Journal of Infrastructure, Policy and Development 2025, 9(1), 10722.
https://doi.org/10.24294/jipd10722

Article

Criminal liability for the misuse and crimes committed by AI: A comparative analysis of legislation and international conventions

Dalia Kadry Ahmed Abdelaziz

Prince Sultan University, Riyadh 12211, Kingdom of Saudi Arabia; Dkadry@psu.edu.sa

CITATION

Abdelaziz DKA. (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

ARTICLE INFO

Received: 4 December 2024
Accepted: 26 December 2024
Available online: 13 January 2025

Abstract: Artificial intelligence is experiencing unprecedented advancements, leading to the emergence of autonomous superintelligent systems that surpass human intelligence in various fields. These systems present novel legal challenges, particularly concerning criminal liability for crimes they may commit. This research examines the current legal frameworks. These frameworks are designed to determine the criminal liability of autonomous superintelligent system, with a focus on issues of intent, autonomous will, and their implications in the context of superintelligent AI. The study highlights specific potential crimes, including cybercrimes and privacy violations, and underscores the urgent need to develop new legal frameworks that address the unique risks posed by these systems. Additionally, the role of international conventions, such as the Budapest Convention, in shaping global standards for these challenges is evaluated. The research argues that current legislation is inadequate and emphasizes the need for legal reform to keep pace with technological advancements, offering a forward-looking approach to criminal responsibility in the age of Artificial Super intelligent.

Keywords: legal personality of AI; advanced intelligence; autonomy decision making; independent will; autonomous vehicles; AI- related cybercrimes

1. Introduction

Modern technology represents one of the most significant achievements of the twenty-first century, reshaping daily life and global interactions.

Among these innovations, artificial intelligence (AI) stands out as a transformative force. It influences domains ranging from personal virtual assistants to complex industrial and healthcare systems. As reliance on AI deepens, interest in advanced systems such as Artificial Super Intelligence (ASI) has grown significantly. ASI, a theoretical stage of AI development, surpasses human intelligence across multiple domains and raises unprecedented legal and ethical questions.

AI is commonly understood in three levels: Narrow AI (or Weak AI) focuses on narrow tasks like voice recognition and chatbots, of which the above-mentioned fall under; Artificial General Intelligence (AGI) is when a machine can (in theory) do any intellectual task at a human level; and finally, Artificial Super Intelligence (ASI), where it is believed to far exceed the capabilities of humans. AGI is not yet realized, and ASI is purely speculative (theoretical), thus also requiring a cautious and hypothetical stance in terms of implications.

The rapid evolution of AI introduces profound legal and ethical challenges. Particularly concerning accountability for autonomous systems' actions.

Self-evolving AI, driven by advanced algorithms, often surpasses traditional control mechanisms. Complicating the attribution of responsibility. Potential harms include cybercrimes such as fraud, data breaches, as well as liabilities arising from autonomous transportation technologies—such as self-driving cars, drones, and trains. The integration of AI into healthcare and advertising further heightens concerns related to confidentiality, privacy, and ethical standards.

Through comparative legislation and international conventions, this paper critically analyzes the criminal liability of ASI. It considers fundamental legal questions such as whether ASI systems should be given legal personality and how liability for their actions might be distributed. It further examines several legal issues, including intent and independent will, discussing whether they apply to ASI systems. Focusing attention on the shortcomings of existing laws, along with case studies detailing AI-centric offenses in different fields, the study emphasizes the necessity for new legislation that reflects the pace of technology.

Its content is organized as follows: In the first section, it considers AI's assimilation into several sectors and identify legal and accountability challenges. The second section centers around the particular issues ASI raises in the realm of intent, independent will, and criminal liability. The third section looks into potential crimes related to ASI, and addresses the issue of the distribution of responsibility among stakeholders, including manufacturers, operators, and the systems. The fourth section juxtaposes national and international statutory approaches to criminal liability for AI, focusing on gaps and opportunities for legislative reform. In the long run, the paper ends with some suggestions like legal solutions and technical solutions, which help include regulating superintelligent AI.

2. Literature review and theoretical framework

The aim of this research is to address the criminal liability of artificial superintelligence, as one of the legal challenges given by autonomous advanced systems. The key research question, therefore, is this: How can the principles of traditional criminal liability be applied in the case of ISI capable of making complex, independent decision-making without direct human intervention? What can we use for the legal basis to establish the criminal liability of these superintelligent systems? The research draws on the theoretical framework for how traditional criminal liability concepts mesh with contemporary theories of superintelligent AI interfacing with the law as a way to answer these questions.

Although the theoretical framework is based on traditional theories of criminal liability such as the theory of intent and volition, this includes laying out how these concepts relate to superintelligent AI systems, in front of heather, could make independent and complex decisions more effectively than humans. The paper also refers to the progress of these theories with respect to ASI, which is capable of making calculations that human logic and analysis cannot handle. This analysis is connected with a review of legal literature and previous studies related to existing legal frameworks, concerning the criminal liability of intelligent systems under national and international law.

The problem of the criminal liability of artificial intelligence has been addressed in several studies, from the enforcement of traditional criminal law rules to intelligent systems (Johnson, 2021), "The Future of AI Criminal Liability" or the problem posed by autonomous systems (Wilson, 2020) "Superintelligent AI and Legal Frameworks".

Several studies have also explored comparative legal models on AI across legal traditions in the European Union, United States, and some specific Asian countries (i.e., "Global AI Legislation," by Marco and Gra (2022). This research is thus justified by the apparent gap of research linking the branches of law discussed here to traditional theories of criminal liability, as applied to ASI. It conducts a comparative analysis between different international and domestic legislations, in light of the legislative vacuum surrounding the criminal liability of ASI, the aim is to present legal proposals that can provide practical insights into new laws that would be informed by theoretical gaps in the literature, in the near future.

The case study follows an analytical methodology, including exploration of legal literature on relevant legislation of ASI and the accountability of organizations managing these systems. The study draws a practice data to explore how different countries manage legal issues around AI. This analysis seeks to present possible methods of instituting criminal liability on ASI, and find legal venues to prosecute and combat evolving problems in this realm. The work seeks to offer practical recommendations that can provide closure for legal lacunas and inform prospective legislation to tackle the challenges, presented by superintelligent AI systems through the combination of theory and practice.

3. Artificial intelligence in various sectors: Legal challenges and accountability

Artificial intelligence (AI) technologies have become essential in modern society, transforming sectors such as healthcare, education, law enforcement, and transportation (Russell and Norvig, 2020; Smith, 2019). These technologies enable machines to perform tasks requiring human intelligence, such as learning, problem-solving, and decision-making. AI is categorized into three main types: Narrow AI (or Weak AI), designed for specific tasks like voice assistants (Russell and Norvig, 2020); General AI, capable of performing any intellectual task a human can; and Superintelligent AI, which surpasses human capabilities and raises serious ethical concerns (Amuda and Rahman, 2024; Bostrom, 2014).

In the legal field, AI is integrated into diverse applications. Machine learning algorithms analyze criminal evidence, detect patterns in criminal behavior, and support parole decisions (Jelonek et al., 2019). Law enforcement agencies use AI to analyze crime scene data and employ facial recognition to identify suspects and solve cases (Akerkar, 2019). In correctional facilities, AI assists in assessing inmates and generating parole recommendations. It also shows potential for autonomously managing correctional facilities, optimizing operations, and reducing the reliance on human supervision (National Institute of Corrections, 2022)

AI advancements are particularly evident in transportation, especially in autonomous vehicles (Alanazi and Alenezi, 2024a). Self-driving cars, produced by companies like Tesla, Audi, and Nissan, operate independently using AI, raising critical liability questions in cases of accidents or malfunctions (Nyholm, 2018). Similarly, drones are increasingly used in logistics and surveillance, completing tasks such as aerial photography, traffic monitoring, and goods delivery without human intervention. These innovations underline the need for clear regulations to address accountability when AI-powered transportation systems cause harm or breach legal norms.

However, as AI systems like autonomous vehicles and drones become more independent, they challenge traditional frameworks of criminal responsibility. Unlike humans, AI systems lack moral judgment and empathy, making decisions autonomously (Nilsson, 2014). This autonomy complicates legal concepts of accountability, raising new questions about responsibility when AI-driven technologies cause harm or violate laws. As AI continues to evolve, legal systems must adapt to address these unique challenges.

The integration of AI into smart transportation and urban infrastructures, particularly in countries like the UAE, represents a new frontier. It highlights the intersection of technological advancements and legal implications. Updated regulatory frameworks are essential to govern these developments and manage the complexities they introduce (Alanazi and Alenezi, 2024b) With each step toward ASI, the implications for criminal law continue to grow. With ASI existing at a level superior to human intelligence, the temptation to abuse ASI, or to deploy it for criminal purposes, increases. For instance, if an ASI system autonomously plans and executes cyberattacks, manipulates financial markets, or engages in espionage, the issues of culpability become more difficult to untangle. This raises challenges to traditional notions of liability and accountability in criminal law, given that there is no human operator present. If a system were to commit a crime autonomously, for example, a crime that aims to deceive society by the force of public sentiment, such as conduct via social networking, or one that harms society, such as automated health problems and finance sectors, choosing who would have responsibility for these crimes—be it the community, developers, users, or the system—would be critical (Bostrom, 2014; Amuda and Rahman, 2024).

This situation presents ethical and legal dilemmas; for example, whether or not ASI could be a legal entity and, if it can, how to prosecute it. In addition, for malfunction and unexpected consequences, for example, an ASI machine learns by itself and starts hurting people, going beyond the scope of human intervention, alluding to the very contentious issue of liability. For example, would the designers of the ASI be liable, or would it be the institutions that utilize these technologies? What is needed now is the development of new accountability frameworks for ASI as it shifts from theory to reality, balancing progress with responsible ASI development and deployment, while ensuring these technologies do not fall into the wrong hands and the potential misuse of ASI by criminals.

Smart Transportation & Urban Infrastructures: The application of AI in smart transportation and urban infrastructures, especially in several countries such as Singapore, exemplifies a new frontier. It underscores the convergence of technology and law. Regulatory frameworks need to adapt to these developments and manage their complexities (Lee and Ang, 2022).

4. Legal challenges in defining criminal liability for artificial superintelligent systems

The rapid development of artificial intelligence, especially superintelligent systems, presents intricate legal challenges regarding the attribution of criminal responsibility. These technologies operate autonomously, exhibiting possibly behaviors, that are not easily traced back to human influence. Traditional principles of criminal law, which emphasize intent and conscious decision-making, face significant limitations in addressing such advancements. As ASI exhibit increasingly autonomous decision-making capabilities, the demand for modernized legal frameworks, to face the future implications, becomes imperative. These frameworks must reconcile technological innovation with the principles of justice and accountability especially in contexts like space exploration, where jurisdictional issues add further complexity.

4.1. Definition of autonomous superintelligent systems

Artificial Super Intelligence could be imagined as a form of artificial intelligence that surpasses human capabilities across all domains, including creativity, problem-solving, decision-making, emotional and social understanding. Such systems might be capable of self-learning and continuous improvement without human intervention, thereby granting the ability to make independent decisions. ASI are distinguished by their self-learning abilities, which allow them to continuously improve over time without additional human input. In theory (ASI) systems could possess decision-making autonomy, allowing them to operate independently and make decisions based on internal algorithms, without direct human control. Furthermore, these systems could possess the capacity for emotional and social understanding, which would complicate the issue of legal responsibility, especially when interacting with humans in ways that require ethical and legal considerations. Artificial Super Intelligence has the potential to outperform human abilities across all cognitive fields, with concerns about the possible risks associated with its self-improvement and self-control capabilities. These systems could pose significant challenges in assigning legal responsibility, as their actions may no longer be traceable to any single human actor (Bostrom, 2014). The evolution of AI towards autonomous decision-making might not only focus on efficient task performance but also on enabling systems to make decisions, based on continuous learning. This autonomy would likely create unprecedented challenges for the legal system, making it difficult to identify a responsible party, when decisions lead to harm or unlawful actions (Russell and Norvig, 2020). Concerns have been raised about the potential threat posed by (ASI) if not properly controlled through design and programming (Hawking and Musk, 2020). The ability of these systems to act independently would likely raise critical questions about accountability, as their decisions are made outside direct human control, presenting challenges for traditional legal frameworks that rely on human intent and oversight.

To better illustrate the differences between Narrow AI, AGI, and ASI, following **Table 1** highlights their capabilities, potential risks, and examples of malicious actions. This comparison provides a clearer understanding of how these AI types differ in their impact and associated challenges.

Table 1. Types of Artificial Intelligence: Capabilities, Risks, and Malicious Applications.

AI Type	Capabilities	Potential Risks	Examples of Malicious Actions
Narrow/Weak AI	Task-specific intelligence, designed for single tasks.	Limited to specific tasks, minimal autonomy.	- Fraudulent recommendations in financial services.
	Often relies on pattern recognition and data processing.	Can be exploited by malicious actors.	- Manipulation of social media content (e.g., fake news generation).
AGI (Artificial General Intelligence)	Hypothetical AI capable of understanding and performing any intellectual task a human can do.	Could surpass human control, leading to unexpected outcomes.	- Unintended consequences from autonomous decision-making in critical systems (e.g., healthcare, transportation).
	Adaptive and able to generalize across tasks.	Risk of prioritizing goals over human values.	- Overriding safety protocols or making decisions without ethical considerations.
ASI (Artificial Superintelligence)	Superior intelligence to human capabilities across all domains.	Potential to cause large-scale destruction if misaligned.	- Full autonomy in decision-making, potentially leading to existential threats (e.g., autonomous weapons, economic manipulation).
	Self-improvement, potentially leading to rapid, uncontrollable advancements.	Risks of autonomous system exploitation or harmful objectives.	- Manipulating or controlling major industries, governmental bodies, or military powers.

This classification serves as a foundation for analyzing the legal challenges associated with autonomous and superintelligent AI systems, which are discussed further in the following sections (Bostrom, 2014; Hawking and Musk, 2020; Russell and Norvig, 2020).

4.2. Legal issues in intent and independent will for criminal liability of artificial super intelligence

Intention and independent will are essential for determining criminal liability. Legal systems typically require these elements to establish criminal intent. However, highly ASI, could a challenge traditional understanding of intent and will (Chalmers et al., 2023). while ASI might be envisioned as capable of making decisions, it could be still argued that such systems are ultimately shaped by human designed and programming (Rubinstein, 2022). The issue arises when these systems hypothesized to self-learn, adapt and make decisions seemingly beyond human control. That leads to s critical questions: Could these decisions potentially be considered as stemming from the system’s independent will? How could criminal intent be assessed in the absence of traditional human qualities such as awareness or moral judgment (Smith, 2022)?

Scholarly opinions on criminal liability for AI vary, particularly ASI, one perspective could be argued for maintaining traditional legal principles, limiting liability to humans—programmers or operators—since the ASI lacks awareness and will, and there for could not be criminally accountable (Chalmers et al., 2023). Others propose shared liability, distributing responsibility between the ASI system and its creators or operators (Rubinstein, 2022). Alternative approach might propose that highly ASI system should be treated as legal entities capable of independent criminal liability, due to their ability to make complex decisions autonomously (Smith, 2022). Finally, some advocate for regulatory or social liability, placing responsibility on organizations that own and control ASI systems with an emphasizing on stringent regulation (Jones and Walker, 2023).

The third approach, advocating for independent criminal liability for highly autonomous systems seems to be seen as the most fitting given the advancements in. As these systems make independent decisions, attributing responsibility solely to humans may no longer suffice. Limiting liability to developers or operators fails to account for the significant role played by ASI in decision-making, that leads to harm. In this hypothetical future, a flexible and adaptive legal framework might be required to address these evolving challenges, ensuring accountability and protecting individual rights.

4.3. The legal labyrinth of the criminal responsibility of superintelligent systems in new borders

Such superintelligent systems may act without any human oversight, causing the issue of their criminal responsibility to be probably more complex than we already know, in cases of, for example, interplanetary technology. This poses fundamental questions regarding the relevance of established precepts of law, like mens rea and agency, in instances where human participation is limited or non-existent. For instance, if superintelligent autonomous systems were operating decentralized operations in entities in, say, space, could their decision-making be viewed as autonomous will, the will of an alien? When the variables in question might be entirely unknown or unknowable, how could any criminal intent be measured? “There is a company—it is simply there, nothing more than digital colonialism” (Binns, 2018; Galloway and Armstrong, 2018).

Previous studies of AI criminal liability have largely addressed AI systems that reside in the human-defined confines of legal jurisdiction, often constrained by geography. Nonetheless, in the scenario where superintelligent systems transcend Earth and function in space or other ungoverned domains, we may not be able to sufficiently cover them with pre-existing legal frameworks, the ones designed for human-native AI. In these new contexts, where these systems are able to make decisions based on variables that we cannot foresee or even comprehend, the issues of intent and independent will become even more complex. If, for example, an ASI system in space autonomously damages something or somebody else, it might prove challenging to hold it criminally liable given the lack of human actors involved, and no oversight or jurisdiction.

In such instances, adapted legal frameworks may prove too sluggish to address these new realities, and assigning accountability may become impossible (Wright, 2020). If jurisdiction is unclear and these systems can function beyond the reach of humans and our legal systems, how do we create responsibility when superintelligent systems make decisions that affect the broader universe, far beyond the reaches of any human border? Such complexities indicate that a brand-new framework for legal accountability may need to be developed, one capable of addressing the unprecedented independence and new frontiers of superintelligent AI systems (Binns, 2018).

5. Potential crimes in artificial superintelligent systems and criminal liability: Who bears the responsibility?

Superintelligent systems are among the most prominent technological innovations, raising numerous legal and ethical concerns. A key issue is criminal liability when damages or crimes result from their use. As these systems develop rapidly, their ability to make independent decisions becomes central, prompting questions about who should bear responsibility for crimes or accidents. Should manufacturers be held accountable for technical defects or programming errors, or should operators or users be liable for misuse or negligence (Kroll et al., 2024)? A more pressing question is whether these systems themselves can be held criminally responsible. Given their decision-making autonomy, can artificial intelligence be deemed capable of legal responsibility, or is responsibility confined to human parties (Maastricht University, 2023)? These questions require thorough examination as the reliance on superintelligent systems continues to grow across various sectors, opening the door to future discussions on potential crimes and criminal liability (Oxford University Press, 2024).

5.1. The potential crimes arising from superintelligent systems and their impact superintelligent

systems present a range of potential crimes across various sectors, including economic, digital, environmental, and logistical fields. These technologies are becoming increasingly integrated into daily life, raising concerns about liability when crimes or damage occur. A critical issue is determining whether the systems themselves can be held criminally responsible, or if accountability should rest with manufacturers or operators (Lau and Haug, 2018).

In the economic sector, AI can manipulate financial markets through high-frequency trading algorithms operating autonomously. Without proper oversight, these systems could cause market fluctuations or crashes, similar to the 2010 “Flash Crash”, where algorithmic trading led to significant financial losses (Kroll et al., 2024). Responsibility in such cases may fall on the companies developing the software or operators failing to supervise the systems, for example, Narrow AI applications have been involved in financial mismanagement due to algorithmic failures or biases, such as when AI-driven credit scoring systems erroneously deny loans to individuals based on faulty data interpretation (Eubanks, 2018).

In the digital realm, AI systems may be involved in cybercrimes, such as hacking or data theft. AI-powered malware can exploit vulnerabilities in digital security to steal sensitive information, violating privacy on a large scale (Maastricht University, 2023). Narrow AI, such as phishing bots, may impersonate individuals and manipulate users into disclosing personal data. Additionally, AGI and ASI systems could autonomously execute cyberattacks, making it difficult to trace their actions back to human perpetrators, thereby complicating the issue of accountability.

Additionally, AI systems could manipulate public opinion or elections by spreading false information or influencing voting patterns, raising ethical and legal concerns about criminal liability for developers.

Regarding environmental crimes, AI's role in energy systems presents significant risks. A loss of control over autonomous renewable energy systems or factory management could result in pollution or environmental harm (Bryson et al., 2023). Decisions made by AI without human oversight could lead to irreversible damage to ecosystems, raising the issue of responsibility for environmental violations caused by autonomous technologies. This could apply to both Narrow AI, which controls specific environmental systems, and potentially to superintelligent systems capable of operating entire infrastructures with unknown outcomes.

In the logistics and military sectors, autonomous vehicles such as self-driving cars, drones, and trains may cause accidents due to programming errors or system failures. A notable incident in 2018 involved an Uber self-driving car that failed to avoid a pedestrian, illustrating the risks associated with insufficient decision-making abilities in autonomous vehicles. Likewise, AI applications in military contexts, like autonomous drones and weapon systems, could lead to unlawful attacks or violations of human rights if these systems make decisions that conflict with international law, raising important questions about accountability (Chavannes et al., 2021). AGI or ASI systems in the military may have the capacity to act without human intervention, creating more complexity in the determination of liability for unlawful actions or war crimes committed by autonomous weapons.

5.2. Criminal liability of manufacturers and operators in advanced systems

Advanced systems capable of autonomous decision-making, such as ASI, may operate based on independent algorithms. However, the responsibility of manufacturers and operators remains unchanged. These systems do not function in isolation; it is the companies and operators who design, program, and manage their development. They are responsible for ensuring that the systems operate within safety parameters and comply with legal and ethical standards. Effective corporate governance plays a crucial role in this context, as it establishes frameworks for accountability and risk management. Research shows that governance codes can significantly influence operational efficiency and compliance, thus reducing the risks associated with advanced systems, particularly those involving ASI (Yaghi, 2024).

If companies fail to meet these responsibilities, such as by neglecting preventive measures or permitting unsafe conditions, they can be held criminally liable, regardless of the autonomy of the decisions made by these systems, this demonstrates that criminal liability for manufacturers is compatible with the concept of autonomous systems especially ASI. Even when systems make decisions based on independent algorithms, the foundational rules set by developers remain crucial in determining liability. Manufacturers are responsible for programming errors, technical flaws, and for failing to implement necessary precautions to minimize risks.

Factors like malice, error, and negligence play a key role in determining criminal liability. For instance, if companies ignored risks or failed to monitor systems effectively, they could be held accountable for negligence. Similarly, operators can be criminally liable if they used the systems in unsafe conditions or did not follow manufacturer instructions. This holds particularly true in the case of ASI, where the system may make decisions based on variables far beyond human comprehension or control. In the case of Artificial Superintelligence (ASI), systems would be able to make military decisions without human involvement, which may create complexity in correctly attributing guilt for unlawful actions or war crimes by autonomous weapons. Should ASI in the military make decisions about attacks without human oversight, breaches of international law, as well as crimes against humanity, could ensue while generating thorny legal questions about accountability.

Manufacturers and operators still hold a central position in criminal liability. Or, more reasonably, even where systems exhibit "autonomy", they must define the standards and safeguards that will maintain safety and integrity. In contrast, critics claim that companies should not be held liable for decisions made by intelligent systems, as doing so raises difficult legal questions (Guerra et al., 2022). Others argue that conventional legal constructs may be insufficient to properly regulate how such systems behave. Liability for such events will need to be based on a specific understanding of how these systems make other decisions. In evolving systems, for instance, algorithms in the context of autonomous systems, accountability becomes more challenging to pin down (Binns, 2021).

Such systems behaving unpredictably lead us to assess fault and culpability, prompting new legal interventions. Others, therefore, claim that if these intelligent systems are autonomous enough to make company liability hard to hold, this would be a case of misapplied criminal liability (Kubica, 2022). Critics of this phenomenon are calling for reforms to the judicial system to address these cases appropriately with legislation that allows for more flexibility in adjudicating legal responsibility. Nonetheless, having differing perspectives does not dilute the need to hold manufacturers and operators responsible for the systems they build. E.g., so long as they control the design and operation of systems, their obligation to guarantee safety and adherence to the law and ethical standards remains paramount (Stanford Law School, 2018).

5.3. Criminal liability of artificial super intelligence entities: Legal and practical challenges

Artificial Superintelligence entities present unprecedented legal challenges in determining accountability for harmful actions, resulting from their independent decision-making process. While ASI systems are theoretically capable of making autonomous choices, they lack independent legal personality, rendering traditional sanctions—such as fines, imprisonment, or detention—inapplicable (Akpuokwe et al., 2024), at this point, developers and operators bear most of the liability for the actions of these systems. Nonetheless, this framework rapidly grows complex when ASI systems do not operate under the direct guidance of a human, drawing attention to the need for all new legal considerations.

Researchers have suggested some new legal regimes that account for the peculiar features of ASI systems in order to tackle these issues. If ASI is capable of operational suspension or deactivation, sanctions focused around these concepts may serve as useful tools for ensuring accountability (Lin et al., 2017).

*Conceptual Framework: The Sui Generis Nature of ASI Personality and Joint Responsibility.

They present unique challenges to established legal doctrines due to their autonomous decision-making ability, ability to learn independently, and adaptability. These attributes set them apart from both human agents and traditional corporate entities, necessitating a reconsideration of traditional legal doctrines (Leenes et al., 2017). In order to adapt to the theoretical nature of ASI, this section proposes an intermediate-level treatment that captures the autonomy of these systems while preventing these systems from being treated as equivalent to human actors (Pagallo, 2013).

Another potential remedy is collective responsibility, which would disperse responsibility for an ASI system among other ASI systems and its builders, operators, and users. This framework takes into consideration how much human involvement factored into the decisions, how much autonomy was afforded the system, and the foreseeability of harm (Calo, 2015; Gless et al., 2016). A shared liability system allows legal systems to be monitored and adjusted, enabling them to remain just both in the sense of flexibility and fairness whilst addressing the evolving nature of risks associated with ASI.

*Accountability Framework in the proposal. The **Table 2** proposes a theoretical model about how the liability responsibility should be split among the different stakeholders involved in the development and operation of ASI systems. This model highlights the speculative nature of ASI accountability as a starting point for future legal discussions.

Table 2. Potential Liability of Stakeholders in Autonomous Superintelligent Systems.

Example	**Potential Liability**	**Stakeholder**
An ASI system misinterprets ambiguous programming, causing harm	Liability for foreseeable risks arising from design flaws or inadequate safeguards	Developers
Negligence in managing updates leads to unauthorized system action	Liability for failing to monitor or control ASI systems adequately	Operators
A user knowingly deploys an ASI system in prohibited or harmful activities	Liability for misuse or intentional exploitation of ASI system	Users
Suspension or deactivation of the ASI system after causing harm autonomously	Hypothetical liability under a sui generis framework recognizing limited ASI culpability	ASI Entities

6. Future Directions for AI Accountability

Until the future where we have an AI that stands equivalent to human intelligence comes to pass, we need to step forward and try to outline the laws that govern our behaviors with an AI that harbors the same characteristics as a higher human. In order to bring justice and protect society when ASI capabilities become practical, we need to build a hybrid model of accountability which takes aspects of both joint responsibility and sui generis legal personality.

*Challenges of artificial superintelligent systems for judicial application.

In the domain of superintelligent systems, courts encounter multiple difficult challenges in terms of determining criminal liability. These systems lack independent legal personhood under today's legal frameworks, but legal cases have made some headway on the issue of liability for systems that can make autonomous decisions. A popular one is related to accidents caused by the latest medical technologies like the "Da Vinci Surgical System." When problems arise because of either malfunctioning systems or programming errors, identifying liability is a complex question. Cases like these highlight the importance of holding manufacturers responsible for the damages caused (Expert Institute, 2021).

Cybersecurity incidents associated with artificial intelligence systems are another example of these challenges. If intelligent systems that are meant to mitigate cyberattacks are vulnerable themselves, then the damage can be extensive. These incidents bring to light critical questions regarding accountability on the part of developers and operators of such technologies (Loaiza et al., 2019). Moreover, the proliferation of superintelligent systems across various sectors—from health care to defense—presents intricate legal quandaries as we try to figure out how to fairly apportion liability when these systems act in their own best interest. The increasing complexity and chaotic behavior of these systems only compound the legal dilemma (Calo, 2015).

These scenarios illustrate the complex legal issues surrounding superintelligent systems as well as the need for strong legal frameworks. Such frameworks need to balance the value of driving technology with the need to establish accountability. Recent studies point out that the development of superintelligent systems will require fundamental changes to current legal systems (Gless et al., 2016). Cross-sectoral incorporation of AI creates unique challenges to the attribution of criminal liability, as the existing legal framework has failed to account for the degree of autonomy displayed by such systems. This will require the legal systems to evolve and fill the gap between traditional AI technologies and systems that have advanced autonomy and reasoning (Bryson et al., 2017). Furthermore, safeguards must be implemented to protect individual and social rights, especially when harm occurs that is no longer under direct humanitarian power.

Considering the aforementioned legal difficulties, it is essential to discuss a more formal theory of responsibility with respect to superintelligent systems. The **Table 3** below offers a suggested schema for allocating responsibility to different parties in the design, running, and use of ASI systems. This model will serve as a jumping-off point for future conversations and attempts to describe potential duties depending on various situations that might unfold.

Table 3. Comparison of AI Types: Capabilities, Risks, and Malicious Actions.

AI Type	Capabilities	Potential Risks	Examples of Malicious Actions
Narrow/Weak AI	Task-specific intelligence, designed for single tasks.	Limited to specific tasks, minimal autonomy.	- Fraudulent recommendations in financial services.
	Often relies on pattern recognition and data processing.	Can be exploited by malicious actors.	- Manipulation of social media content (e.g., fake news generation).
AGI (Artificial General Intelligence)	Hypothetical AI capable of understanding and performing any intellectual task a human can do.	Could surpass human control, leading to unexpected outcomes.	- Unintended consequences from autonomous decision-making in critical systems (e.g., healthcare, transportation).
	Adaptive and able to generalize across tasks.	Risk of prioritizing goals over human values.	- Overriding safety protocols or making decisions without ethical considerations.
ASI (Artificial Superintelligence)	Superior intelligence to human capabilities across all domains.	Potential to cause large-scale destruction if misaligned.	- Full autonomy in decision-making, potentially leading to existential threats (e.g., autonomous weapons, economic manipulation).
	Self-improvement, potentially leading to rapid, uncontrollable advancements.	Risks of autonomous system exploitation or harmful objectives.	- Manipulating or controlling major industries, governmental bodies, or military powers.

Furthermore, superintelligent systems are to be both highly advanced and fluid, which will require a flexible set of legal parameters in order to tackle the complex problems associated with liability. As technology progresses, the demand for creative approaches to establish accountability will be even more pressing, prompting continuous legal adaptation and the establishment of strong guardrails, which is very crucial (Democratic Arab Center for Strategic, Political, and Economic Studies, 2024).

7. Frameworks for addressing criminal liability of autonomous superintelligent systems: National and international perspectives

The rapid development and widespread use of autonomous superintelligent systems (ASI) in various sectors, have created an urgent need for legal frameworks, to address the challenges of assigning criminal liability. A comprehensive response is required, integrating both national and international legal systems to ensure accountability and foster innovation.

Major jurisdictions like the United States, the European Union, and China are actively developing national legislation to address these issues. However, these efforts are often insufficient to address the complexities of superintelligent systems, As ASI continues to evolve, existing frameworks frequently struggle to keep pace with rapid advancements in AI, highlighting the need for updates to current laws and the formulation of new international agreements. For instance, the United Arab Emirates (UAE) has emerged as a global leader in AI governance and regulation. By implementing frameworks that prioritize both technological innovation and legal accountability, the UAE demonstrates its commitment to leveraging superintelligent systems responsibly (Almheiri et al., 2024).

This integrated approach underscores the importance of combining national and international efforts to effectively address the criminal liability of autonomous superintelligent systems (ASI). By analyzing the legal frameworks of key jurisdictions, the following sections will explore the challenges and opportunities in this rapidly evolving field (Calo, 2019).

Nonetheless, the international legal framework that governs space activities today is far from complete, especially concerning ASI, in particular superintelligent autonomous systems that might be used in outer space. While the 1967 Outer Space Treaty holds states "individually and jointly" responsible for space activities, it does not address the issue of criminal liability for intelligent systems operating beyond Earth. This gap necessitates the creation of new laws to define criminal liability for space-based autonomous systems, especially in scenarios where national authorities lack jurisdiction (United Nations Office for Outer Space Affairs, 1967). Legal scholars advocate for new international agreements to adequately address these emerging challenges as ASI continue to develop in space exploration (Kling, 2019; Viscusi, 2021).

*****Empirical Evidence on the Impact of Legal Frameworks on the Development of AI.

As proven by empirical evidence, legal frameworks significantly affect the development of Autonomous Superintelligent Systems — ASI. For instance, Jones et al. Smil (2013) highlighted that the lack of clear and harmonized artificial intelligence regulation in the USA has led to delayed adoption, especially in the domains of autonomous vehicles. Issues on regulatory compliance and liability have left many ASI technologies in an experimentation phase. The Computer Fraud and Abuse Act (CFAA) and similar legislation are out of date and cannot accommodate the operation of AI systems autonomously in the physical world and therefore aren't addressing damage/harm caused by AI systems (U.S. Department of Justice, 2023).

As an example, Smith (2022) shows how overregulation in the European context has impeded the growth of AI technologies across many sectors like health and fintech. The General Data Protection Regulation (GDPR), although essential for protecting privacy, is regarded by some as too strict, making it harder for AI start-ups to create fresh applications. The GDPR has proved a significant hindrance to innovation due to the red tape and high compliance cost involved, particularly for small- and medium-sized enterprises (Vogt and von dem Bussche, 2017). In a similar vein, Roland Berger (2024) also emphasizes that EU AI companies have experienced significant rollouts because of complex legal standards that require compliance, which has programmed Europe's AI race to be less competitive globally.

In contrast, Zhang (2023) indicates that the relatively flexible regulatory environment prevailing in China has allowed for rapid progress in AI; however, he cautions that the Chinese authorities have not yet enacted specific legislation regarding ASI, which could have dire consequences, primarily in vital areas, such as healthcare and transportation, affected by autonomous decision-making systems that could generate substantial risks. While the Measures for Managing Generative AI (Ministry of Industry and Information Technology of the People's Republic of China, 2023) are an important step towards regulating new technologies, there are significant gaps in addressing the risks that ASI presents as an emerging technology.

These empirical findings suggest that while some jurisdictions are stepping up to regulate AI technologies more broadly, there remains an incredible deficit of coherent, future-oriented laws governing autonomous superintelligent systems (ASI). The urgent demand is for relevant, contemporary legal structures allowing the innovation and security of ASI technologies in a pragmatic manner.

7.1. Legal framework in the United States

In the United States, legal frameworks are beginning to address issues of responsibility for ASI systems, but significant challenges remain. A key piece is the application of the Computer Fraud and Abuse Act (CFAA), which serves as a cornerstone for combating cybercrimes. While the CFAA primarily targets crimes involving human actors, its applicability to ASI is unclear. If ASI system is be implicated in cybercrimes or harm individuals or institutions, determining responsibility becomes a complex issue, particularly when the system operates independently of human oversight (U.S. Department of Justice, 2023). The Current legal framework fails to adequately address the autonomous decision-making of ASI. This gap in the law creates ambiguity regarding criminal liability, particularly when the ASI system's actions are not intentional but instead result from unforeseen errors or malfunctions. As ASI evolves to make more independent decisions, it is hypothesized that the need for legal updates will become increasingly urgent to accommodate these rapid advancements in technology and ensure appropriate accountability.

Furthermore, the concept of liability for manufacturers, operators, and programmers of ASI systems is also gaining attention. proposals suggest that the manufacturers should be held accountable for damages may be caused because of decisions made by ASI systems, Given the increasing presence of ASI in sectors such as healthcare, military applications, and space exploration, clear legal definitions for criminal liability are crucial. This will be essential to address the complex responsibility dynamics that arise when an ASI system acts autonomously.

The hypothesis that ASI could eventually be recognized, as a "legal entity" capable of bearing liability to include damages caused by unintended errors or malfunctions of ASI, rather than just actions that are deliberately caused by humans (Third Way, 2020).

In light of these developments, the United States will need to enhance its legal frameworks to address criminal liability for ASI. As these systems evolve, clearer laws will be essential to ensure accountability while supporting technological innovation (Third Way, 2020)

7.2. Legal framework in the European Union

The European Union (EU) has taken a leading role in addressing the legal challenges posed by emerging technologies, including autonomous intelligent systems (ASI). The EU's approach emphasizes a balance between fostering innovation, protecting human rights, and ensuring public safety. A cornerstone of this effort is the Artificial Intelligence Act (AI Act), designed to regulate AI systems by promoting innovation while safeguarding fundamental rights. The Act classifies AI systems based on their risk levels, imposing stricter requirements on high-risk systems, such as those used in critical infrastructures and law enforcement (European Commission, 2021).

In addition to the AI Act, the General Data Protection Regulation (GDPR) addresses privacy concerns, emphasizing transparency in the collection and processing of personal data. This regulation is critical for managing how intelligent systems handle personal data, influencing the development and deployment of AI technologies in Europe (Vogt and von dem Bussche, 2017).

Ethics also play a key role in the EU’s strategy. The Ethical Guidelines for Trustworthy AI, issued by the European Commission, aim to ensure that AI development respects human dignity and fundamental rights. These guidelines stress the importance of transparency, accountability, and the prevention of discrimination in the deployment of AI systems (European Commission, 2019).

Further, the Council of Europe has proposed a draft Framework Convention on AI and Human Rights, which aims to align the use of AI systems with fundamental human values. This initiative addresses broader legal challenges, focusing on the responsible and ethical use of these technologies, Given the increasing capabilities of ASI, it is hypothesized that future frameworks will need to specifically address the risks and rights associated with such systems (Council of Europe, 2021)

Despite the comprehensive nature of the AI Act, the EU faces challenges in keeping pace with rapid technological advancements. These include the need for regular updates to legal frameworks and ongoing debates about the adequacy of current laws to address the risks posed by superintelligent systems. While the AI Act is a significant step toward effective regulation, future adjustments will be essential to address emerging challenges and ensure the safe and ethical integration of advanced ASI systems (Council of Europe, 2021, Roland Berger, 2024)

7.3. Legal framework in China

In China, the government is actively developing a comprehensive regulatory framework for AI, with an emerging focus on superintelligent AI (ASI) and its criminal liability. The Personal Information Protection Law (PIPL) and the Cybersecurity Law are key pieces of legislation that regulate data usage within intelligent systems. These laws impose strict controls over data handling, marking a foundational step toward establishing a legal framework for AI, even though they do not specifically address superintelligent ASI.

In 2023, China also introduced the Measures for Managing Generative AI, which set standards for the safe and responsible use of AI technologies, including text and image generation tools.

Although no specific laws exist yet for Artificial Super Intelligence in China, the government is committed to developing incremental legislation that adapts to technological advancements. The aim is to continuously update AI-related legal frameworks to address emerging challenges in the field (Liu, 2023; Zhang, 2022; Ministry of Industry and Information Technology of the People’s Republic of China, 2017).

7.4. International agreements

The Budapest Convention on Cybercrime (2001) remains the primary international legal framework for combating cybercrime. However, as AI technologies, particularly ASI, continue to evolve, legal gaps in the convention become evident. While the convention addresses crimes such as hacking, cyber espionage, and online fraud, it does not specifically cover crimes may committed by autonomous or ASI systems that operate without human intervention (Council of Europe, 2021).

With the rapid development of ASI, the international community faces new challenges in determining criminal liability for superintelligent systems. A critical issue arises when an intelligent system causes harm or commits a crime, but no identifiable individual can be held responsible. This challenge is especially significant for superintelligent ASI, which operates independently through complex algorithms that may be beyond human comprehension or control (Anderson and Rainie, 2022).

In addition to the Budapest Convention, various international initiatives are underway to strengthen the legal frameworks for AI. A key development is the Council of Europe's Framework Convention on AI and Human Rights, signed in September 2024. This is the first binding international legal framework for AI regulation, focusing on human rights, democracy, and the rule of law. The agreement complements the EU AI Act, creating a risk-based approach to managing AI challenges and setting a precedent for international cooperation in AI governance. Although these agreements are still in their early stages, they represent a significant step toward establishing global standards for ASI regulation and addressing possible crimes related to ASI (Council of Europe, 2024; European Commission, 2024).

8. Towards legal and technical solutions: Addressing challenges related to autonomous superintelligent systems

With the rapid advancements in ASI, legal systems face significant challenges in regulating the legal responsibility of these autonomous systems. It is crucial to explore both legal and technical solutions, that might keep pace with these developments and provide effective ways to address the challenges posed by t ASI Effectively enforcing these laws and solutions requires implementation mechanisms, in addition to new frameworks. Such mechanisms need to encompass both legal frameworks and technological safeguards, including, for example, regulatory authorities, international collaboration on enforcement, and more sophisticated monitoring systems, to ensure that superintelligent systems do not violate legal and ethical norms. These solutions are briefly summarized below.

8.1. Development of new legal frameworks

A central issue in addressing Artificial Superintelligent systems is unconventional liability, as traditional concepts of criminal liability, which depend on identifiable individuals or entities, are difficult to apply. When possible, damage or crimes result from the actions of these systems, direct accountability cannot always be attributed to human entities, due to the system's autonomy or the complexity of its decision-making process.

One proposed solution is alternative liability, which holds entities with the power to influence the actions of intelligent systems accountable, such as developers or system operators. Instead of attempting to hold the AI system itself liable, accountability is directed toward the entities controlling these systems, such as the producing companies or operators. This allows for justice without assigning responsibility for each individual mistake, especially in systems that operate independently based on complex, often opaque algorithms.

Additionally, ongoing liability can be incorporated, extending to the monitoring of intelligent systems after deployment. In this model, companies and developers remain responsible for ensuring that intelligent systems continue to comply with legal frameworks and regulations, helping to prevent future harm. This reflects a shift in legal perspectives, viewing intelligent systems not as mere tools but as complex entities requiring continuous oversight to ensure no violations or damages occur (Janssens, 2018).

The development of legal frameworks is not limited to criminal liability but extends to various aspects of legal responsibility, such as civil liability, corporate responsibility, and individual civil rights. Regarding civil liability, it is essential to establish legal mechanisms for compensating damages caused by intelligent systems, particularly when identifying the responsible party directly is difficult. These frameworks might include fines or compensation methods for individuals or property affected by these systems’ actions.

Corporate responsibility requires legal frameworks, that ensure companies developing and operating intelligent systems are held accountable. These regulations should include requirements for transparency and integrity, in the design and implementation of systems, as well as ethical standards ensuring that the impact of these systems on society and safety is positive. To protect individual rights, laws should safeguard against negative impacts of intelligent systems, such as privacy violations or discrimination. Legal frameworks must include mechanisms for individuals to object to decisions made by these systems and seek compensation if their rights are infringed upon.

Overall, the development of legal frameworks for Artificial Super Intelligence requires a comprehensive legal system, that addresses various aspects of responsibility, including criminal and civil liability, corporate responsibility, and the protection of individual rights, ensuring justice and safeguarding social interests in this evolving field (Council of Europe, 2020; Dignum, 2020; European Commission, 2023; US Department of Commerce, 2022).

8.2. Technological solutions to strengthen the legal governance of superintelligent systems

As reliance on superintelligent systems grows, the need for innovative technical solutions to support legal frameworks becomes increasingly urgent. Effective governance requires integrating both legal and technical aspects to ensure accountability and transparency.

One effective technical solution is the development of intelligent monitoring systems capable of tracking the decisions made by superintelligent systems. These systems use technologies like Explainable ASI to provide clear insights into how decisions are made, enhancing trust in these systems. Additionally, machine learning techniques can be integrated with legal compliance, verification tools to ensure that intelligent systems remain compliant with existing laws (Dignum, 2020; European Commission, 2023).

Other solutions include the use of blockchain technologies, to enhance transparency and trust in decision-making processes. Blockchain records each decision-making process in an immutable ledger, ensuring integrity and facilitating audits and investigations in case of violations (Council of Europe, 2020; US Department of Commerce, 2022).

Collaboration between stakeholders, through technological platforms, shared between regulatory authorities and companies is also necessary. These platforms facilitate communication and coordination, helping to ensure that systems remain compliant with legal standards. Flexible technical policies must also be established to allow quick updates to systems, ensuring their ongoing alignment with legal changes (Dignum, 2020).

8.3. International cooperation: The need for coordination among countries to address (ASI) challenges

Addressing the legal challenges of ASI systems requires effective international cooperation. Given ASI’s global impact, coordinating legal frameworks across countries is essential to establish common policies that regulate the criminal and civil liability of these systems. International cooperation enables the exchange of legal knowledge and expertise, contributing to the development of standardized practices, avoiding legislative contradictions that may hinder justice or accountability (Council of Europe, 2020; European Commission, 2023; US Department of Commerce, 2022).

This collaboration, may require the creation of comprehensive international agreements, to impose uniform standards on companies operating AIS. Such agreements could ensure that companies are held accountable based on clear legal responsibilities, including commitments to transparency and integrity, preventing possible harm from these systems (Dignum, 2020; European Commission, 2023). Specifically, international cooperation should focus on safeguarding individual rights, protecting against privacy violations, discrimination, and providing clear mechanisms for compensation in cases of harm.

8.4. Avenues to bring legal frameworks to bear on superintelligent systems

Socio-technical frameworks lack full consideration when extrapolated to superintelligent systems and will be unable to resolve the enforcement of laws that apply to such systems. There is a growing need for dialogue between national and international legal frameworks, as well as technical tools that guarantee inter-state responsibility in the area of crime. This interaction is especially important in relation to the enforcement of mechanisms toward criminal liability. That is why, at the international level, it will probably be necessary to establish dedicated regulations and regulators to monitor intelligent systems and their permanent revision in order to ensure compliance with legal standards. For instance, one could recommend the creation of an independent testing committee on autonomous AI technologies like machine learning to assess the impact on society, monitor real-world implementations of AI systems in fields like health care and transportation, and ensure that these systems are compliant with ethical and legal standards (Cath et al., 2018; Gasser and Almeida, 2017).

But effective implementation of criminal responsibility would require not only strong domestic legal systems but also the strengthening of international collaboration. We need systems for sharing information between countries and coordinating investigations into crimes that may be committed by autonomous superintelligent systems. While international conventions like the Budapest Convention already serve a crucial role in encouraging compliance with cybercrime laws between countries, it could be expanded to further include AI-related issues in order to ensure consistency as technology evolves (Council of Europe, 2001; Schmitt, 2020). Nations would have a globally coordinated approach to the fundamental adaptation of existing conventions and treaties around AI and superintelligent systems.

Technologically, sophisticated tracking and digital record-keeping mechanisms will be critical to oversee autonomous intelligent systems. In this regard, blockchain technology may prove to be a particularly useful means of keeping records for every decision made by these systems so that everything is open in real-time. These records could be of significant service in criminal investigations related to AI and superintelligent systems: they could provide traceability as well as clarity concerning what these systems actually did (Tapscott and Tapscott, 2016). This has to be complemented by the development of new judicial mechanisms to deal with non-compliance by such systems. That may include holding the creators or organizations responsible for the actions of the systems they create, or finding ways to limit the operational scope of systems that do not meet legal standards.

More severe cases might require penalties specifically designed to address the criminal responsibility of autonomous systems. These penalties would provide deterrents at the upper end of the scale and would also ensure that autonomous systems do not continue to cause harm after having been found criminally liable. One possible penalty could be the confiscation of property related to those systems, including but not limited to hardware, software, or any other relevant asset. Confiscation might be especially meaningful in instances where the systems are used to conduct illegal activities or when they are considered too dangerous to maintain. That’s similar to human criminal punishment in which the state seizes assets obtained through criminal activities. Damage beyond forfeiture could be another potential punishment by dismantling the system itself. This would mean shutting down and physically destroying the hardware or deleting the software that runs the system. An extreme treatment of the kind may well be warranted for systems regarded as an ongoing risk to the public or to the state, much as dangerous machines or contraband are destroyed (Abbott, 2020).

These penalties also serve the purpose of judicial deterrence, as well as a post-finding of criminal liability, preventing autonomous systems from inflicting additional harm. Although the ability to penalize autonomous systems is novel, they are also highly responsible to the principal who designs and deploys them. For the law to stay in step with fast-developing AI technologies, its frameworks must evolve, ensuring that all those involved — including the AI systems themselves — are answerable for the harm they cause.

9. Conclusion

With the advancement of Artificial Superintelligent system, legal systems face significant challenges in determining the criminal and civil liability of these systems. Current legal frameworks are insufficient to keep up with these rapid developments, as Artificial Super Intelligence may perform complex actions without direct human intervention, complicating the attribution of responsibility. Furthermore, there is a pressing need to develop legal frameworks, that address the criminal liability of parties involved in the development, and the operation of these systems, such as corporations and developers. Multinational corporations, operating across borders, further complicate these issues, as their legal responsibilities span multiple jurisdictions, necessitating a distinct approach, to address the liability of these global entities. These frameworks must also account for individual rights issues, such as privacy, anti-discrimination, and protection of individuals from the effects of ASI-driven decisions.

Regarding international legal frameworks, it is crucial to enhance cooperation between states, to establish uniform legal standards governing the liability for actions that may be committed by ASI. Current international agreements, such as the Budapest Convention, focus on cybercrime but lack provisions addressing ASI-related issues, requiring the development of new treaties, that provide clear details on criminal liability and technologies involved. Moreover, given the speed of technological advancement, future treaties should be adaptable and regularly updated to keep pace with innovations in ASI technology.

In addition, it is essential to develop technological solutions, that support legal frameworks, such as intelligent systems leveraging explainable ASI and blockchain technologies, to ensure transparency in decision-making by smart systems. These solutions will enhance trust in Artificial Super Intelligence, ensuring compliance with existing laws. As ASI systems evolve, it may become necessary to consider direct legal recognition of ASI, as an entity capable of bearing responsibility in specific contexts, especially when their actions transcend human control.

Penalties for Artificial Superintelligence system itself must also be integrated into legal frameworks. This may involve seizing any ASI-related assets, like hardware, software, or data, on rare occasions, destroying the system to stop any future hazards. “Those measures would provide an environment in which AIS could be held criminally responsible, as would the developers and operators, thus serving as a powerful deterrent to future violations and as a method of reinforcing the legal accountability of those that build and manage these innovative new technologies.” This solution would at the same time present a legal system that increasingly catered to the new problems posed by the autonomous nature of AI by exploring the potential for directly punishing the systems themselves.

The challenges posed by ISA require a coordinated international response, to create innovative legal and technological frameworks that address the risks associated with these systems, ensuring justice and the protection of individuals’ fundamental rights. In particular, a balanced approach that integrates international cooperation, legal innovation, and technological solutions will be key to managing the complexities arising from the influence of multinational corporations across various legal jurisdictions and to addressing the unique ethical and legal implications of Artificial Super Intelligence systems.

Acknowledgments: Author of this Article would like to thank the Governance and Policy Design Research Lab (GPDRL) of Prince Sultan University (PSU) for their financial and academic support to conduct this research and publish it in a reputable Journal.

Conflict of interest: The author declares no conflict of interest.

References

Abbott, R. (2020). The Reasonable Robot: Artificial Intelligence and the Law. Cambridge University Press

Abbott, R., & Sarch, A. (2019). Punishing artificial intelligence: Legal fiction or science fiction. UC Davis Law Review, 53, 1-40. Retrieved from https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/53-1_Abbott_Sarch.pdf

Akerkar, R. (2019). Artificial intelligence for business. SpringerBriefs in Business. Springer.

Akpuokwe, C. U., Adeniyi, A. O., & Bakare, S. S. (2024). Legal challenges of artificial intelligence and robotics: A comprehensive review. Journal of Computer Science & IT Research Journal, Volume 5, Issue 3

Alanazi, F., & Alenezi, M. (2024a) . A framework for integrating intelligent transportation systems with smart city infrastructure. EnPress Publisher, LLC. https://doi.org/10.24294/jipd.v8i5.3558

Alanazi, F., & Alenezi, M. (2024b). Driving the future: Leveraging digital transformation for sustainable transportation. EnPress Publisher, LLC. https://doi.org/10.24294/jipd.v8i3.3085

Almheiri, S., Alsaadi, F., & Almazrouei, A. (2024). "AI Governance and Regulation in the UAE." International Journal of AI Law and Ethics

Amuda, Y. J.,& Rahman, SA. (2024). Artificial intelligence for food production among smallholder farmers: Towards achieving sustainable development goals (SDGs) in Nigeria. Creative Publishing House. https://doi.org/10.62754/joe.v4i1.4202

Binns, R. (2018). Legal Frameworks for the Use of Autonomous Systems in Outer Space. Springer

Binns, R. (2021). On the apparent conflict between explainability and fairness in machine learning. Communications of the ACM, 64(7), 62-71.

Bostrom, N. (2014). Superintelligence: Paths, dangers, strategies. Oxford University Press.

Bryson, J. J., Diamantis, M., & Grant, T. (2017). "Of, for, and by the people: The legal lacuna of synthetic persons." AI & Society, 32(3), 521-534.

Calo, R. (2015). "Robotics and the Lessons of Cyberlaw." California Law Review, 103(3), 513-578.

Calo, R. (2019). "Artificial Intelligence and the Law: Challenges and Opportunities." Harvard Journal of Law & Technology

Casey, M., & Walker, C. (2020). Artificial intelligence in healthcare and the law: Regulation, risks, and opportunities. Cambridge University Press.

Cath, C., et al. (2018). Artificial Intelligence and the 'Good Society': The US, EU, and UK Approach. Science and Engineering Ethics, 24(2), 505-528.

Chalmers, R., Liddy, J., & Mason, T. (2023). The legal challenges of autonomous artificial intelligence systems. Oxford Journal of Legal Studies, 44(3), 673–699. https://doi.org/10.1093/ojls/gqad045

Council of Europe. (2021.). Artificial intelligence and criminal law. Retrieved from https://www.coe.int/en/web/cdpc/artificial-intelligence-and-criminal-law

Council of Europe. (2024). Council of Europe Framework Convention on Artificial Intelligence and Human Rights. Retrieved from Council of Europe.

Democratic Arab Center for Strategic, Political, and Economic Studies. (2024). The future of artificial intelligence: Legal and ethical challenges. Retrieved from https://democraticac.de/wp-content/uploads/2024/0

Dignum, V. (2020). Responsibility and artificial intelligence. In M. D. Dubber, F. Pasquale, & S. Das (Eds.), The Oxford handbook of ethics of AI (online edn, 9 July 2020). Oxford Academic. https://doi.org/10.1093/oxfordhb/9780190067397.013.12

Engelke, P. (2020). AI, society, and governance: An introduction. Atlantic Council. Retrieved from http://www.jstor.org/stable/resrep29327

European Commission. (2024). European Union's Artificial Intelligence Act (AI Act). Retrieved from European Commission.

Expert Institute. (2021). "Liability in Medical Technology: A Case Study of the Da Vinci Surgical System." Journal of Health Law & Policy.

Galloway, S., & Armstrong, B. (2018). Space Law and Governance of Autonomous Systems in Outer Space. Cambridge University Press

Gasser, U., & Almeida, V. A. (2017). A Layered Model for AI Governance. IEEE Internet Computing, 21(6), 56-62.

Gless, S., Silverman, R., & Weigend, T. (2016). "Artificial Intelligence and the Future of Law." Journal of Law and Technology, 29(2), 275-310

Guerra, A., Parisi, F., & Pi, D. (2022). Liability for robots I: Legal challenges. Journal of Institutional Economics, 18(3), 331–343. https://doi.org/10.1017/S1744137421000825

Guerra, F., Parisi, G., & Pi, R. (2022). Legal implications of intelligent systems: Challenges and solutions. International Journal of Law and Technology, 15(2), 102-119.

Harris, J., & Jones, L. (2019). Artificial intelligence in medicine: Legal challenges and implications. Journal of Law, Medicine & Ethics, 47(4), 563-574.

Hawking, S., & Musk, E. (2020). Concerns on superintelligent AI and its implications for humanity. Journal of Artificial Intelligence and Ethics, 6(2).

Howell, B. (2024). Regulating artificial intelligence in a world of uncertainty. American Enterprise Institute. Retrieved from http://www.jstor.org/stable/resrep64560

Janssens, L. (2018). A prospect of the future: How autonomous systems may qualify as legal persons. In L. Janssens, E. Bayamlıoğlu, I. Baraliuc, & M. Hildebrandt (Eds.), Being profiled: Cogitas ergo sum: 10 years of profiling the European citizen (pp. 116–121). Amsterdam University Press. https://doi.org/10.2307/j.ctvhrd092.24

Jones, P., & Walker, T. (2023). Ethics and regulation of autonomous systems. Springer Publications.

Kling, L. (2019). Artificial Intelligence and the Law of Outer Space. Space Law Review, 44(2), 202-218

Kubica, M. L. (2022). Autonomous vehicles and liability law. The American Journal of Comparative Law, 70(Supplement_1), i39–i69. https://doi.org/10.1093/ajcl/avac015

Lee, J., & Ang, S. (2022). Artificial Intelligence in Smart Cities: Legal and Ethical Challenges. Journal of Technology and Law, 15(2), 45-67.

Leenes, R., van Brakel, R., & Koops, B. J. (2017). "The Rise of Autonomous Systems and the Law." Artificial Intelligence and the Law: Proceedings of the 8th International Conference on AI and Law.

Lin, P., Abney, K., & Jenkins, R. (Eds.). (2017). Robot ethics 2.0: From autonomous cars to artificial intelligence. Oxford University Press.

Loaiza, D., Birdwell, M., Kennedy, P., & Visser, L. (2019). "Cybersecurity, AI, and the Rule of Law: Who Takes Responsibility?" Journal of Technology & Security Law.

Maastricht University. (2023). Artificial intelligence and criminal responsibility: Emerging legal frameworks. Retrieved from https://www.maastrichtuniversity.nl

Ministry of Industry and Information Technology of the People's Republic of China. (2023). Measures for Managing Generative AI. Retrieved from https://www.miit.gov.cn.

Mittelstadt, B. D. (2023, February 23). Who is liable for AI-driven accidents? The law is still emerging. Centre for International Governance Innovation. Retrieved from https://www.cigionline.org/articles/who-is-liable-for-ai-driven-accidents-the-law-is-still-emerging/

Mnih, V., Kavukcuoglu, K., Silver, D., Riedmiller, M., & Hassabis, D. (2015). Human-level control through deep reinforcement learning. Nature, 518(7540), 529-533. https://doi.org/10.1038/nature14236

Nyholm, S. (2018). The ethics of crashes with self-driving cars: A roadmap. Philosophy Compass, 13(e12507). https://doi.org/10.1111/phc3.12507

Oxford University Press. (2024). Artificial intelligence and the law: Analyzing legal accountability for autonomous systems. Retrieved from https://academic.oup.com

Pagallo, U. (2013). "The Laws of Robots: Crimes, Contracts, and Torts." Springer.

Patil, M., & Rao, M. (2019). Studying the contribution of machine learning and artificial intelligence in the interface design of e-commerce site. In S. Satapathy, V. Bhateja, & S. Das (Eds.), Smart Intelligent Computing and Applications (Vol. 105). Springer.

Roland Berger. (2020). Scale-up Europe: How to build world-class European startups. Roland Berger. Retrieved from https://www.rolandberger.com

Roland Berger. (2024). AI Innovation in the European Union: Regulatory Challenges and Market Impact. Roland Berger Strategy Consultants

Rubinstein, D. (2022). Criminal liability for AI-caused harm: Mens Rea and beyond. British Journal of Criminology, 62(1), 257–273. https://doi.org/10.1093/bjc/azab017

Russell, S., & Norvig, P. (2020). Artificial intelligence: A modern approach (4th ed.). Pearson.

Schmitt, M. N. (2020). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press

Smith, A. Jr. (2019). Biopolitics: Look in the lost and found for peace of mind. Springer US.

Smith, H. (2022). The Economic Impact of Over-Regulation on AI Startups in Europe. European Innovation Review, 45(1), 78-92

Stanford Law School. (2018). Automated vehicles: Legal and regulatory challenges (SSRN version). Stanford Law School. Retrieved from https://law.stanford.edu/wp-content/uploads/2018/04/automated-vehicles-article-SSRN-version-pdf-3-28-18.pdf

Stanford Law School. (2018). Legal accountability in autonomous systems: A study of manufacturer and operator liability. Stanford Journal of Law and Technology, 22(2), 156-173.

Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Portfolio Penguin.

Thrun, S. (2019). Artificial intelligence for robotics: Build intelligent robots that perform human tasks using machine learning and probabilistic reasoning. O'Reilly Media

U.S. Department of Justice. (2023). Computer Fraud and Abuse Act (CFAA) and its Applicability to Autonomous Systems. Retrieved from https://www.justice.gov

United Nations Office for Outer Space Affairs. (1967). The Outer Space Treaty. Retrieved from https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html

Viscusi, W. (2021). The Future of Autonomous Systems in Space: Legal and Ethical Considerations. Journal of Space Law, 49(1), 112-130

Vogt, B., & von dem Bussche, A. (2017). General data protection regulation (GDPR): A practical guide. Springer.

Vogt, L., & von dem Bussche, A. (2017). The GDPR and the European Digital Economy: Balancing Innovation and Privacy. European Business Law Review, 28(3), 389-410

World Intellectual Property Organization. (2020). Artificial intelligence: A WIPO conversation. WIPO Secretariat. Retrieved from https://www.wipo.int/meetings/en/details.jsp?meeting_id=12345

Wright, M. (2020). Artificial Intelligence and the Legal System: Challenges in the Space Context. Routledge

Yaghi, R. (2024), Corporate governance codes: A controversial efficiency? EnPress Publisher, LLC. https://doi.org/10.24294/jipd.v8i7.4359

Zhang, W. (2022). China's data security laws and AI regulations: A comprehensive review. International Journal of Artificial Intelligence Law, 8(2), 114-136

Zhang, W. (2023). AI Regulation in China: Opportunities and Challenges. Journal of Asian Legal Studies, 29(4), 211-227.