regulatory instruments addressing civil liability for damages.

The legal sources analysed in this study include the Moroccan Code of Obligations and Contracts (MCOC), French Civil Law No. 131 of 2016, and the United Kingdom's General Data Protection Regulation (GDPR) [29; 30]. Examining these instruments enabled the identification of both structural strengths and regulatory shortcomings within existing AI-related civil liability regimes. Concurrently, the comparative legal approach was applied to contextualise the specific legal challenges encountered by Morocco in addressing civil liability issues. This analysis drew upon prior scholarly literature and relevant legal cases, allowing for the identification of effective practices embedded within Moroccan law that may mitigate such challenges. The scope of the comparative analysis was deliberately confined to the Moroccan, French, and British legal frameworks to ensure analytical depth and coherence. Finally, the collected data were systematically examined using content analysis as the primary analytical technique [31]. This method provided comprehensive insights into the legal treatment of civil liability for damages caused by artificial intelligence within the selected jurisdictions.

4. Results and Discussion

4.1 Civil Liability for Damages Caused by AI

The criteria governing civil liability differ from those applied to the assessment of damage caused by artificial intelligence and may diverge from other established liability regimes, including objective, tortious, and contractual liability. Within this framework, civil liability arises primarily through the existence of a causal relationship between the harmful act and the resulting damage. When applied to AI-related harm, this principle is increasingly linked to mechanisms of automatic compensation, with particular emphasis placed on establishing a clear cause-and-effect connection [32]. Contractual liability, by contrast, emerges from the breach of obligations contained within a valid contract by one of the contracting parties. In the context of AI, this form of liability presents substantial difficulties, especially where autonomous systems or AI-driven agents independently generate decisions without direct human intervention.

Objective liability, on the other hand, focuses on the relationship between damage and error from the perspective of the injured party, without requiring proof of fault [33]. This model is particularly relevant to AI applications, where the autonomous and often uncontrollable nature of intelligent systems elevates the level of risk associated with their operation. As a result, liability for AI-related harm increasingly prioritises the protection of victims rather than fault attribution. In addition to recognising AI-related liability, contemporary legal discourse places strong emphasis on ensuring compensation for both tangible and intangible harm. Within the AI domain, insurance mechanisms are frequently proposed as effective tools for guaranteeing victim compensation. Furthermore, the promotion of human rights has reinforced the importance of physical integrity and personal safety as foundational elements in the development of comprehensive compensation systems [34].

Consequently, domestic legal frameworks are expected to operate in conformity with relevant international agreements, preventing internal legislation from undermining established protective standards. This approach prioritises the interests of the injured party over those of the individual responsible for the harm, reflecting an evolving conception of social responsibility. Within this context, legal systems increasingly impose compensation obligations on debtors even where damage results from unforeseen or accidental events [35]. The overarching objective of such insurance-based and liability mechanisms is to ensure that victims receive compensation in all circumstances, thereby reinforcing fairness and legal certainty in the allocation of AI-related risks.

4.2 Civil Liability for Damages Caused by AI under the Moroccan Law

Artificial intelligence has emerged as a highly influential instrument capable of producing both beneficial and harmful outcomes, thereby exerting a direct impact on users' lives. In contemporary practice, AI systems are increasingly employed to process and analyse individuals' personal data, often without obtaining prior consent. In such circumstances, affected individuals are legally entitled to seek compensation for the harm suffered [36]. This entitlement is grounded in the principle of tort liability as recognised under Moroccan law. Accordingly, Article 77 of the MCOC explicitly provides that:

"Any act committed by a person, intentionally or unintentionally, without being authorized by law, that causes damage to another, the perpetrator shall be obliged to compensate for this damage if it is proven that this act was the direct cause of the damage" [29].

Furthermore, in instances where a technology company collects users' data without consent through AI, resulting in harassment, theft, or other forms of harm, the affected individuals are entitled to claim compensation under the provisions of Article 77 of the MCOC. A significant concern arising from the use of AI involves erroneous data analysis, which can lead to flawed decision-making processes. Consequently, the entity responsible for the AI system is obligated to provide compensation to all impacted parties, in accordance with the stipulations set forth in Article 78 of the MCOC.

"Every person is liable for the moral or material damage he causes, not only by his act, but also by his error, if it is proven that this error is the direct cause of that damage" [29].

Similarly, where a recruitment company employs AI to evaluate candidates' CVs and a qualified applicant is unjustly rejected due to a technical malfunction, the affected candidate may pursue legal action against the company to claim compensation. Additional legislation addressing the protection of personal data and consumer privacy under Moroccan law is summarised in Table 1.

Table 1: Laws for Consumer Protection under Moroccan Law [29]

Laws	Description
"Law No. 09-08 on the Protection of Personal Data"	It protects users' personal information from unauthentic sources. Article 7 of this law states: "Data of a personal nature may only be processed if the person concerned has given their explicit consent."
"The Consumer Protection Law (Law No. 31.08)"	Under this law, the companies are required to provide clear and transparent information to the consumers regarding the usage of their personal information. Article 25 of this law states: "Every supplier or service provider must provide the consumer with the necessary information about the characteristics of the product or service provided to him."
"Civil Protection under Law No. 24.09 on Product and Service Safety"	This law obligates the companies to avoid such technologies that can cause privacy concerns for the users.

4.2.1 Case Analysis

Recently, Morocco has witnessed a significant rise in cases stemming from the unauthorised collection of data and the deployment of AI in surveillance activities. These developments have generated a range of ethical and legal concerns, notably affecting freedom of expression. A prominent example involves the targeting of human rights defenders Maati Monjib and Abdessadak El Bouchattaoui, who were compromised by the Pegasus spyware [37] According to Amnesty International, in 2019 both individuals were subjected to illegal investigations via malicious SMS messages. Additionally, network injections enabled unauthorised access to their private communications and movements, constituting a clear violation of privacy rights and posing a threat to their civic engagement. Similarly, journalist Omar Radi was targeted using Pegasus spyware, resulting in a breach of his personal privacy [29]. Beyond spyware,

Moroccan authorities have also employed the Eagle system and other hacking tools to conduct mass data collection, raising concerns about the emergence of an unchecked surveillance state. These incidents have highlighted broader issues related to the integration of AI within legal and judicial processes. To mitigate risks associated with overreliance on AI, emphasis is placed on preventing algorithmic bias and ensuring the incorporation of human oversight within judicial decision-making.

4.3 Civil Liability for Damages Caused by AI under the French Law

Article 1242 of the French Civil Code (Law No. 131 of 2016) provides that:

"A person and an individual are not only responsible for the damages that arise from his personal actions, but also for any damage that results from the actions of individuals or things under his responsibility or custody" [30].

French law further distinguishes between design protection and usage guardianship, particularly in relation to complex technologies such as AI-dependent robots. Design protection imposes obligations on the manufacturer, based on their rights over information processing and the creation of the technology. However, this has given rise to practical challenges, especially in identifying the precise causes of damage. To address such difficulties, the deployment of assistive robots has been proposed as a mitigating measure. In addition, French law differentiates between legal guardianship and actual custodianship. In the landmark 1941 Frank case, the French judiciary adopted the actual custody theory, which establishes that:

"The caretaker is the person who has the authority that is related to controlling, managing, and guiding the thing. In Egypt, the jurisprudence has unanimously agreed that the actual guardian is responsible for the harm caused by things" [30].

Consequently, it is essential for the custodian to demonstrate that they are exercising their authority to control, guide, and manage the AI system effectively. French law addresses civil liability for AI within the framework of its Civil Code, emphasising the application of principles such as negligence, fault, and responsibility. This approach recognises the autonomous nature of AI and ensures that liability is appropriately assigned to those who have the capacity to oversee and direct its operation.

4.4 Civil Liability for Damages Caused by Artificial Intelligence under British Law

In the United Kingdom, civil liability for artificial intelligence is principally grounded in tort law and contract law. Tort law, which addresses non-contractual civil obligations, has developed over time to regulate harmful human conduct. The integration of AI has introduced novel forms of harm, generating complex legal challenges and necessitating clear delineation of liabilities and rights. In response, the "Artificial Intelligence and Civil Liability Project BCLI" was launched in 2021 with the objective of adapting tort law to provide effective civil remedies for victims and to propose legal reforms addressing AI-related issues [38]. Under the current UK legal framework, claimants bear the burden of establishing causation, damage, or breach, a requirement that is often complicated by the opacity and complexity of AI systems. The Consumer Protection Act 1987, which addresses defective products, is relevant but presents practical challenges when applied to AI technologies [39]. Similarly, the Equality Act 2010 provides a legal basis for addressing discrimination arising from AI operations [40]. Additionally, the UK's GDPR safeguards the privacy and security of online users, a provision that extends to AI applications [41]. The comparative analysis conducted in this study highlights the importance of integrating robust and context-specific legal frameworks to govern AI civil liability. While Moroccan, French, and UK laws acknowledge AI-related civil liability and aim to protect victims' rights, the practical implications and effectiveness of these legal instruments remain under continuous scrutiny.

5. Conclusion

At present, the use of AI technologies has become widespread and integral to daily activities. While AI offers substantial benefits, it has also raised significant concerns regarding privacy and data protection. In response, the concept of AI civil liability has gained prominence in recent years and has been addressed within various legal frameworks, including those of Morocco, France, and the United Kingdom. For example, the MCOC incorporates the principle of tort liability, which seeks to safeguard the rights of individuals adversely affected by AI technologies. The recent increase in online theft and cybercrime cases further underscores the necessity of implementing effective legal mechanisms to enforce civil liability. Similarly, French Civil Law No. 131 of 2016 prioritises the protection and safe utilisation of AI technologies. In contrast, UK law does not contain explicit provisions on AI civil liability but relies on the GDPR to ensure the protection of online users. The comparative analysis conducted in this study highlights the need for the development and implementation of legal provisions that explicitly address AI civil liability within these jurisdictions, ensuring clear accountability and enhanced protection for affected individuals.

6. Recommendations

Based on the findings of the comparative analysis, several recommendations can be proposed for the Moroccan government to enhance the legal framework governing AI civil liability:

- Morocco should develop and incorporate specific legal provisions addressing the use of AI, with a particular focus on civil liability. Such provisions would protect the rights of users and provide a clear legal basis for the regulation and lawful deployment of AI systems.
- Regulations pertaining to AI should also be integrated within both contractual and tort law. This integration would establish clear responsibilities for manufacturers, users, and developers of AI technologies, fostering accountability across all parties. Aligning these provisions with practices observed in French and British law would strengthen their practical applicability.
- Encouraging partnerships between the Moroccan government and international human rights organizations, such as the United Nations, would support the protection of AI users' rights. Collaboration at this level would facilitate the adoption and integration of AI civil liability principles within Moroccan legislation.
- Policymakers are advised to harmonise Moroccan law with relevant international standards and regulations concerning AI. This alignment would enable the legal system to remain responsive to ongoing technological advancements in AI, thereby enhancing the overall effectiveness and robustness of civil liability mechanisms.

7. Research Implications

This study presents implications across multiple levels, particularly concerning artificial intelligence. From a legal perspective, it examines the role of cybercrime and the ways in which AI-based technologies facilitate violations of privacy. The research also incorporates a comparative analysis of different legal systems, highlighting that many countries lack sufficient resources to address the complexities associated with advanced technologies. This underscores the necessity of developing comprehensive civil liability provisions, particularly within the context of Moroccan law. From a policy perspective, the findings indicate that Moroccan legislation requires alignment with international organisations to establish structured laws capable of effectively addressing civil and cybercrimes. The study further emphasises the importance of integrating AI-specific regulations into Moroccan law to ensure both accountability and protection for affected individuals. At the international level, the research offers recommendations aimed at safeguarding fundamental human rights in the digital era, thereby enhancing legal and compliance frameworks and fostering public confidence in AI technologies within Morocco. Academically, the study contributes valuable insights into Morocco's legal code and provides a detailed comparative analysis with French and British frameworks. The literature reviewed underscores the intersection of AI and cybercrime, illustrating significant implications for civil society. Moreover, the research identifies the need for future investigations into legal models that incorporate AI, which could inform the development of systematic frameworks for legislation, judicial practice, and scholarly research.

8. Limitations and Future Studies

This study presents several limitations. Firstly, it focuses primarily on comparative analyses of laws, civil liability, and cybercrimes, limiting its scope to Moroccan, British, and French legal frameworks while not examining the role of courts and their jurisprudence in addressing AI-related issues. Secondly, the research concentrates on civil liability and its various types, without considering other liability theories, which reduces the diversity of legal perspectives. Additionally, although the study addresses AI-based technologies, it does not account for contemporary AI models or their specific characteristics. The research emphasises civil liability and damages caused by AI but does not explore other legal domains, such as the implications of AI in governance, administration, or broader legal practice. Furthermore, the study does not consider machine learning AI models and their effects on the legal system, which limits its analysis of emerging legal challenges.

References

[1] Biedron SR. Cybercrime in the Digital Age: University of Oxford; 2024.Retrieved from: https://ora.ox.ac.uk/objects/uuid:5fe21811-9bf6-4489-b91d-a195366122e3

[2] Čerka P, Grigienė J, & Sirbikytė G. Liability for Damages Caused by Artificial Intelligence. Computer Law & Security Review. 2015;31(3):376-389 https://doi.org/10.1016/j.clsr.2015.03.008

[3] Farajpour R, & Gunkel D. Legal and Comparative Analysis of Civil Liability of Artificial Intelligence in Automated Decision-Making. 2025 https://doi.org/10.61838/kman.aitech.3.1.16

[4] Khan MNI, & Goswami D. Cybercrime and Contractual Liability: A Systematic Review of Legal Precedents and Risk Mitigation Frameworks. Journal of Sustainable Development and Policy. 2025;1(1):1-24 https://doi.org/10.63125/x3cd4413

[5] Romagna M, & Leukfeldt RE. Social Opportunity Structures in Hacktivism: Exploring Online and Offline Social Ties and the Role of Offender Convergence Settings in Hacktivist Networks. Victims & Offenders. 2024:1-23 https://doi.org/10.1080/15564886.2024.2372054

[6] Tarrad AM. Mistakes That Cause Civil Liability for the Use of Intelligent Applications (A Comparative Applied Legal Study). Journal of Law. 2025;6(2):1-9 http://doi.org/10.47310/iajl.2025.v06i02.006

[7] Wall DS. Cybercrime: The Transformation of Crime in the Information Age: John Wiley & Sons; 2024. https://doi.org/10.13140/RG.2.2.28017.45928

[8] Yar M, & Steinmetz KF. Cybercrime and Society2023. http://doi.org/10.4135/9781446212196

[9] Schjolberg S. The History of Cybercrime: BoD – Books on Demand; 2020. https://www.researchgate.net/publication/313662110

[10] Alhyari FMA, & Almahasneh YOM. The Legal Basis for Liability Resulting from Damages from the Use of Artificial Intelligence (Comparative Study). International Journal of Legal & Religious Sciences. 2023 https://journals.mejsp.com/assets/uploads/journals-researches/1711535935_2245001720.pdf

[11] Babanina V, Tkachenko I, Matiushenko O, & Krutevych M. Cybercrime: History of Formation, Current State and Ways of Counteraction. Amazonia Investiga. 2021;10(38):113-122 https://doi.org/10.34069/AI/2021.38.02.10

[12] Volodymyr Z, Valery B, Borys K, Volodymyr S, Oleksiy O, & Yehor PT. Artificial Intelligence and Cybercrime: New Challenges and Prospects for Legal Regulation. Contemporary Issues in Artificial Intelligence. 2025;1 https://doi.org/10.69635/ciai.2025.11

[13] Caneppele S, & Da Silva A. Cybercrime. Research Handbook of Comparative Criminal Justice: Edward Elgar Publishing; 2022. p. 243-260. https://doi.org/10.4337/9781839106385.00024

[14] Kelsen H. General Theory of Law and State: Routledge; 2017. https://doi.org/10.4324/9780203790960

[15] Hogan-Burney A. Cybercrime Disruption through Civil Litigation and Equitable Remedies. 2023.Retrieved from: https://www.lawfaremedia.org

[16] Chandra A, & Snowe MJ. A Taxonomy of Cybercrime: Theory and Design. International Journal of Accounting Information Systems. 2020;38:100467 https://doi.org/10.1016/j.accinf.2020.100467

[17] Ibrahim S, Nnamani D, & Okosun O. Types of Cybercrime and Approaches to Detection. IOSR Journal of Computer Engineering. 2021;23(5):24-26 http://doi.org/10.9790/0661-2305022426

[18] Phillips K, Davidson JC, Farr RR, Burkhardt C, Caneppele S, & Aiken MP. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences. 2022;2(2):379-398 https://doi.org/10.3390/forensicsci2020028

[19] McGuire M, & Holt TJ. The Routledge Handbook of Technology, Crime and Justice. Abingdon: Routledge; 2017. https://www.routledge.com/The-Routledge-Handbook-of-Technology-Crime-and-Justice/McGuire-Holt/p/book/9780367581404

[20] Marelino A. Understanding the Types of Cyber Crime and Its Prevention. Mathematical Statistician and Engineering Applications. 2022;71(1):108-112 https://doi.org/10.17762/msea.v71i1.50

[21] Soyer B, & Tettenborn A. Artificial Intelligence and Civil Liability—Do We Need a New Regime? International Journal of Law and Information Technology. 2022;30(4):385-397 https://doi.org/10.1093/ijlit/eaad001

[22] Ross DL. Civil Liability in Criminal Justice: Routledge; 2023. https://doi.org/10.4324/9781003170792

[23] Abdullah M, Nawaz MM, Saleem B, Zahra M, Ashfaq EB, & Muhammad Z. Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data. Analytics. 2025;4(3):25 https://doi.org/10.3390/analytics4030025

[24] Killcrece G, Kossakowski KP, Ruefle R, & Zajicek M. State of the Practice of Computer Security Incident Response Teams (CSIRTs). Pittsburgh, PA, USA: CMU/SEI; 2003.Retrieved from: https://apps.dtic.mil/sti/pdfs/ADA421664.pdf

[25] Holt TJ. The Human Factor of Cybercrime. London: Routledge; 2019. https://library.oapen.org/bitstream/id/6dbdcb14-86a4-4dd5-98b8-6dcd623c9268/9781138624696_oachapter13.pdf

[26] Council of E. Computer-Related Crime. Manhattan; 1990.Retrieved from: https://www.coe.int/en/web/cybercrime

[27] Bertolini A. Artificial Intelligence and Civil Liability. 2020 https://www.iris.sssup.it/handle/11382/536310

[28] Ikram M, & Kenayathulla HB. Out of Touch: Comparing and Contrasting Positivism and Interpretivism in Social Science. Asian Journal of Research in Education and Social Sciences. 2022;4(2):39-49 http://doi.org/10.55057/ajress.2022.4.2.4

[29] Ezzerouali S, Arifin R, & Banane MC. Can Moroccan Law Ensure Substantive Justice in Protecting Private Life from AI's Impact? Substantive Justice International Journal of Law. 2025;8(1):1-15. http://doi.org/10.56087/substantivejustice.v8i1.333

[30] Yas N, Al Qaruty R, Hadi SA, & AlAdeedi A. Civil Liability and Damage Arising from Artificial Intelligence. Migration Letters. 2023;20(5):430-446 https://www.researchgate.net/publication/375194842

[31] Hamzani AI, Widyastuti TV, Khasanah N, & Rusli MHM. Legal Research Method: Theoretical and Implementative Review. International Journal of Membrane Science and Technology. 2023;10(2):3610-3619 https://doi.org/10.15379/ijmst.v10i2.3191

[32] Borghetti JS. Civil Liability for Artificial Intelligence: What Should Its Basis Be? La Revue des Juristes de Sciences Po. 2019(17):94-102 https://ssrn.com/abstract=3541597

[33] Burylo Y. Civil Liability for Damage Caused by Artificial Intelligence: The Modern European Approach. Entrepreneurship, Economy and Law. 2022;6:5-11 http://doi.org/10.32849/2663-5313/2022.6.01

[34] Benhamou Y, & Ferland J. Artificial Intelligence & Damages: Assessing Liability and Calculating the Damages. Leading Legal Disruption: Artificial Intelligence and a Toolkit for Lawyers and the Law2020. https://ssrn.com/abstract=3535387

[35] Hassan MR. Civil liability for damages from artificial intelligence. Artificial Intelligence Information Security. 2024;2(5):121-200 https://doi.org/10.21608/aiis.2024.331823.1012

[36] Hamouti N, & Elbouzidi A. The Importance of Artificial Intelligence in the Field of Moroccan Criminal Law: What Impact on the Legal Protection of Personal Data? 2024 https://scopmajd.com/wp-content/uploads/2024/08/1-4.docx-1.pdf

[37] Amnesty I. Morocco: Human Rights Defenders Targeted with NSO Group's Spyware. 2019.Retrieved from: https://securitylab.amnesty.org/latest/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/

[38] British Columbia Law I. Artificial Intelligence and Civil Liability. 2024.Retrieved from: https://www.bcli.org/wp-content/uploads/Report-AI-and-civil-liability-final.pdf

[39] Hodges C. The Consumer Protection Act 1987. Product Liability: Informa Law from Routledge; 2020. p. 59-86. https://www.legislation.gov.uk/ukpga/1987/43/contents

[40] Equality Act, The Stationery Office (2010). https://www.legislation.gov.uk/ukpga/2010/15/contents

[41] Halawi L, & Makwana A. The GDPR and UK GDPR and Its Impact on US Academic Institutions. Issues in Information Systems. 2023;24(2) http://doi.org/10.48009/2_iis_2023_120