Assessing Legislative Gaps in Qatari Law Regarding AI-Driven Misinformation: Insights from the UAE Legal Framework

Mashaallah Othman Alzwae[1*], Abdelnaser Aljahani[2], Zinah Ghanim Younus[3]

[1] Faculty of Law, University of Benghazi, Benghazi, 00218, Libya

[2] College of Law, University of Sharjah, Sharjah, 00971, United Arab Emirates

[3] College of Law, University of Ninevah, Mosul, 00964, Iraq

[*] Corresponding author: mashaallah.alzwae@uob.edu.ly

Article	Abstract
	This study aims to examine the weaknesses of Qatari laws and assess their effectiveness in combating this new type of crime by comparing them with the UAE's Anti-Rumours and Cybercrime Law No. 34 of 2021, Article 54", as a strong example of legislation in this area. The study highlights Singapore's law as a Southeast Asian example that explicitly criminalises "the creation or modification of robots as an artificial intelligence system used to spread misinformation," similar to the UAE law, indicating that the UAE law is more effective and comprehensive in combating these crimes. The study adopts a comparative analytical approach, which is the most appropriate approach to addressing emerging legal issues, such as those linked to the utilisation of AI systems to spread misleading content. The findings reveal weak Qatari legislative protection in this area, pointing to the need to reform the Anti-Cybercrime Law No. 14 of 2014. This law explicitly defines bots, rumours, and misinformation, and criminalises the act of "creating or modifying an electronic bot intended to publish, republish, or circulate misleading information in the country, or enable any other person to publish, circulate, or republish such information, or delete an electronic bot after committing a crime with the intent to mislead justice." It also revisits traditional criminal liability rules to align Qatari legislation with relevant international standards and Qatar's Artificial Intelligence Strategy.

INTRODUCTION

Amid growing global concern about the use of AI-powered bots to spread rumours or misinformation, this study seeks to shed light on the legislative vacuum

in Qatari law. There are no explicit provisions criminalising the creation or modification of an electronic bot to spread rumours or misinformation (Kaawoan, 2020). In contrast, the UAE legislature has explicitly intervened through Article 54 of the Anti-Cybercrime and Rumor Law to combat this emerging type of crime. This law is one of the first and most distinctive texts of its kind in the Arab world to clearly address this issue. In our study, we employed an analytical and comparative legal approach to examine the effectiveness of current Qatari laws in combating this crime, drawing on a comparison with UAE law. Based on this, we can propose appropriate legislative reforms consistent with international standards pertaining to the regulation and oversight of cognitive computing technologies. We also propose appropriate legislative reforms based on international standards related to the institutional regulation of   intelligent automation

Taking into account the foregoing, information technology has witnessed significant developments, especially with regard to the method of spreading rumours and misleading information on the Internet (Barlian et al., 2025; Woolley, 2022). It is no longer necessary for rumours or misleading information to be spread directly by the user. Instead, it has become possible to spread them without direct human intervention by the user, using robots supported by artificial intelligence and prepared for publication (Cantika Aulia et al., 2023; Tomassi et al., 2024). The danger of these tools lies in their superior capabilities in increasing the spread of misleading media content and amplifying it significantly beyond the capabilities of the human user, expanding the scope of their reach to different segments of society. In our view, this allows for a significant impact on public opinion in society amidst important and sensitive periods, such as the period of legislative or presidential elections or municipal councils, that do not tolerate the circulation of misleading information (Shao et al., 2018; Vosoughi et al., 2018).

In addition, these tools may also be intended to incite public opinion via the spread of misleading information against the government or one of its affiliated institutions or departments, especially during critical periods such as the spread of infectious diseases or when disasters or accidents occur. The goal is to demonstrate the government's inability to deal with such situations, in favour of opposition parties or other parties outside the state.

Undeniably, in our assessment, it constitutes a threat to public trust and social stability in the state, in addition to threatening cybersecurity (Szmurlo & Akhtar, 2024; Thakur & Breslin, 2021) by undermining public confidence in official digital sources for disseminating information in the country. This negatively impacts the integrity and security of the digital infrastructure, which serves as a vital component of cybersecurity. These emerging technologies pose a significant challenge to criminal justice systems (Quattrocolo, 2018) in, for example, determining criminal liability and identifying criminally responsible individuals (Pagallo, 2017).

Given the rapid growth of intelligent robots and their significant potential to spread falsehoods, states must take some measures, considering a range of international standards to encourage the responsible and secure use of these systems. For example, since Art. 19 of the UNICCPR ensures the right to express opinion, states may impose restrictions to shield the rights and the standing of others or to maintain social order, national security, or collective health. Article 20 of ICCPR further strengthens these restrictions, explicitly prohibiting provocation of unlawful differentiation, antagonism, or violent conduct, which is essential for dealing with robots spreading malicious rumours.

Taken together, these Obligations arising from ICCPR form the basis of international standards that oblige states to incorporate these provisions into the national legal framework regulating robots. In other words, no one disputes that enshrining these standards in domestic laws enables governments to develop ethical systems that combine technological innovation with protection against misinformation, establish strong safeguards for freedom of expression, and identify systemic threats to public trust and democratic discourse.

In this context, the OECD Principles on Artificial Intelligence and Robotics are essential, as they constitute the ethical and regulatory framework for these technologies (Rawat et al., 2024). To more effectively address these emerging technological challenges, it is essential to develop national legislation. In this regard, Article 54 of the UAE Anti-Cybercrime and Rumor Law stands out as the first Arab legislation to explicitly address this emerging type of crime. This article criminalises the design or alteration of a robot or an AI-powered bot aimed at spreading rumours or spurious information. From a comparative legal perspective, it is worth noting that Qatari law does not include a similar provision, despite the increasing reliance on the use of AI systems utilised for disseminating misinformation.

While the debate surrounding the use of intelligent bots to spread disinformation is still in its infancy, it is beginning to take shape in the academic literature. Rather than offering comprehensive legal solutions, existing studies often highlight specific risks and impacts, indirectly pointing to the need for legal intervention. One such study relevant to ours is Xu study (Xu, 2017), which focused on how algorithmic propagators influence political discourse in a country by targeting influential political figures in society.

One significant outcome highlighted by this within the scope of our study is that it pointed to the problem of how to determine legal responsibility for spreading rumours or misleading information through algorithms. We also refer to Rajaram's study (Huang et al., 2024), which addressed the danger of robots' influence on human memory through the transmission of misleading information or various rumours. In the context of confronting the threat of these tools, the study proposes

supporting the design of robots that prevent the dissemination or circulation of misleading information, albeit for non-criminal purposes.

In addition, a study by Jiang indicated that the spread of rumours via robots can be reduced by using deep learning algorithms to verify the credibility of information disseminated by robots (Jiang et al., 2023). This is similar to the research conducted by Sharkey (Sharkey & Sharkey, 2021), investigating the application of robotics systems to commit illegal acts, such as spreading rumours, violating privacy, and defamation.

Although there has been emerging academic discourse addressing the issues stemming from the use of AI-powered bots to spread false information, these studies have focused on the technical, psychological, or social dimensions, excluding the legal aspect, particularly criminal liability related to the intentional use of these tools to spread rumours or misinformation. Consequently, there is a lack of legal studies on determining criminal liability in cases where AI systems are used to disseminate misinformation and influence public opinion without direct human intervention. Our study is the first to address this issue, particularly in the Arab world, and more specifically in the UAE and Qatar.

This study is gaining increasing importance in light of growing international concern about the misuse of AI (Siraj et al., 2025), particularly bots (Partow-Navid & Slusky, 2023), to spread rumours or misinformation and influence public opinion. This poses a real challenge for national legislators to align their legislation with international standards within this scope. In this context, Qatari criminal legislation lacks explicit and specific provisions addressing this use, unlike UAE legislation, which includes explicit provisions regulating this issue and is considered among the most advanced in this field.

Accordingly, the study aims to 1) analyse the adequacy of current traditional texts in Qatari legislation to address the deliberate use of AI-powered robots to spread rumours or misleading information and the need for new legal texts to address this emerging pattern of crimes, 2) study the UAE experience through Article 54 of Law No. 34 of 2021 on Confronting Rumors and Cybercrimes as an advanced model in this field that Qatari legislators can benefit from in legislative reform, 3) propose effective legal reforms to address this type of crime, consistent with international standards regarding AI governance and Qatar's strategic plan for the use of AI.

From this perspective, the problem to investigate is: Does the absence of an explicit legal provision in Qatari legislation criminalising the creation or modification of an electronic robot to spread rumours or misleading information constitute a legislative vacuum that requires legislative amendment? How can the UAE's experience be leveraged to fill this legislative gap, if it exists?

METHODS

The study adopts a comparative analytical approach, which, in our opinion, is the most appropriate approach to addressing emerging legal issues, such as those linked to the utilisation of AI systems to spread misleading content. The comparative approach enables us to identify weaknesses in Qatari legislation compared to the advanced UAE legislation in addressing this issue. In contrast, the analytical approach allows for an in-depth analysis of the texts and an assessment of their adequacy and effectiveness, with reference to the Singaporean approach to combating misinformation spread through AI systems. The study analyses the following legal texts:

1. Article 54 of the Qatari Penal Code No. 11 of 2004, concerning the rules for attributing criminal liability.
2. Article 6 of Qatari Law No. 14 of 2014 on Confronting Cybercrime, concerning combating the propagation of rumours and protecting the state's integrity and stability
3. Articles 1 and 54 of The UAE law on Confronting rumours and Cybercrimes No 34 of 2021, which explicitly criminalise the creation or modification of an electronic bot with the intent to spread misleading information.
4. Articles 1 and 8 of the Law on Protection from False Information and Online Manipulation in Singapore in 2019 and its amendments

These texts were chosen for their direct relevance to the study's topic: how to regulate criminal liability for the spread of rumours or misleading information disseminated via AI-powered bots without direct human intervention. Furthermore, they are valuable compared to the legislation studied, as Qatari law lacks an explicit text regulating this issue. Meanwhile, UAE legislation represents a unique and advanced model in the Arab world, as it includes a clear and explicit text on this matter. The study compares three main legal aspects.

The first relates to the clarity and precision of criminal texts associated with the use of AI systems utilised for disseminating false information. The second refers to the scope of criminal liability in cases where the criminal act is committed without direct human intervention and the effectiveness of traditional texts in achieving effective responses in this regard. The third axis concerns the extent to which these texts are compatible with international standards, such as Articles 19-20 of the ICCPR and the OECD and UNESCO Principles on Artificial Intelligence. Legal information and data were collected from multiple sources, including national legal texts, legal literature relevant to the study, the official website of the Supreme Judicial Council in Qatar, and applicable international standards.

RESULTS AND DISCUSSION

The Conceptual and Technical Framework for Spreading Rumours via AI Systems Utilised for Disseminating Misinformation

1. Defining Software Robots (Bots) and their Role in Producing Fake Content

Article 1 of UAE law 34-2021 regarding countering rumours and cybercrime defines a robot as "An electronic program designed or modified to perform automated tasks efficiently and quickly." This definition reflects the UAE legislator's awareness of the risks posed by technological advancements to rights and freedoms, as well as its commitment to keeping pace with the legal developments necessary to address digital developments. This definition also provides a clear and fundamental interpretative reference for criminal justice and judicial bodies when dealing with emerging cybercrimes. On the other hand, Qatari legislation lacks a similar definition.

This deficiency is not limited to a mere gap in concept or language; it has extremely significant legal implications, as the ambiguity and precise interpretation of technical tools such as robots may weaken the theoretical foundation necessary to understand or classify the actions carried out using these technologies and, consequently, describe them with the correct legal description. There is no doubt that the absence of a precise legal definition of technical concepts leads to ambiguity in judicial application and undermines legal certainty (Ficsor, 2018; Hariyanto et al., 2024).

Software robots, commonly known as "Bots" can be defined as computer programs designed to perform a set of tasks automatically based on pre-programmed instructions sent over the internet (Flores, 2021). These robots are used to carry out various online activities, including, for example, providing digital services to users, collecting data at high speeds, and creating, publishing, or republishing digital content without direct human intervention (Kurian & Varghese, 2021). This publishing on social media networks is usually done with superior capabilities that exceed those of the human user (Chng, 2023). This publishing of fake content undoubtedly contributes to forming a false viewpoint among users about some issues and affects public opinion in society on a broad scale in a way that may be difficult to remedy (Wang et al., 2018).

In addition to the aforementioned risks, bots have the functionality that enables anonymity of the real operator, making it difficult to determine the source of rumours or misinformation (Soares, 2024). What further complicates the matter, in our view, is that these bots can mimic human behaviour in writing or publishing in a professional manner, making it difficult to accurately trace their source, thus allowing the original perpetrator to escape justice. There is no doubt that the increased use of social networks by various segments of society will increase the magnitude of the aforementioned risks (Kumar et al., 2017).

2. The Legal Challenge of Attributing Criminal Acts to Non-Human Actors

It can be said that there is a legal dilemma regarding how to assign criminal responsibility in the case of spreading rumours or misleading information via robots, as it is unattainable, according to the established doctrines of penal responsibility, to assign responsibility to a non-human entity (Consulich, 2023), and it can only be assigned to a human element that can be held accountable for its crime (Eliot, 2021). This is because the human element is the only one that has emotions and will, which are the two essential elements for assigning criminal responsibility according to traditional rules. These elements are not possessed by robots that operate with artificial intelligence and perform their tasks without direct human intervention (Lagioia & Sartor, 2020).

Therefore, the current criminal legal system faces a significant challenge in determining who bears criminal liability when a criminal act is committed using these technologies (Xudaybergenov, 2023). Is it the programmer who designed the robot? Or the user who used the bot to spread rumours? This stems from the legal dilemma that is attributable to the fact that intelligent bots spread rumours without direct human intervention, making it difficult to prove fault and criminal intent in such cases (Barfield, 2018).

In an attempt to resolve this legislative gap, the 2019 OECD Principles on the Applications of Artificial Intelligence call for the need to hold AI actors, such as developers and users, accountable while respecting the rule of law standards. We believe that bridging this legislative gap can only be achieved by developing legal concepts that go beyond traditional criminal liability principles, such as vicarious criminal liability or agency through non-human intermediaries, as emphasised in the 2021 UNESCO Position Paper on AI Utilization.

Accordingly, we believe that these frameworks provide the appropriate basis for addressing this legal dilemma, and taking into account Art. 15 of the IC on CPR linked to the legality of crimes and punishments and its prior stipulation by the legislator, we see the possibility of assigning criminal responsibility to a person according to their participation in the crime and their ability to anticipate its consequences. This matter requires establishing a clear legal basis that defines this responsibility (Dvornikova & Osadchaya, 2024).

To expand the scope of criminal liability in this case and enhance the chances of attributing it to a specific person, it is not necessary to attribute it to the perpetrator based on the presence of bad faith, but rather it could be based on the presence of gross negligence or recklessness in using this software without taking the necessary precautions to avoid the harmful outcome, including the failure to implement control mechanisms that would prevent the misuse of robots (Saxena et al., 2024).

European AI law has emphasised the concept of risk-based liability, whereby responsibility rests with effective oversight of systems. This was emphasised in the attribution rules of the 2017 Tallinn Manual. In addition, states are responsible for effectively monitoring technologies and tools with foreseeable risks. This, in our view, is implicit in the due diligence obligation contained in the Corfu Channel case (Piernas, 2024). We believe that legislators should take these international standards into account when drafting national laws regulating the use of AI systems.

Therefore, the increasing reliance on AI systems in information mediation and their impact necessitates the adoption of new rules for criminal attribution (Sourdin, 2015) that allow for the identification and punishment of those responsible for the crime, avoid excessive expansion of traditional legal texts, and respect the principle of criminal legality. Achieving this important balance undoubtedly requires reforming existing laws to ensure the safe use of modern technologies and achieving harmony between technological developments and the needs of criminal justice.

This requires that technological developments serve humanity, not be a blight upon it. Conversely, some legislation has acknowledged these gaps and addressed them with explicit provisions, such as Article 54 of the UAE Anti-Rumors and Cybercrime Law of 2021, which explicitly criminalises the act of designing or modifying AI-powered robots for the purpose of spreading false information. However, Qatari law does not contain a similar legal provision. Accordingly, we believe that Qatari legislators must address this legislative gap to enhance the efforts of criminal justice agencies in combating the spread of rumours using artificial intelligence systems.

UAE Legislation: Criminalising the Act of Spreading Rumours Using AI Systems Utilised for Disseminating Misinformation (Analysis of Article 54 of the Anti-Rumors and Cybercrime Law (2021))

In the context of the UAE legislator's awareness of the danger of spreading rumours or misleading information through artificial intelligence systems, Article 54 of the Anti-Rumors and Cybercrime Law No. 34 of 2021 addressed this problem by explicitly stipulating the criminalisation of the act of creating or modifying robots whenever this was done with the intention of publishing, republishing, or circulating false information or news in the country or helping others to publish, republish, or circulate it.

We believe that, through this ruling, the UAE legislator has largely succeeded in addressing the problem of using robots to spread rumours or misleading information without direct human intervention. As previously stated, traditional rules of penal responsibility are insufficient to engage with issues arising from AI utilisation to spread misleading information (Rachum-Twaig, 2020).

It is worth noting that the aforementioned provision in Article 54 was first included in UAE legislation under Law No. 34 of 2021 and was not included in the

Anti-Cyber Technology Crimes Law No. 5 of 2012 and its amendments or Law No. 2 of 2018. This demonstrates the UAE legislator's desire to keep pace with developments and protect society, whether the perpetrator of the crime is a natural person or a juridical person.

It is worth noting that criminal liability in this article extends not only to the person who created the robot, but also to those who programmed or modified it. The 2021 UNESCO/OECD Principles on AI Moral Dimensions call for shared responsibility and emphasise that algorithms have to work with transparency, clarity, and in accordance with human values.

Within this scope, we believe it is vital to emphasise the importance of UAE legislation aligning with international standards for enhancing Openness and Answerability in the application of Computational tools that leverage AI capabilities to combat misinformation. This requires respect for fundamental communicative liberty and the right to access public data as fundamental rights while protecting public security in the country, provided that a balance is struck between fundamental rights and combating crime.

This is in line with the UN Committee on Civil and Political Rights. According to General Comment number 34 issued by the UN body overseeing the ICCPR, particularly in relation to art. 19, states are urged to adopt laws to address misinformation that threatens the rights and reputations of others, as well as community order "HRC General Comment No. 34, para. 21." Article 54 of the Anti-Rumors and Cybercrime Law reflects these standards, as not only the creators but also the programmers and modifiers of intelligent robots are held responsible, thus reinforcing the principle of accountability in the evolution and deployment of implementation intelligence.

This article is arguably of paramount importance, as it represents a decisive and significant step by the UAE legislature within the legal framework governing artificial intelligence and could be used in Arab countries, notably Qatar. This trend reflects an advanced legal response by the UAE legislator to the difficulties linked with employing contemporary technologies, threatening the country's social and political security (Siabro, 2021). This matter is in line with the UAE's national strategy for artificial intelligence.

In particular, unlike the Qatari legislator, the UAE legislator has been keen to establish a clear and specific definition of false information. Thus, the UAE legislator demonstrates an advanced awareness of the nature of information published online, which may harm public security in the country or mislead public opinion. Article 1 of the Anti-Rumors and Cybercrime Law defines false information as "Information that is wholly or partially untrue, either in itself or in the context in which it appears." This definition is characterised by its comprehensiveness and flexibility, as it is not limited to information that is inherently false, but extends to information that may be

partially true but misleading because it is presented in an incorrect manner, which may change its meaning or cause confusion or chaos in the country.

This definition, therefore, accommodates modern misinformation techniques used by intelligent robots, where the information published appears to be accurate and neutral (Hamsin et al., 2023), but in reality, it can have dire consequences for the security and stability of society. Based on the above, we believe that Qatari law, as currently formulated, is unable to address complex digital phenomena owing to the absence of a precise definition of rumours or false content.

However, despite the importance of Article 54 in establishing an explicit legal basis for the liability of programmers and developers of AI Systems utilised for disseminating misinformation, we believe that the legislature has omitted to include the act of deletion alongside the act of creation or modification. This lack of a provision for deletion constitutes a loophole in the legal text, allowing the perpetrator of this newly emerging crime to have the opportunity to mislead justice, prevent his traces from being traced, or uncover the crime by deleting evidence, thereby escaping punishment.

In our view, this requires the legislature to expand the scope of criminalisation to include the act of deleting a robot after it has been used to spread rumours, especially given the nature of this digital crime and the difficulties of proving it. Furthermore, the practical application of this article may raise numerous legal challenges, most notably how to prove the criminal intent of the programmer or developer of AI systems utilised for disseminating misinformation.

We believe this requires precise digital tools and an in-depth analysis of system behaviour. The lack of judicial applications of this article at the time of this study may be due to the novelty of the text on the one hand and the difficulty of technical proof on the other. This highlights the need to develop digital proof tools, including techniques for tracing the source of programming commands and analysing server logs. This, in turn, requires close cooperation between law enforcement agencies and artificial intelligence experts to ensure accurate interpretation of behaviour.

Importance of Explicit Criminalisation

Undoubtedly, the explicit criminalisation of creating or modifying an electronic bot with the intent to spread online rumours represents an important legislative development, as it contributes to determining criminal liability for spreading rumours via bots, thus bridging the legislative gap related to traditional liability rules. It can be argued that the explicit criminalisation of creating or modifying an automated bot intended to spread rumours may help limit the widespread use of bots to spread online rumours, a challenge that traditional legal rules are unable to address.

The issue of attributing criminal liability to non-human agents within the scope of artificial intelligence remains a profound and highly controversial legal and philosophical challenge (Mikhaleva & Shubina, 2020). Therefore, we believe that

explicit criminalisation, as outlined above, enhances the effectiveness of criminal justice mechanisms in curbing the uncontrolled spread of rumours or misinformation on social media, which may threaten societal stability or incite violence or hatred in society (JHA, 2023). Explicit criminalisation also reflects the UAE's commitment to protecting society from the challenges arising from the use of AI systems utilised for disseminating misinformation to spread rumours. As previously mentioned, explicit criminalisation may also prevent a broader interpretation of traditional criminal law to encompass new digital challenges.

This, in turn, will prevent any potential inconsistencies in judicial rulings on the same case and preserve an essential principle of criminal law: the legality of crimes and punishments. Furthermore, the new approach taken by the UAE legislator in the aforementioned Article 54 affirms the UAE's commitment to legally regulating the use of AI-equipped autonomous robots and ensuring that its domestic legislation complies with international standards in this regard, such as the guidelines developed by the Economic Cooperation and Development Organization, which strive to foster transparency, justice, and answerability in the use of AI (Andrea Widener, 2019). Similarly, efforts are underway within the European Council regarding a treaty regulating the use of Algorithmic intelligence in areas that impact individual rights and public security (van Kolfschooten & Shachar, 2023). These trends mirror the growing international consciousness of the issues accompanying the usage of artificial intelligence and the necessity for legal frameworks to prevent its misuse. In this context, we argue that the creative solution adopted by the UAE legislator in Article 54 merits commendation and adoption.

Insights from Southeast Asia: Singapore's approach to combating misinformation with AI systems

In light of promoting the debate on criminalising the utilisation of intelligent algorithms in the context of false information dissemination, it is worth noting the legislative experience of Singapore in protecting against electronic deceptive narratives and influence efforts, as stipulated in the Act 2019 and its 2021 Amendments. This law protects information and the integrity of societal dialogue in Singaporean society (Chng, 2023) from false information spread by AI systems on social platforms (Uyheng et al., 2021). Article 1 of the Act defines an electronic bot as "a computer program created or modified to perform automated tasks."

Section 8 of the Act criminalises "Creating or modifying an electronic bot with the intent to publish or enable the publication of a factually false statement in Singapore." It should be noted that, concerning the scope of the penal act, Singapore law shares the same provisions as the UAE law in criminalising the creation or modification of an electronic bot with the intent to publish or enable others to publish misleading content.

We believe that while Singaporean law accurately defines misinformation as false or incorrect statements, it is more narrowly defined than the term used in UAE law to define "False information." This term, as defined by the UAE legislator in Article 1 of the Anti-Rumors and Cybercrime Law, includes "rumours and statements that are false or misleading, in whole or in part, whether in and of themselves or in their context." We believe that the UAE legislator's formulation in this regard achieves a more effective response to the spread of misinformation, as the purpose of the text, which is to protect the security of society, order, and the safety of the state, may also be achieved through misinformation, in whole or in part, depending on its nature and the context in which it appears.

Even if the information is true in and of itself, its use outside its temporal or spatial context, or its combination with misleading analyses, renders it false and misleading in its function. This poses a significant risk, especially given the ability of AI-powered bots to amplify, spread, and reshare news at tremendous speed.

The UAE law differs from Singapore's in that Singapore's law is limited to the act of "creating or modifying an electronic bot with the intent to publish or enable the publication of information that is false in terms of fact," while the UAE legislator adds the act of republishing or circulating. We believe the UAE's formulation will again provide a more effective response to the use of AI systems to spread misinformation.

Lack of criminalisation in Qatari law

1. The Qatari Penal Code's effectiveness in dealing with AI-driven misinformation

Qatari Penal Code No. 11 of 2004, recently amended by Law No. 14 of 2024, does not include any new provisions applicable to information technology-related crimes. We believe this is because, despite its recent publication, the legislator did not intend, at the time of its issuance, to address issues related to the use of modern technologies, particularly those related to artificial intelligence, such as the dissemination of misinformation by intelligent automated systems.

Therefore, the provisions contained in this law are drawn from established notions of criminal culpability, which require awareness and will on the part of the criminally responsible person, according to Article 54 of the Qatari Penal Code.

Of course, these conditions are not met by robots that operate independently of humans, rely on pre-programmed instructions, and lack awareness or criminal intent. Therefore, no human actor can be held criminally liable for spreading false information or rumours via intelligent robots, whether the person who designed the robot or the person who developed or modified it, according to the traditional rules of Qatari law. Furthermore, current rules do not explicitly criminalise the act of creating, modifying, or programming robots with the intent to spread rumours. Therefore, the absence of explicit criminalisation, as previously mentioned, poses a

legal challenge in determining criminal liability. Attempts to expand existing legal provisions to include such acts risk violating the rule of lawfulness in criminal justice, which prohibits the application of penal law by analogy or broad interpretation (Moreno, 2017).

Furthermore, determining the criminal liability of robot designers or developers under the rules of criminal conspiracy, stipulated in Article 39 of the Penal Code, is problematic. This provision presupposes the existence of an act of incitement or collusion between two natural persons. In the context of intelligent robots, deployment may occur autonomously, without direct command or immediate human intervention, thus severing the causal link required under traditional principles of incitement (Jaconelli, 2018).

The fundamental legal difficulty lies in the ambiguity of determining liability, whether it is the developer who programs the robot or the end user who activates it. Even if the programmer is considered a moral agent by using the robot as a tool, this analogy again conflicts with the criminal law requirement to establish a precise legal definition of prohibited behaviour. Therefore, holding these individuals accountable requires legislative innovation, not interpretation (Tkacz, 2020).

Furthermore, Article 136 of the Qatari Penal Code, recently added by Law No. 2 of 2020, penalises "transmitting, issuing, or reissuing deceptive or defamatory claims, misleading assertions, or inciting narratives intended to undermine state interests or provoke societal unrest." Although it is a new provision that should keep pace with emerging legal challenges, it does not cover cases where rumours or misleading news are spread via artificial intelligence-powered robots operating without direct human intervention. This provision requires that the perpetrator be a natural person, as it does not explicitly address the possibility of the perpetrator being a non-human element.

Moreover, the text stipulates that the intent is to cause harm, undermine sovereign interests, or stir up public opinion. These are, in our view, elements that are difficult to prove when the perpetrator is unknown or non-human. Furthermore, this article is included in the Penal Code, and the rules for attributing criminal liability stipulated in this law assume that the perpetrator is an individual or a legal entity in certain cases not covered by the aforementioned Article 136. These rules also do not address the case of the perpetrator being a non-human element. Therefore, this article is also unable to address this issue, and to say otherwise would be to leave this text with an intolerable burden and is a clear violation of the rule that states that there is no crime and no punishment except by law.

It can be argued that the Qatari legislator should have shown flexibility and expanded the scope of this law to address new challenges, mainly since this law constitutes the general provisions of Qatari criminal legislation and, therefore, should be referred to when specific criminal laws are found to be deficient. Without such

reform, the legal system will remain insufficient to deter or punish the misuse of emerging technologies (Simmler & Markwalder, 2019). We believe that the absence of an explicit criminal provision in Qatari law contradicts the 2019 OECD AI Principles on Strict Accountability in AI, as well as UNESCO's recommendations on the need to enact national laws to combat AI misuse. This exposes Qatar to the risks of AI misuse, which contradicts its strategic vision for AI governance.

2. Legislative Gaps in Qatari Special Laws: The Cybercrime Law and Other Related Legislation

In addition to the shortcomings of the Penal Code, other apparent shortcomings in Qatar's specific laws are evident, most notably the Anti-Cybercrime Law. Article 6 of Qatar's Anti-Cybercrime Law No. 14 of 2014 criminalises the dissemination of rumours that may harm public safety, public order, or the internal or external security of the state. While this provision shares a similar preventative purpose with Article 54 of the UAE Anti-Rumors and Cybercrime Law of 2021, it is much narrower in scope and does not explicitly address modern technological means, such as AI systems utilised for disseminating misinformation.

To illustrate this, Article 1 of Law No. 14 of 2014 defines a "Website" as "a place with a specific protocol address where various data and information can be provided or processed on the Internet." Although this article has not yet been applied judicially, we believe this definition will pose significant challenges when interpreting its application to AI systems utilised for disseminating misinformation. Unlike traditional websites, which are typically operated by humans, AI systems utilised for disseminating misinformation often operate autonomously, according to pre-programmed algorithms without direct human control or immediate supervision (Ferrara, 2017). This technical independence complicates interpretive efforts to include robots within the Qatari legislator's definition of a "website."

The current definition assumes direct human intervention in the production or processing of online data, which does not apply to autonomous AI systems utilised for disseminating misinformation, as they analyse and process data and make decisions autonomously (Al-Fatih et al., 2025) and lack a specific address or central access point. Furthermore, in an attempt to bridge this legislative gap, Article 6 could be interpreted teleologically and expanded to address emerging robot threats. AI systems utilised for disseminating misinformation could be included if the robot continues to spread misinformation or rumours online and can be tracked via a specific IP address.

However, even with this teleological interpretation of Article (6), we believe the legal definition remains narrow and insufficient to bridge the legislative gap resulting from the absence of explicit provisions addressing the use of AI systems utilised for disseminating misinformation in Law No. 14 of 2014. This definition only

addresses cases where the AI systems utilised for disseminating misinformation have a specific IP address, such as traditional websites.

Accordingly, the use of such systems to spread rumours does not meet the legal standards required by Article (6) unless it is proven that the information or rumours were continuously processed via a specific IP address with a human operator. Therefore, we believe that despite this expansive interpretation of Article (6), it cannot encompass the technical characteristics of such systems that distinguish them from traditional websites.

We believe that this expansive interpretation of Article 6 contradicts the criminal rule asserting that crimes must be previously defined by the legislator and that new acts not previously criminalised by the legislator may not be criminalised. It also poses another practical problem, namely that differing judicial interpretations of the said article will lead to differing judicial rulings in their application. Based on the above, we believe that Article 6 is insufficient to combat the spread of rumours or misinformation using artificial intelligence systems. This necessitates the Qatari legislator's intervention with an explicit text to address this legislative gap and safeguard Qatari society, particularly given the growing use of social media platforms in Qatar. In our opinion, this means greater opportunities for the spread of rumours or misinformation using artificial intelligence systems compared to traditional means.

It is noteworthy that this legislative vacuum exists in other laws in Qatar, namely Law No. 8 of 1979 regarding publications and publishing, Law No. 34 of 2006 on the Regulation of Communications, and Law No. 27 of 2019 on Combating Terrorism. None of these laws contains specific provisions to combat the dissemination of rumours or misleading information by AI-powered robots without direct human intervention. They do not contain any provisions imposing criminal liability on the creation or modification of AI-powered robots to spread rumours or misleading information. Instead, they assume that the perpetrator of the crime is a human element or a legal entity in certain circumstances.

3. The Need to Update Qatari Legislation

An analysis of Qatari law, both the 2004 Penal Code and the Anti-Cybercrime Law No. 14 of 2014, reveals a significant legislative gap in combating unlawful acts involving AI systems, including the crime under study: spreading rumours using AI systems utilised for disseminating misinformation. We find that current provisions in previous laws lack precision and clarity in defining the criminal liability of individuals who create, modify, or program robots with the intent to commit the crime of spreading rumours. This omission is in stark contrast to what the OECD Principles on AI call for: clear legal accountability aimed at the crafting and integration of machine intelligence platforms to mitigate harm and build public trust. Similarly, Advisory on AI Ethical Standards of the Universal Organization for Education, Science, and Culture (2021) emphasises the urgent need for national legislative action

against the misuse of AI, particularly in ways that threaten public order, incite hatred, or undermine democratic processes.

Moreover, this shortcoming in Qatari law undoubtedly contradicts the objectives of Qatar's AI policy, announced through the Qatar National Artificial Intelligence Strategy of 2019. These objectives include developing a legislative approach that ensures the ethically sound, safe, and accountable rollout of AI solutions and supporting a safe and reliable digital ecosystem (Qatar Computing Research Institute, 2019). This casts doubt on the practical achievement of the strategy's stated objectives. As long as the law remains rooted in frameworks that assume human action and control, it will be ill-equipped to address emerging crimes (Abdelaziz, 2025) committed by advanced robots operating independently of humans in real time.

This creates a normative vacuum that may encourage criminals to exploit this legislative deficiency and commit their crimes without criminal liability or punishment. It is also important to note that while the Qatari judiciary has demonstrated commendable efficiency in adjudicating cybercrime cases, as evidenced by a 100% resolution rate for 194 cases in 2024 (Supreme Judiciary Council, 2024), the absence of explicit legal provisions for AI-related crimes may ultimately limit the judiciary's ability to handle more advanced and technologically complex cases in the future.

Therefore, it has become imperative for Qatari lawmakers to undertake comprehensive legislative reform to explicitly define criminal acts involving artificial intelligence and autonomous systems, expand the scope of criminal liability to include individuals who create, deploy, or manipulate these systems for the purpose of committing cybercrimes, and align national legislation with international best practices to ensure Qatar's capacity to withstand evolving online risks.

Qatari legal texts demonstrate that, as Qatari legislation currently stands, they do not comply with international standards pertaining to the regulation of smart algorithm driven and the regulation of its use in disseminating information, such as the principles contained in the UN Guidelines on Responsible machine-based cognition and human rights standards that emphasise respect for freedom of expression and that combating misleading news should not be at the expense of freedom of expression. It is, therefore, necessary to quickly implement legislative reform that is consistent with international standards to ensure legal effectiveness in combating the dissemination of misleading information and respect for basic human rights.

Without these reforms, we believe that Qatar's legal system is weak and unable to respond to emerging technical risks resulting from the growing use of new technologies in various fields, thus failing to effectively confront the new generation of cybercrimes related to machine-based cognition.

CONCLUSION

This study has revealed a significant legislative gap in Qatari criminal law concerning the use of AI-powered robots to disseminate rumours and misinformation. Existing legal provisions are primarily rooted in traditional notions of criminal liability that presuppose human or legal personhood, rendering them ineffective in addressing actions committed by autonomous digital agents. While laws such as the Cybercrime Law No. 14 of 2014 criminalise the spread of false information through websites, they lack explicit references to intelligent robotic systems and do not define critical terms such as rumours or AI-powered robots. This definitional ambiguity and legislative silence limit the applicability and enforcement capacity of current laws in responding to AI-driven misinformation. Furthermore, the absence of judicial precedent or legislative initiatives in this area highlights the urgency for comprehensive legal reform. Comparative insights from jurisdictions such as the UAE demonstrate more advanced and adaptive approaches, particularly through provisions that criminalise the creation and use of robotic systems to spread false content. However, even these progressive models face challenges, including the difficulty of proving intent and ensuring a balance between enforcement and fundamental rights like freedom of expression. To address these issues, the study recommends legislative amendments that incorporate precise terminology, expand criminal liability to cover AI-related acts, and establish specialised bodies combining legal and technical expertise. These measures should align with Qatar's broader digital transformation objectives and international best practices, ensuring that the legal system remains responsive to the complexities of emerging technologies.

REFERENCES

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), 10722. https://doi.org/10.24294/jipd10722

Al-Fatih, S., Roziqin, A., Asyari, M. D., & Ezzerouali, S. (2025). Legal Reform in Village Law-Making Process Using Artificial Intelligence: Is It Necessary? *Journal of Law and Legal Reform*, *6*(2), 757–782. https://doi.org/10.15294/jllr.v6i2.21116

Andrea Widener. (2019). New AI policy guidelines adopted. *C&EN Global Enterprise*, *97*(21), 13–13. https://doi.org/10.1021/cen-09721-polcon6

Barfield, W. (2018). Liability for Autonomous and Artificially Intelligent Robots. *Paladyn, Journal of Behavioral Robotics*, *9*(1), 193–203. https://doi.org/10.1515/pjbr-2018-0018

Barlian, A. E. A., Latipulhayat, A., Rusmiati, E., Wulandari, W., & Sukma, A. N. A. (2025). Electronic Criminal Justice in Indonesia: Challenges and the Future Measures. *Jambura Law Review*, *7*(1), 243–274. https://doi.org/10.33756/jlr.v7i1.27805

Cantika Aulia, Egi Nugraha, & Raja Benhard Parlindungan. (2023). Copyright

Responsibilities of Artificial Intelligence in the Digital Age. *Indonesia Law Reform Journal*, *3*(2), 145–154. https://doi.org/10.22219/ilrej.v3i2.26042

Chng, K. (2023). Falsehoods, Foreign Interference, and Compelled Speech in Singapore. *Asian Journal of Comparative Law*, *18*(2), 235–252. https://doi.org/10.1017/asjcl.2023.9

Consulich, F. (2023). Criminal Law And Artificial Intelligence: Perspective From Italian And European Experience. *European Criminal Law Review*, *13*(3), 270–307. https://doi.org/10.5771/2193-5505-2023-3-270

Dvornikova, P. A., & Osadchaya, A. S. (2024). Artificial Intelligence And The Law: The Challenges Of Establishing Criminal Liability In The Digital Age. *Juridical Scientific and Electronic Journal*, *8*, 330–333. https://doi.org/10.32782/2524-0374/2024-8/77

Eliot, L. (2021). The Legal Quandary When AI Is The Criminal. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3963422

Ferrara, E. (2017). Disinformation and social bot operations in the run up to the 2017 French presidential election. *First Monday*. https://doi.org/10.5210/fm.v22i8.8005

Ficsor, K. (2018). Certainty and uncertainty in criminal law and the 'clarity of norms' doctrine. *Hungarian Journal of Legal Studies*, *59*(3), 271–289. https://doi.org/10.1556/2052.2018.59.3.3

Flores, L. (2021). Artistic and Literary Bots. In *Electronic Literature as Digital Humanities* (pp. 131–143). Bloomsbury Publishing Inc. https://doi.org/10.5040/9781501363474.ch-011

Hamsin, M. K., Anggriawan, R., & Jiatrahman, F. (2023). Unveiling Ethical Implications: AI Robot Accountability in Islamic Context. *Jurnal Media Hukum*, *30*(2), 117–135. https://doi.org/10.18196/jmh.v30i2.18524

Hariyanto, H., Idamatussilmi, I., & Rismana, D. (2024). The government's role in legal protection of land ownership: Urutsewu case. *Legality : Jurnal Ilmiah Hukum*, *32*(2), 277–291. https://doi.org/10.22219/ljih.v32i2.34254

Huang, T.-R., Cheng, Y.-L., & Rajaram, S. (2024). Unavoidable social contagion of false memory from robots to humans. *American Psychologist*, *79*(2), 285–298. https://doi.org/10.1037/amp0001230

Jaconelli, J. (2018). Incitement: A Study in Language Crime. *Criminal Law and Philosophy*, *12*(2), 245–265. https://doi.org/10.1007/s11572-017-9427-8

Jalahussein, A., Mohammad, A., Fadelmansour, A., & Jalal, B. K. (2024). Legal Liability Arising from Artificial Intelligence Activities. *Journal of Ecohumanism*, *3*(6), 338–346. https://doi.org/10.62754/joe.v3i6.4006

JHA, R. K. (2023). Challenges of Fake News and Its Impact on Society in the Digital Era : A Critical Analysis. *International Journal For Multidisciplinary Research*, *5*(2). https://doi.org/10.36948/ijfmr.2023.v05i02.2401

Jiang, J., Chen, X., Huang, Z., Li, X., & Du, Y. (2023). Deep reinforcement learning-based approach for rumor influence minimization in social networks. *Applied Intelligence*, *53*(17), 20293–20310. https://doi.org/10.1007/s10489-023-04555-y

Kaawoan, G. K. (2020). Implementasi Mediasi Penal dalam Penyelesaian Body Shaming secara Siber, Mungkinkah?/The Implementation of Penal Mediation in Resolving Cyber Body Shaming, Is It Possible? *De Jure: Jurnal Hukum Dan*

Syar'iah, *12*(2), 140–155. https://doi.org/10.18860/j-fsh.v12i2.10868

Kumar, S., Villa, R. A., & Carley, K. M. (2017). Identifying Bots that Spread Fake News. *SBP-BRiMS. Washington, DC.*

Kurian, E., & Varghese, S. (2021). Relevance of Bots in Software and Their Impacts on Software Security. *Lecture Notes In Engineering And Computer Science*, *2242*, 207–212.

Lagioia, F., & Sartor, G. (2020). AI Systems Under Criminal Law: a Legal Analysis and a Regulatory Perspective. *Philosophy & Technology*, *33*(3), 433–465. https://doi.org/10.1007/s13347-019-00362-x

Mikhaleva, E. S., & Shubina, E. A. (2020). Challenges and Prospects of the Legal Regulation of Robotics. *Actual Problems of Russian Law*, *1*(12), 26–35. https://doi.org/10.17803/1994-1471.2019.109.12.026-035

Moreno, M. C. (2017). Imprescriptible crimes and the non-retroactivity of criminal norms. *Crítica Penal y Poder*, *12*, 140–167.

Pagallo, U. (2017). AI and bad robots: the criminology of automation. In *The Routledge handbook of technology, crime and justice* (pp. 642–652). Routledge.

Partow-Navid, P., & Slusky, L. (2023). The Need for International AI Activities Monitoring. *Journal of International Technology and Information Management*, *31*(3), 114–127. https://doi.org/10.58729/1941-6679.1564

Piernas, J. (2024). The international law principle of due diligence and its application to the cyber context. *Anales de Derecho*, *41*(1), 66–95. https://doi.org/10.6018/analesderecho.594441

Qatar Computing Research Institute. (2019). *National artificial intelligence strategy for Qatar. Qatar Center for Artificial Intelligence.*

Quattrocolo, S. (2018). The impact of AI on criminal law a, and its twofold procedures. In *ResearchHandbook on the Law of Artificial Intelligence* (pp. 385–409). Edgar Elgar.

Rachum-Twaig, O. (2020). Whose robot is it anyway?: Liability for artificial-intelligence-based robots. *U. Ill. L. Rev.*, 1141.

Rawat, D., Rawat, D., Rawat, A., Pandey, A., Chauhan, G., & Aluvala, S. (2024). Ethics in the era of Intelligent Machines: Legal Perspective and Regulatory Implications. *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, 1–7. https://doi.org/10.1109/KHI-HTC60760.2024.10481959

Saxena, A., Bhatt, R., Bansal, S., Arora, M., Mahato, N., & Gupta, T. (2024). Liability and Responsibility for AI Systems in Computer Engineering and Law. *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1–6. https://doi.org/10.1109/ICCCNT61001.2024.10725153

Shao, C., Ciampaglia, G. L., Varol, O., Yang, K.-C., Flammini, A., & Menczer, F. (2018). The spread of low-credibility content by social bots. *Nature Communications*, *9*(1), 4787. https://doi.org/10.1038/s41467-018-06930-7

Sharkey, A., & Sharkey, N. (2021). We need to talk about deception in social robotics! *Ethics and Information Technology*, *23*(3), 309–316. https://doi.org/10.1007/s10676-020-09573-9

Siabro, A. (2021). The Influence Of Scientific And Technological Development On The Transformation Of The Global Security Paradigm. *European Political and Law Discourse*, *8*(5), 6–13. https://doi.org/10.46340/eppd.2021.8.5.1

Simmler, M., & Markwalder, N. (2019). Guilty Robots? – Rethinking the Nature of Culpability and Legal Personhood in an Age of Artificial Intelligence. *Criminal Law Forum*, *30*(1), 1–31. https://doi.org/10.1007/s10609-018-9360-0

Siraj, A., Jabbi, Y., Budhiartie, A., & Mustaffa, A. (2025). Redefining Accountability: AI's Role in Prosecuting Transnational Crimes under International Law. *Audito Comparative Law Journal (ACLJ)*, *6*(2), 124–145. https://doi.org/10.22219/aclj.v6i2.40434

Soares, H. (2024). *The Spread of Fake News by Social Bots: Perspectives on Social Bot Regulation* (pp. 189–204). https://doi.org/10.1007/978-3-031-47946-5_11

Sourdin, T. (2015). Justice and technological innovation. *Journal of Judicial Administration*, *25*, 2.

Supreme Judiciary Council. (2024). *Annual statistical report 2024*. Supreme Judiciary Council.

Szmurlo, H., & Akhtar, Z. (2024). Digital Sentinels and Antagonists: The Dual Nature of Chatbots in Cybersecurity. *Information*, *15*(8), 443. https://doi.org/10.3390/info15080443

Thakur, S., & Breslin, J. G. (2021). Rumour prevention in social networks with layer 2 blockchains. *Social Network Analysis and Mining*, *11*(1), 104. https://doi.org/10.1007/s13278-021-00819-y

Tkacz, S. (2020). Zasada nullum crimen sine lege jako źródło poszukiwania językowej granicy wykładni prawa karnego? *Archiwum Filozofii Prawa i Filozofii Społecznej*, 81–95. https://doi.org/10.36280/AFPiFS.2020.2.81

Tomassi, A., Falegnami, A., & Romano, E. (2024). Mapping automatic social media information disorder. The role of bots and AI in spreading misleading information in society. *PLOS ONE*, *19*(5), e0303183. https://doi.org/10.1371/journal.pone.0303183

Uyheng, J., Ng, L. H. X., & Carley, K. M. (2021). Active, aggressive, but to little avail: characterizing bot activity during the 2020 Singaporean elections. *Computational and Mathematical Organization Theory*, *27*(3), 324–342. https://doi.org/10.1007/s10588-021-09332-1

van Kolfschooten, H., & Shachar, C. (2023). The Council of Europe's AI Convention (2023–2024): Promises and pitfalls for health protection. *Health Policy*, *138*, 104935. https://doi.org/10.1016/j.healthpol.2023.104935

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, *359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

Vuletić, I. (2021). *Criminal Law and the Challenges of Autonomous Intelligence: Substituting a Theory of Guilt with the Division of Labor* (pp. 111–126). https://doi.org/10.1108/S0193-589520210000029007

Wang, P., Angarita, R., & Renna, I. (2018). Is this the Era of Misinformation yet. *Companion of the The Web Conference 2018 on The Web Conference 2018 - WWW '18*, 1557–1561. https://doi.org/10.1145/3184558.3191610

Woolley, S. C. (2022). Digital Propaganda: The Power of Influencers. *Journal of Democracy*, *33*(3), 115–129. https://doi.org/10.1353/jod.2022.0027

Xu, J. (2017). *Representing big data as networks: new methods and insights*. University of Notre Dame.

Xudaybergenov, A. (2023). Toward Legal Recognition of Artificial Intelligence

Proposals for Limited Subject of law Status. *International Journal of Law and Policy*, *1*(4). https://doi.org/10.59022/ijlp.55