Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

ISSN: 2584-0142
PSYCHOPEDIA JOURNALS
International Journal of Interdisciplinary Approaches in Psychology (IJIAP)

Victims of Artificial Intelligence: Perspective on Criminal and Civil Liability

[1]**Shristi Singh**, *Department of Biosciences, Graphic Era (Deemed to be University), Dehradun*

[2]**Divyansh Kumar**, *Department of Biosciences, Graphic Era (Deemed to be University), Dehradun*

[3]**Ashmit Guleria**, *Department of Biosciences, Graphic Era (Deemed to be University), Dehradun*

[4]**Gandhik Sai**, *Department of Biotechnology, Invertis University, Bareilly*

[5]**Satyam Srivastav**, *Department of Biotechnology, Invertis University, Bareilly*

[6]**Priyanka Soni**, *Nims School of Forensic Sciences, Nims University Rajasthan, Jaipur*

[7]**KM Shruti**, *Department of Forensic Science, Adamas University, Kolkata*

[8]**Rajat Singh**, *Department of Forensic Science, Adamas University, Kolkata*

rajatsinghresearch@gmail.com

Abstract: The possibility of unforeseen consequences and harm to people known as AI victims has grown in importance as artificial intelligence continues to permeate various industries. The complicated terrain of criminal and civil liability with regard to victims impacted by AI systems is critically examined in this article. In the wake of unfavourable AI-related incidents, the article offers a comprehensive examination of the difficulties and moral issues surrounding the accountability of AI developers, operators, and stakeholders. It delves into case studies and real-world instances where individuals have suffered harm due to AI failures, biases, or unintended consequences. By analyzing these scenarios, the chapter seeks to highlight the varied nature of AI-related victimhood and the need for a nuanced legal structure to deal with the diverse forms of harm inflicted. Moving on, the article additionally explores the evolving legal landscape surrounding criminal liability in AI incidents. It investigates the role of negligence, intent, and corporate responsibility in determining criminal

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

culpability. Furthermore, it scrutinizes emerging legal precedents and the difficulties in identifying criminal intent with AI systems or their human operators. The subsequent section shifts the focus to civil liability, emphasizing the complexities of seeking compensation for AI-related harm through legal channels. Discussions cover issues of foreseeability, duty of care, and the establishment of causation, underscoring the challenges faced by victims seeking recourse in civil courts. Nonetheless, the article discusses the possible legislative and regulatory frameworks that could ensure accountability in the development and implementation of AI technology. It discusses the initiatives being taken to develop guidelines for ethical use of AI technology, such as the incorporation of ethical values into legal frameworks. This chapter is a valuable resource for legal professionals, policymakers, and scholars grappling with the complex issues of victimhood in relation to AI technology. The opinions presented in this chapter add to the continuing discussion on the creation of efficient legal frameworks that strike a balance between innovation and the defence of those who endure the unforeseen repercussions of artificial intelligence.

Keywords: *AI; AI-Victim; Forensic; Legal Analyses*

1. Introduction

John McCarthy in his analysis on Dartmouth Summer Research Paper (1956), first moulded the term Artificial Intelligence (AI). Although his research didn't mention the high-tech purpose of AI, hence defining it as "in ways that would be called intelligent if a human were so behaving." Considering technology as the factor, the definition further refers to "technology that is able to function appropriately with foresight of its environment". AI was also defined by the Government Office of Science UK as "the analysis of data to model some aspect of the world. Inferences from these models are then used to predict and anticipate possible future events." The computer follows the step-by-step instruction to perform a particular task and creates the statistical model (Walz, 2019). One of the 21st century's cutting-edge technologies, AI is reshaping industries and fundamentally altering the manner in which individuals communicate, work, and live. From its early beginnings to the complex systems that exist today, artificial intelligence has advanced significantly and has also shown considerable progress in sectors like computer vision, natural language processing (NLP), reinforcement learning, deep learning, and generative adversarial learning (Jiarawattanakul, 2023).

Advances in computer vision can be attributed to AI's capacity to analyse visual data. These days, these technologies are utilised in image analysis for medicine, self-driving vehicles, and

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

facial recognition, among other applications that improve safety and efficiency in our daily lives. AI systems can now comprehend and communicate with human language through the use of NLP. This discovery facilitated the development of chatbots and virtual assistants like Siri. Reinforcement learning is a distinct area of AI that has eventually made great progress. Because of this, machines can now learn from their activities in an environment and use that knowledge to play sophisticated games, allocate resources optimally, and even command robots. The potential of GANs, a particular kind of neural network, to produce realistic content such as text, photos, and videos has garnered an abundance of fascination. They work in creative industries including entertainment, design, and the arts (Jiarawattanakul, 2023).

1.1 *History of Artificial Intelligence*

From 1931 to date, the field of artificial intelligence has been significantly impacted by computer science (CS). The first electronic computer, called the Electronic Numerical Integrator and Computer (ENIC), was built during World War II and resulted in the creation of AI designed for particular uses. The development of AI in America, Britain, and several European countries during the 1960s and 1970s. The DENDRAL program, a pattern area for AI, emerged in the 1960s and early 1970s. In the 2000s, IBM's Deep Blue supercomputer transformed nanotechnology and computer science, leading to sovereign cars, latest robotics and emotional robots.

1.2 *Current condition of AI*

There have been major technical improvements in AI in recent years, especially in the use of ML and deep learning (DL) methods (Llorca et al., 2023). Natural Language Processing (NLP) has recently focused on improvements in AI analysis and mechanism. Many companies, such as Google, Facebook, and IBM, have been involved in the research and development of AI. AI has already been applied in space exploration, computer language understanding, and the design of human learning models. AI has now entered all activities and has become a major aspect of life. Some tasks are automated, while others remain unchanged.

1.3 *Impact of AI on society*

AI systems contain the tendency to deliver benefits and opportunities for our societies as a whole by developing and modifying items and offerings throughout many different application fields (Llorca et at., 2023). Social Impact of an AI is characterised to be strongly affected by information, including from the industry in which it originated for applications, and context in which it is used. In the last decades, numerous predictions have been made on AI and its impact on society. AI has enormous potential for enhancing the comprehension of the world but can also be harmful if used improperly or without proper assessment. AI offers the

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

opportunity to enhance the lives of individuals, enhance the society's ability to resolve problems and advance morality and solidarity. AI is used to boost medical results by discovering drugs, improving healthcare, and advancing in education.

1.4 *AI Victims*

An "AI victim" is an individual who experiences damage as a consequence of engaging in AI technologies. Listed here represent few instances in which AI could unfavourably impact individuals:

a) ***Segregation and Unfairness*:** By permitting the data that was given to instruct them to propagate, AI systems possess a tendency to prejudice against or perpetrate actions of unfairness against specific populations of individuals.

b) ***Privacy Violation*:** The application of AI has the ability to breach the privacy of individuals by collecting and evaluating sensitive data with no consent.

c) ***Functions:*** Individuals in multiple sectors could potentially lose their positions as a result of intelligence-based technologies which could possibly result in financial strain and unemployment.

d) ***Deception and Tampering:*** Programmes based on AI possess the potential to propagate inaccurate data, influence public perception and impact the way individuals act and think.

e) ***Monitoring and command*:** AI monitoring methods possess a tendency to adversely impact the rights of individuals to confidentiality and independence, consequently contributing to enhanced enforcement and oversight of their behaviour (Socatiyanurak et al., 2021).

1.5 *Rights of victims of AI*

Individuals that might have been harmed through AI systems are now realising the fact that they ought to be given privileges, identical to what victims of conventional offences acquire. Such rights may take the form of:

a) ***Right to Disclosure*:** For the purpose to assure equity and reliability, AI platform's methods for making conclusions ought to remain observable and accessible.

b) ***Right to Description:*** Persons whose lives are influenced by AI judgements need to be provided with enough knowledge to figure out the techniques and reason associated with those findings.

c) ***Right to privacy and data protection*:** Individuals ought to possess the legal right to confidentiality and safeguard their data as AI algorithms often depend on tremendous amounts of information about individuals.

d) ***Ethical challenges*****:** Addressing AI and its influence on citizens, there are numerous ethical challenges along with constitutional rights. Making certain that AI technologies are developed and implemented in an approach that supports freedom, respect, and fundamental rights is essential (Wemmers et al., 2012).

1.6 *AI-related Incidents*

The problems of safety, ethics, security and privacy continue to influence AI (Nasim et al., 2022). Instances associated with AI could be categorised into multiple groups. Authenticity crimes, unpredictable AI outcomes, trading via algorithm, phishing, fake information, and security breaches are aspects of harmful use of AI systems (Härkänen et al., 2021). Instances autonomous machines, who lack a common record of their errors are different types. These instances illustrate the importance of an AI Incident Database for gathering and analysing real errors with the aim to enhance security (McGregor et al., 2020; Blauth et al., 2022).

1.7 *Criminal incidents*

Criminal circumstances concerning AI have arisen due to the harmful utilisation and abuse of the abilities of AI. Security incidents, unpredictable AI results, algorithms for trading membership inference crimes, phishing, fake information, malware, and autonomous weapon systems are few referrals of these circumstances (Blauth et al., 2022). There have been situations where AI has been proved harmful, such as an AI robot in a motorbike factory killing a worker (Hallevy et al., 2010). The legal system encounters problems as a consequence of an increase in crime associated with AI. The government has to judge whether the rules currently established are sufficient to deal with these crimes (Al Qatawneh et al., 2023).

1.7.1 Hacking and cybercrimes

Hackers utilize technology to obtain information, perform fraud or lead to harm. The word “Cybercrime” indicates a broad range of crimes linked to the cyber world. It comprises Hacking, Phishing, Malware, cyber stalking, and identity theft. They are not limited to criminal acts performed by devices such as computers (Chakraborty et al., 2023). The legal framework has faced challenges as a result of an elevation in crimes linked to AI and the emergence of risks that are facilitated by AI(Al Qatawneh et al., 2023).The legal system has encountered problems as an outcome of an escalation in AI-related crimes and the rise of risks that are enabled by AI (Al Qatawneh et al., 2023). AI is utilised by organisations more frequently as their initial phase of protection against cybercrime as it can recognise new incidents quicker than individuals. Hackers may nevertheless take advantage of flaws in AI systems, including data manipulation crimes, and spread of incorrect data (Mahmud et al., 2021).

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

1.7.2 Autonomous vehicle accidents

AI associated instances affecting autonomous vehicles raise challenging issues of ethics and faith. Analysis demonstrates the fact that human operators and autonomous systems (self-driving vehicles) assigned distinct responsibilities including the latter commonly considered more responsible for almost the same activities and its effects (Zhang et al., 2021). An analytical agent-based accident identification system featuring smart accident warnings and protection abilities have been offered to deal with the increasing frequency of automobile crashes globally. The system makes applications for AI to improve rescue team synchronisation as well as rapid response speed (More et al., 2023). The requirement for precise regulation and legal structures has been emphasised through legal issues in events concerning Unmanned Aerial Vehicles (UAVs) and AI that point out the obstacles in providing accountability amongst the programmers, administrators and third parties (Shirokova et al., 2022). AI continues to develop healthcare diagnosis and autonomous systems which propose new dangers. In order to enhance security and management in these emerging fields careful examination of lapses must be done (Poon et al., 2019; Macrae et al., 2022).

1.7.3 AI-generated fraud and scams

AI is being effectively utilised to tackle crimes and thefts. One technique is for recognising adverse calls as well as prospective indications of scams with precision by making use of AI and ML algorithms to identify and analyse illegal conversation by phone (Malhotra et al., 2023). Likewise, AI, specifically ChatGPT, has been utilised to deceive criminals towards spending precious and resources on fictional transactions, illustrating AI’s efficiency in preventing mail-borne risks (Cambiaso et al., 2023). In addition, it has been recommended to utilise Generative Adversarial Networks (GANs) to replicate fake activity trends. By recording different fake transaction trends adjacent to class borders, GANs enhance the identification of fraud and enhance the effectiveness of classifiers (Pandey et al., 2022).

1.8 *Civil incidents*

Responsibilities of damage generated by (AI) technologies is an area of dispute in Civil Incidents concerning AI. As the European Commission's supervision measures make obvious, the advancement of AI presents issues concerning the obligation of numerous stakeholders that contribute to the “Value Chain” of AI technologies (Bonna et al., 2021). Analysis indicates the importance of determining every aspect of civil responsibilities regarding damage that results from, reviewing policies, and global standards (D'Alfonso et al., 2022). Based on the analysis, there have been constant disputes regarding the duties of AI developers and users, and there are proposals for authorities that recognise AI as an indicator of higher risk (Martsenko et al.,

2022). Although there is compact danger for commercial airliners through AI incidents, there have been reported animal occurrences, majority of them occur at night during aircraft landing and show particular types of cooperation (Kharitonova et al., 2022).

1.8.1 Privacy violations

There are numerous types of privacy violation including the risks of data disclosure in applications for mobile devices to interpersonal distance violation in everyday interactions (Luo et al., 2021). When observed through situations involving tech-facilitated privacy violation in real life situations, technology contributes an essential role of rendering privacy violation accessible (Windl et al., 2023). Issues surrounding ethical breaches and privacy violations are growing throughout the development of AI. Recommendations for securing the private details have been established through data protection laws such as the Central Consumer Protection Act (CCPA) and General Data Protection Regulation (GDPR), nonetheless specific guidelines could vary beyond these standards (Kaur et al., 2022). Since there is boundary instability that results from voice-activated gadgets, invasion of privacy that led to distant responses have been identified from interview-based research on AI application (Alshamsan et al., 2022). The effect of AI affecting citizen's privacy causes major concern, and challenges about ensuring privacy while using AI technology must be resolved (Walters et al., 2021).

1.8.2 Discrimination and bias in AI algorithms

There are numerous instances in which discrimination due to algorithms could show up, like feature-selective discrimination, connective discrimination, and pricing discrimination assisted through large amounts of data, each of which may result in adverse impact (Laacke et al., 2023). The AI technology errors contain the tendency to develop gradually, affecting public opinions and occasionally causing injustice (Leavy et al., 2020). Since this could influence individuals in everyday instances including loan acceptance, it has become essential to ensure that certain AI technologies refrain from discriminating on the basis of important attributes (Pappada et al., 2022). Imbalance and discrimination might be maintained by unknowingly collecting societal discrimination within the information that is utilised for training AI computer programs (Shin et al., 2023). Harmful judgements for decision making via algorithms remained an unresolved challenge since they may additionally result in unequal assessment and adverse impact on application of AI (Tao et al., 2022).

1.8.3 AI-related employment issues

The worldwide employment landscape is experiencing shifts as AI technologies grow more widespread. The rapid development in AI applications has resulted in higher requirements

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

for advanced technical abilities in AI, which often surpasses the total number of vacant positions (Krassadaki et al., 2023). Although AI offers the possibility of substitute hiring using smart machines (robots) and programmes and enhancing productivity, it additionally creates difficulties (Rickardo et al., 2023). The alteration throughout the character of employment caused through incorporation of AI generates discussion regarding the benefit and challenges of AI and ML (robots) throughout the working environments, which will certainly influence employment opportunities in the years to come (Ivanova et al., 2022). Additionally, the increasing utilisation of AI in the position of management is transforming organisations and raising discussions regarding the private nature of AI as an employer as well as its authority among individuals (Stefański et al., 2022). Policy considerations raise the spotlight to the fact that invading AI tools can be in work employment and the significance of particular laws for protecting the rights of employees as AI progresses (Ponce et al., 2021).

2. Legal Framework

AI-specific legislation and regulations are currently developing and vary greatly between states. Nonetheless, there are a few crucial areas where rules and regulations frequently come into proximity to AI:

2.1 *Data protection laws*

The compilation of laws and regulations which regulate the collection, utilisation, preserving, and revealing of sensitive information are referred to as Data Protection Laws. The guidelines have the goal to preserve the confidentiality of individuals and make sure that organisations manage the sensitive data appropriately. Privacy laws usually specify the rights and privileges individuals have when it comes to their private information, the duties of enterprises that gather and manage information, and the penalties for disobedience. For the purpose to assure that the liberties and security of those who are impacted by AI platforms be acknowledged, laws governing data protection that applies to AI victims are required. Rules are required when AI algorithms are utilised for making assessments which impact a particular individual with the goal to avoid any potential damage (Agarwal et al., 2012).

2.2 *Cybersecurity regulations*

The rapidly evolving field of cybersecurity regulation is complicated and ever-changing, encompassing multiple parties and divisions of administration, which leads to a situation of legal uncertainty (Siboni et al., 2019). Numerous strategies are currently established into effect by a lot of nations, namely the UK, US, France, Germany, and the EU, for dealing with cybersecurity risks within the business-civilian sector (Heim et al., 2023).

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

Considering the present structure without an agency with specialisation having complete administrative and investigative influence, there is an acknowledged demand for a comprehensive approach to cybersecurity rules in the United States (Plachkinova et al., 2022). Moreover, the development of security threats such as warfare and espionage has drawn focus toward the requirement of modifying laws and regulations in order to tackle emerging technologies and challenges all over the world (Streich et al., 2022). In order to adequately tackle cybercrime and strengthen national security, administrators have to understand the manner in which cybersecurity laws and regulation have evolved in the past and identify trends and vulnerabilities (Greiman et al., 2022).

2.3 *Product liability laws*

The responsibility for assuring the security of goods launched onto the trade has been placed through product liability law on producers, suppliers, vendors, as well as other parties that matter. Planning, generation, and sales problems constitute some of the challenges it addresses. A claim for Product Liability is sometimes conducted by an individual which suffers damage with the shortcoming of a good with the objective to obtain compensation for destruction. By enforcing responsibility from every stakeholder involved in the manufacturing process and distribution network, these laws attempt to secure or protect customers towards harmful goods (Panchbhai et al., 2022). With the objective to strengthen the safety of consumers in India, the proposed Consumer Protection Act of 2019 put in an assortment of significant changes. Some of the aspects addressed by the article are:

a) **Principle of "Unfair Contract":** It is developed with the objective of protecting consumers from commitments that might be adverse (unpleasant) or harmful towards consumers.
b) **Settlements of conflicts:** It was developed for negotiation as an avenue of mediating conflicts between consumers, presenting more efficient and affordable choice than prolonged court proceedings.
c) **Development of the Central Protection Agency:** The Central Protection Agency was founded through legislation to enhance the implementation of the rights of consumers through the power to inquire into allegations received by consumers and impose orders requiring them to cease operations.

The above features are the indication of the attempts made by the government to enhance the laws governing consumer protection in the country and offering consumers more avenues for solving problems and assuring equal consideration throughout the retail sector (Panchbhai et al., 2022).

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

2.4 *Anti-discrimination laws*

Anti-discrimination laws serve as vital for preventing disparity and securing those who are excluded. These rules alter the accordance with development in society (Slootmaeckers et al., 2023), and they are required for safeguarding human rights and equality treatment (Sumodiningrat et al., 2022). They confront numerous kinds of biases depending on gender, colour, race and religion with adjustments based on political and historical instances. According to studies, the enactment of discrimination laws has an impact on monetary choices and business viability, particularly with regard to the ratio of debt along with operational efficiency (Greene et al., 2022). Likewise, research demonstrates how different anti-discrimination laws might impact discrimination based on gender on financial funding, underlining the importance for legal methods that reduce the bias and preserve revenue (Kelley et al., 2022).

3. Gaps and Challenges in the Current Legal Framework

To successfully regulate the creation, application, and utilisation of AI technology, a number of loopholes and difficulties in the present legal framework around AI must be addressed. Among these shortcomings, some includes:

3.1 *Inadequacy in addressing AI-specific issues*

a) **Deficiency of Guidelines:** Even though the prospective consequences of (AI) on work settings have been highlighted, currently there aren't appropriate regulations and legislations to deal with the situation and establish adequate safety measures and instruction (Rodrigues et al., 2022).

b) **Utilisation of civil right framework to trademark administration:** However beneficial civil framework might possess shortcomings which make it necessary for revising their constraints on the management of the protection of trademark property. Although the positive aspect of this structure, problems including disrespect and conflicts with regard to the rule linger in certain locations (nation), and they have a direct effect on the significance of societal regulations in the factors of AI software (Bakiner et al., 2023).

c) **Difficulties concerning Confidentiality and Information Safeguarding:** Offers severe security and protection of information issues which includes those connected to consent with authorization, monitoring, and the breach of information security privileges, as reported by legal authority and information security entities (Rodrigues et al., 2020).

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

d) **Shortage of Computational Visibility:** With regards to, the shortage of computational visibility (Algorithmic Transparency) is an important issue with adverse repercussions for democracy and justice (Rodrigues et al., 2020).

e) **Distinctive issues caused by AI:** Its development creates distinctive issues that the present state of rights of humanity can't handle. These issues involve factors including national and international disparities, the destruction of the results from data-driven industries, or the demand for greater engagement with intellectual debate for the purpose to appreciate and minimise the adverse consequences of expertise (Bakiner et al., 2023).

3.2 *Difficulty in attributing responsibility in autonomous systems*

The complexity of allocating culpability in self-regulating (autonomous) systems highlights the significance it is for preserving adequate human oversight for the purpose to rectify social or moral challenges and uphold responsibility while working through such technological advances (Santoni de Sio et al., 2018). Given that autonomous systems are complicated and consist of multiple associates, distributing duty creates an assortment of challenges. Several of the issues that arise comprises of:

3.2.1 Unanticipated Performance:

Given that autonomous machinery depends on computations and data mining, they are particularly vulnerable to unanticipated performance. Typical instances of such machines comprise autonomous vehicles and powered by AI machines. It could be tricky to identify the reason of any unfavourable happening due to its variability (Grimm et al., 2017).

3.2.2 Insufficient Monitoring:

During unpredictable and immediate circumstances, associates might possess no control regarding the choices and actions implemented by self-sufficient systems. Being out of immediate oversight causes it to be tougher to determine fault whenever errors or damage arise (Grimm et al., 2017).

3.2.3 Intricate chain of distribution:

The establishment and execution of autonomous machinery consist of an intricate chain of distribution comprising numerous associates, involving programmers, shoppers, consumers, and officials. It could possibly be complicated to figure out whomever is accountable for which issue in this intricate network of associates (Grimm et al., 2017).

3.2.4 Regulatory Structures:

The issues that arise with autonomous systems could prevent them from being properly tackled through present-day legislative structures. Independent systems possess a distributed

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

process of making resolution and complexity in technologies which could prove challenging to standard fault-based methods, including carelessness, to be held responsible (Grimm et al., 2017).

3.2.5 Interaction and Instruction:

Insufficient data regarding the responsibility and restrictions of self-governing structure may end up resulting in error of judgement, incomprehension, and disagreement within individuals caused by insufficient interactions, understanding, and instruction. The absence of common comprehension could render determining accountability substantially more complicated (Grimm et al., 2017).

3.2.6 Monitoring and Verification:

This is necessary to implement rigorous monitoring and verification techniques in order to ensure the reliability as well as security of systems that are autonomous. Nevertheless, it could be challenging to pinpoint fault for tragedies or failures when inspection processes go bad or verification processes are inadequate (Grimm et al., 2017).

The issues mentioned above emphasise the crucial importance of an exhaustive structure that successfully confronts the intricate problems of accountability allocation of self-learning system, specifically in consideration of a constant advancements in AI systems and how they are gaining information throughout various sectors (Coeckelbergh et al., 2020).

4. Criminal Liabilities

4.5 *Challenges in prosecuting AI-related crimes*

AI can work in a way that can be considered as “criminal” by society. Prosecuting AI-related crimes is a very challenging task in determining criminal liabilities for AI sections (Khisamova & Begishev, 2019). The legal explanation of AI and the extent of involvement in criminal activities increase complex issues regarding accountability. Questions arise about the criminal liabilities of AI systems (Singh et al., 2025; Gautam et al., 2025). users and designers, as well as the need for a new legal personality for AI responsible for their system’s actions. Some argue for granting AI an “electronic legal personality” to maintain its accountability for its actions independently (Dimitrova, 2022). Additionally, the self-learning and self-developing capabilities of AI complicate the assessment of its criminal liability. Despite these complexities, there are calls for legislative measures to address AI crime effectively.

4.5.1 Attribution issues

Attribution of criminal liabilities involves issues such as determining who should be held responsible for the legal or illegal acts carried out by AI systems. Issues of attribution in

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

Criminal liabilities are very significant and serious. AI is complex due to the autonomous nature of AI and its difficulty in making the coordination of both the system and its creators accountable. (Vojtuš et al., 2022). The current legal systems overcome the gaps in address involving g AI- related crime and have difficulty in attributing criminal liability to AI due to the absence of the conventional means in these systems. Many researchers have proposed several legal models to overcome these problems or issues, stressing the need for a revaluation of the conceptualization of AI in the legal system. Examining the applicability of different legal models, for instance Hallevy et al. (2010), and examining how the current criminal laws can be extended to include the accountability of AI (Dimitrova, 2022).

4.5.2 Difficulty in defining criminal intent in AI systems

Defining Criminal intent in AI systems for criminal liabilities carry a remarkable challenge due to the unique nature of AI. The ongoing legal framework faces difficulty to address the accountability of AI for criminal acts (Kamalova, 2020). Some proposed that AI could be held liable if it independently formulates algorithms and increases the chance of harmful consequences. However, determining the responsibility of criminal acts by AI programmers, makes, and users is also a complicated issue (Saud, 2024) The concept of "malicious intent" in AI systems raises questions about human behaviour or entity. Traditional criminal law faces on ground difficulties in adapting to the complexities of AI, showing the requirement of further research and potential adjustment in legal frameworks.

5. Proposed legal solution

In the realm of AI, the problem of criminal liabilities for all the damages and losses that happen because of AI entities is a pressing concern. Various legal models have been proposed to solve this, including the three models discussed by Hallevy et al. (2010). One prevalent advice is the proper implication of a strict liabilities regime for the producer of AI or other concerning authority, including AI itself. However, attributing legal culpability of AI systems poses challenges, especially in establishing a causative link between Ai action and damages. Despite the rapid development in AI, current legal frameworks often place the burden of liability on users rather than AI itself.

5.1 *Establishing clear liability for AI developer*

Because of the autonomous nature of AI systems, fixing the liability of AI developers is one of the most difficult tasks in cases involving crimes related to AI. Fixing the liability of AI developers in criminal cases is a very necessary legal solution to address the liability gap in cases where victims are harmed by AI systems. The current legal debate on AI liability

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

emphasizes the need for changes to ascertain that developers are accountable for the actions of their creations. According to McCauley (2007), generally, AI is designed using three laws of robotics proposed by Isaac Asimov. These robots are prohibited from doing any harm to humans either directly or by not taking action to protect humans from any type of harm. Robots will obey all human orders, as long as the order does not conflict with the first law. The robot must do everything possible to guarantee its own safety, if it does not conflict with the first and second laws.

5.2 *Creating specialised courts or tribunals for AI-related crimes*

As victims of AI increase with time establishing specialised courts or tribunals for AI-related crime are very important in the legal field. These specialised courts help to solve many complex challenges proposed during the time of prosecuting AI related crime in normal courts. There are some key reasons for establishing a specialized court as discussed by Nerantzi & Sartor (2024). These include:

a) **Requirement of special court or tribunal:** Given the complexity of AI- driven crimes and the evolving legal landscape surrounding them, there is a growing recognition of the need for specialized courts or tribunals dedicated to handling AI- related cases with more efficiency.

b) **Legal framework:** These courts could play a very crucial role in developing a specific legal framework to mark the nuances of AI-related crime, it also ensures that victims get justice against AI-related crimes.

c) **Expertise:** Judges, prosecutors, and legal professionals appointed for these special courts or tribunal must have expertise in AI technology and its implications in criminal law. This knowledge is very crucial for prosecuting AI related crime in court of law.

d) **Transparency and accountability:** These courts might enhance transparency and accountability in adjudicating AI-related cases, ensuring that decisions are based on a deep understanding of the technology and its implications for criminal liabilities.

Criminal liabilities about the use of AI explores the complexities of assigning legal responsibility for criminal activities involving AI technology. It emphasises the necessity for specialised legal frameworks and courts to annotate AI- related crimes effectively.

6. Civil Liabilities

Privacy concerns in the context of AI are multifaceted and require a comprehensive approach that considers data protection, algorithm fairness, transparency and regulatory oversight. As AI develops very rapidly, data security is an integral part of civil liabilities.

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

6.1 *Invasion of privacy through AI surveillance*

AI surveillance is very common nowadays. As AI grows with the time, it is challenging to secure personal and organisation privacy. Sometimes AI surveillance is used for invasion of privacy, as hackers have a chance to get personal information of individuals without their consent. This may involve different types of personal information such as private photos, bank account details, personal conversation with their colleagues etc. Over a few decades AI surveillance has been used in organisations. In the era of highly advanced AI, management has technology that allows for the monitoring of employees in new and different ways. Management has access to monitoring web- browser, email and keystrokes etc of employees. AI also used to get biometric data of individuals. In cases of invasion of privacy through AI surveillance, establishing civil liabilities can be very complex due to the evolving nature of AI technology. Current fault-based liability regimes may need to accept to overcome the challenges caused by AI's characteristics like lack of causality and continuous learning capability (law of governance and technology series). The concept of liability for AI action changes from time to time, with fault based, faultless, and risk-based approaches being considered (Zech, 2021). The addition of several stakeholders in the AI system further complicates liability allocation, necessity enhanced duties of care and shared liability among tortfeasors. To protect victims from harm, it is important to change existing laws governing how parties prove their cases against AI, so there is equal access to courts and defendants can establish a minimum level of security for victims. Also, it is essential that a legal framework specifically designed for AI technologies be implemented so that there is a method for addressing violations of the right to privacy and to hold those responsible for any violations committed through use of AI technologies (Zech, 2021).

6.2 *Unauthorised use of personal data by AI systems*

Incidents like data breach and unauthorised use of data are very common. Unauthorised use of personal data by AI systems and data breach is illegal. Data breach is a broader form of compromise which involves stealing of data. While unauthorised use of data is comparatively less serious as it involves getting access to personal data without any permission. Individuals who get access to data might be outsiders or even an authorised user. Many organisations around the world are concerned about data security because of the advancement of AI (Zhang et al., 2021). These companies are now focusing on data security. When individuals are harmed by the unauthorized use of their personal data by AI systems, civil liability becomes an important mechanism of protection and compensation. The very nature of AI lack of causality, opacity, and unpredictability makes it difficult to establish causality, which requires a relook

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

at liability rules to make it easier to prove liability on the part of the plaintiff. The issue of legal liability for AI systems is complex and involves issues of fault, standard of conduct, and connecting the actions of AI systems to the damage suffered. Moreover, the allocation of damage suffered by AI systems under the current tort law in the EU and US is also being researched to identify the gaps in protecting those who are harmed.

7. Discrimination and bias in AI

Victims of discrimination and bias in the AI system may suffer from challenges in seeking compensation due to the complexities of determining liabilities in AI- related disputes. The existing EU liability framework is deemed inadequate to ensure proper compensation for harm inflicted by AI, necessitating amendments to provide greater protection for injured parties (Sipior et al., 2023).

7.1 *Impact on marginalised communities*

Discrimination and bias in the AI system have a huge impact on marginalised communities, intensifying the living inequality and perpetuating discrimination. Some key points explain it in detail.

a) Racial Disparities

There are several marginalized racial groups, such black and hispanic communities, that are generally excessively affected by biassed AI. Discriminatory AI in various domains can worsen existing racial disparities, from education to law enforcement.

b) Gender disparities

It particularly affects women and gender diverse individuals. For example, when AI is used to hire employees for any job and others via biassed AI may favour male or women applicants over other applicants. Limited career opportunities for women can enhance gender wage gaps.

c) Socioeconomic Inequities

Biased AI and discrimination AI can reinforce socioeconomic disparities by discriminating between rich and poor people based on their economic background, hindering their access to opportunities, resources and services.

d) Vulnerable Inequities

Vulnerable populations, including the elderly and individuals with disabilities, may have different challenges due to bias or discriminating AI. For example- If AI used to manage a health care centre that exhibits age bias, elderly patients may receive suboptimal care or be denied access to certain medical facilities for some specific disease.

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

e) Privacy and data exploitation

Marginalised communities are generally disproportionately impacted by privacy violations resulting from biassed AI (Soni et al., 2023; Singh et al., 2022). Access to private data through biassed AI can affect more individuals with limited resources to protect their private data.

7.2 ***Legal avenues for victims of AI bias***

Legal avenues for victims of AI are necessary to secure liability and seek redress for any harm caused by discriminatory AI systems. Some potential legal avenues for victims of AI by Oh (2023) include: Anti- discrimination laws, Current anti- discrimination laws are not able to overcome the issue of discrimination through biassed AI on the basis of race, gender or disabilities. Victims may pursue legal action under law that prohibits discrimination in various contexts, including employment, housing and public services. Data protection regulation that every individual has the right regarding the processing of their personal data under data protection laws, such as the general data protection regulation (GDPR) in the European union. Individuals who are victims of privacy violation by biassed AI systems may have legal recourse under data protection regulation. Those who are suffering from discrimination civil rights law ensure equal treatment under the law. Victims of AI bias that infringes upon their civil rights may seek legal remedies through civil rights litigation. In case, a group of individuals in a similar manner by bias AI, victims can follow class action lawsuits. This allows multiple victims to collectively seek compensation and hold the responsible parties accountable for the harm caused by a biassed AI system. By using relevant regulatory bodies responsible for overseeing AI technologies and data practices victims of AI bias can file complaints. Regulatory agencies may investigate complaints, enforce compliance with existing regulations and impose penalties on entities found to be engaging in discriminatory AI practices.

7.3 ***Employment-related issues***

In cases when harm is caused by AI in an employment- related context, determining civil liability can be complex and very challenging. The existing EU liability framework may not adequately compensate injured parties for AI related damages, highlighting the need for amendment to ensure proper protection for claimants. Some employment related issues given by Gredka-Ligarska (2024) include:

a) Job displacement due to automation

Job displacement due to automation is a significant concern raised by scholars and experts in the context of AI and emerging technologies. Due to automation driven by AI, humans are replacing humans in many traditional jobs. AI is very accurate and fast as compared

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

to humans so many companies prefer AI over humans. Many studies have analysed the risk of automation for jobs in OECD countries, highlighting the potential impact on employment. Automation can lead to increased efficiency and productivity in every sector; it also raises concerns about the displacement of workers and the need for reskilling and upskilling to adapt to the changing job market. As AI grow very rapidly in recent times, it is responsibility of policy makers, business and individuals to overcomes the challenges of job displacement through proactive measure such as education and training program.

b) Liability for AI-driven employment decisions

Liability for AI- driven employment decisions is a complicated and evolving area of concern as AI is used more for appointing, hiring and other aspects of human resources. The AI used to make employment decisions raises questions about fairness, bias, transparency and accountability (Soni et al., 2025; Soni et al., 2023; Singh et al., 2022). Nowadays AI is used very commonly to make hiring or promotion decisions, there is a risk of unintentional discrimination based on factors like gender, race or age. If these decisions result in adverse outcomes for individuals, there may be legal implications related to discrimination and civil rights violations. In the context of liability, it is crucial for organisations to ensure that their AI systems are designed and implemented in a way that complies with anti- discrimination laws and regulations. Organisation may be held liable for discrimination practises that result from the use of AI in employment decisions (Kharitonova et al., 2022).

8. International Perspectives

In comparing the AI related laws and regulation globally, it demonstrates a changing environment that is influenced by various participants. In recent periods, countries with advanced AI technologies are staying on their strategies for more advancement in their technology with effort in the path of more enforceable laws. The EU stands at the highest position in AI regulation in establishing and maintaining the security related to privacy. In comparison, laws and regulations in the U.S and China are supposed to be broader and shallower than those in the EU. The rules and regulations also define the importance of ethical considerations in the development of AI with the primary motive of health care, autonomous vehicles, public administrations etc. Overall, the rules and regulations globally help to evolve the AI by updating standard guidelines etc.

The primary prerequisite for AI systems with significant risks is the need to conduct a conformance evaluation prior to product launch. To guarantee that the system is both technically sound and consistent with the law, this evaluation aims to verify that the system is

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

built upon a sufficient risk assessment, appropriate mitigation methods, and high-quality data sets. For regulators to evaluate the system's compliance, the evaluation should also verify the availability of documentation, activity logging to guarantee result traceability, user transparency and information, proper human oversight, robustness, correctness, and security. The nations of the EU are not stagnating. In 2018, both Germany and France established national AI initiatives; Italy as well as Spain followed in 2020. Additionally, supervisory agencies for data protection have already begun to act. Clearview AI was fined 20 million euros by France's Commission Nationale de l'Informatique et des Libertés (CNIL) in the month of October 2022 for invading the privacy of French users (Rozenshtein, 2023). Following the discovery that users' chat titles and payment details had been compromised in a data breach, the Italian data security supervisory authority, Garante, placed an indefinite ban on ChatGPT in March. The Garante expressed concerns regarding ChatGPT's inadequate transparency, the legality of the personally identifiable information processing used to train the algorithms used by the platform, and the accuracy of the responses it gave users. As a result of OpenAI's (ChatGPT developer) endeavours to address these issues, the Garante lifted the ban in April (Rozenshtein, 2023).

Congress in the United States has enacted and is now adding several legislative measures targeted at regulating aspects of AI. The National AI Initiative Act, often known as the U.S. AI Act, was signed into law in January of 2021. The National AI Initiative was founded by this legislation with the goal of advancing and coordinating AI-related research and development throughout the nation. The Federal Trade Commission's (FTC) initiatives in research, law enforcement, and advisory papers highlight the significance of AI technologies having the following qualities: explainability, accountability, fairness, openness, and empirical validity (Thomas, 2023).

Asian countries lack adequate laws for AI, though some countries have implemented rules and regulations that govern AI. China has produced a “Next Generation AI Development Plan” in June 2017 that is in line with its extensive AI regulations. The Expert Group on the Implementation of AI Principles and Japan's Ministry of Economy, Trade and Industry (METI) have collaborated to create a paper named “Guidelines for Governing the Implementation of AI Principles Version 1.1.” The Council for Integrated Innovation Strategy defined the Social Principles of Human-Centric AI in March 2019, and these recommendations offer a description of the concrete actions to take to align with them (Thomas, 2023).

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

9. Cooperation and challenges in addressing cross-border AI incidents

Cultural cooperation between various parties is necessary for the success of any ethics policy and governance initiatives. It refers to multiculturalism i.e. different nations and cultures will ensure that AI is appropriately used. Cross culture cooperation is necessary for various reasons. It must be guaranteed that no part of society in the world is neglected by AI. The first thing that must be done with AI is to bring about broad benefits across society globally. Second researchers around the whole world will exchange their expertise, utilise resources and adopt the recommended practices (Min, 2023). This will help in quicker discoveries of the beneficial AI applications and at the same time, the backdrop of related ethical and safety issues. Cooperation among the countries is very necessary because we give AI applications all by ourselves, we must act together for this. Cooperation between the countries based on worldwide can ensure the common goals at their environmental diversities (Rádi, 2023). The most common challenges that are faced during cross border cooperation is Mistrust between the two regions or cultures in AI ethics and governance. Globally widespread mistrust is between technologists, scholars and policymakers of the USA and China. Political tensions between two powerful association i.e. USA and China have turned into an issue that has been raised in recent years, both these associations give a neck-to-neck competition in AI development just like a race between two countries. Another challenge that is faced by cross border cooperation is that global cooperation should be accompanied by working on the difference of cultural and geographical particularities (Rádi, 2023).

10. Ethical Considerations

AI is the machine ability to perform the tasks that are associated with the human mind. AI is the most popular technique that is used by 90% of the people in the world. Hence it plays the most crucial role in the human world. It includes various fields like financial, transportation and healthcare etc. 30 to 40% of the people in the world say that AI has various disadvantages and humans cannot rely on it but according to the studies that AI is very helpful for the betterment of the society. This is proved by the ethical principles and considerations of AI development. One of the major ethical considerations encompassed by AI is bias. There are many factors that include gender, racial and cultural biases. For example, gender which is used for the hiring process can lead to the decrease in the no. of women candidates for specific positions (Matyuk, 2022).

There are two kinds of AI bias. First, the use of bias in AI leads to the discrimination and biases in society that stopped many years ago. Second, bias in AI development systems

can lead to unnecessary behaviour with the individuals. The next ethical consideration related to AI is Privacy. It is one of the major functions of the AI to collect personal information about the user and collect a large amount of data. If this personal data is not handled carefully then this might create a big issue regarding the security purpose. The main issue regarding this is how data is collected and used. One of the major issues related to privacy in AI is the misuse of personal data of individuals. Another issue related to AI is data breach (Rozenshtein, 2023). If the private data is not protected with care that is taken by the AI, then it is possible some unauthorised person may access your data, and this could lead to identity theft. People in the society are not aware of these frauds, and they give sensitive information to the AI system like healthcare info. & financial info. Now the AI system is more protected by the development of Biometrics and facial recognition techniques to record the behaviour of individuals and to reduce privacy related issues (Huriye, 2023).

10.1 *Establishing ethical guidelines for AI practitioners*

Establishing ethical guidelines for the new practitioners in AI is very difficult due to the rapid increment of AI in society (Matyuk, 2022). The Software Development Lifecycle (SDLC) phases are not completely addressed by the current methods of RAI (Responsible AI) with the primary motive of gathering information when leaving other phases unsupported. There are various issues concerning the ethical guidelines and terminologies that are used in AI development systems. To resolve these issues, we need to modify the AI principles that are used in development of AI by generating strong RE (requirement engineering). By providing consistency in the terminologies and in ethical guidelines, adding requirement engineering correctly then the practitioners can effectively develop the AI system that is used widely across the world (Matyuk, 2022).

10.2 *Balancing technological advancements with ethical responsibility*

It is important to identify the ethical dimensions that come in AI infusion in educational learning and never consider them as secondary. As AI developed as a core which contains several constituents like educative domains, different parties that are present in between AI and other organisations. With the help of education, a person can learn about how to behave, way of speaking and gain knowledge. In the education system, there are two other main ethical dimensions i.e. data security and privacy. The collection and storage of complex data in more amounts can make an issue of data security and its privacy. Software engineers and policy makers of educational institutions play a very crucial role in maintaining the private or sensitive information and transparency and provide legal data that are not against the individual rights and upload ethical principles. The addition of AI in the educational field requires legal ethical

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

principles, policies and other key responsibilities that make a balance between advanced technology Like AI and responsibilities. The collaboration of AI in the educational field contains a lot of issues that need to be solved like human-machine interface, algorithm bias and a lot more. Scientists also confront methods of procuring data, designing algorithms and the ethical procedures associated with the education sector. In today's world it is necessary to add AI in every field of work especially in the education sector to identify challenges, risk and ethical considerations. (Jiarawattanakul, 2023).

11. Future Outlook

AI related liability facing various kinds of challenges because of the possible risk that derives from the introduction and application of AI technologies in the society. The current problem is just to prove the malfunction in accidents related to AI that are shown by major functions of AI like logical, lack of causality, opacity and many more. For more precise working of AI, we need to evolve the existing regulations concerning liability. For updating civil liabilities, it involves a rule which is known as "No fault redress rule." It Means the injured persons should receive compensation for their injuries without having to prove fault against any individual. This rule will help indirectly in the evolution of AI. Therefore, the AI related liability always runs in between the range from broad expansion to narrow expansion in AI technology (Chandra & Sanjaya, 2023).

12. Recommendations for enhancing legal frameworks

There are several recommendations that are considered for enhancing the legal outcomes of the framework: First is, the use of technology for the advancement in the security system of patents plays a very important role in global rights protection in AI technology. Second, by adding global lifecycle analysis leads to the quality of AI systems and enforcement of law. By exploring the tools that are launched by the government, and their mechanisms can help us to understand the operational gap in AI governance (Chandra & Sanjaya, 2023). By creating open rules and regulations and institutions will be needed to control AI technology like facial recognition. By using these two steps of recommendations of enhancing the legal framework, AI technology can be strengthened to give an innovation to the world without harming the society. (Almeida et al., 2023).

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

13. Conclusion

Unquestionably, the development of AI has transformed many facets of society and presented previously unheard-of chances for advancement and creativity (Kandpal et al., 2025). All computer learning is based on AI, which is also the foundation for all complicated decision-making in the future. AI is revolutionising healthcare by forecasting patient outcomes and identifying illnesses. Early illness diagnosis and treatment can be facilitated by machine learning models' faster and more accurate analysis of medical data, including MRI and X-ray images, than by human analysts. The legal, ethical, and societal ramifications of its usage are becoming increasingly crucial to address as we incorporate technology more fully into every aspect of our lives.

Looking over international laws for AI, many nations and areas are addressing the legislation of AI. Since various circumstances may call for different approaches and goals, there is no universal approach to governing AI. It's crucial to remember that most nations currently have relatively little experience with AI legislation and regulations. To guarantee that AI is researched and applied in a way that is ethical, responsible, and advantageous for everybody, there is also an imperative for international cooperation and communication. Examining the viewpoint on civil and criminal accountability about AI victims highlights the complex issues we encounter while negotiating this quickly changing environment. The challenges are numerous, ranging from algorithmic biases producing biassed decisions to the possibility of harmful autonomous systems. To further develop comprehensive approaches that strike a balance between innovation, accountability, and social well-being, it is imperative that stakeholders including technologists, politicians, legal professionals, and ethicists engage in multidisciplinary discourse and collaboration.

References

Agarwal, V. (2012). Privacy and data protection laws in India. *International Journal of Liability and Scientific Enquiry, 5*(3-4), 205-212.

Al Qatawneh, I. S., Moussa, A. F., Haswa, M., Jaffal, Z., & Barafi, J. (2023). *Artificial Intelligence Crimes.*

Almeida, V., Mendes, L. S., & Doneda, D. (2023). On the development of AI governance frameworks. *IEEE Internet Computing, 27*(1), 70-74.

Alshamsan, A. R., & Chaudhry, S. A. (2022, December). Detecting Privacy Policies Violations Using Natural Language Inference (NLI). In *2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)* (pp. 1-6). IEEE.

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

Bakiner, O. (2023). The promises and challenges of addressing artificial intelligence with human rights. *Big Data & Society*, *10*(2), 20539517231205476.

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. *Ieee Access*, *10*, 77110-77122.

Bonna, A. P., & Sá, V. V. (2021). Responsabilidade civil do médico por erros ocasionados no uso da inteligência artificial. *Revista Brasileira de Direito Civil em Perspectiva*, *7*(1), 45-66.

Cambiaso, E., & Caviglione, L. (2023). Scamming the scammers: Using chatgpt to reply mails for wasting time and resources. *arXiv preprint arXiv:2303.13521*.

Chakraborty, A., Biswas, A., & Khan, A. K. (2023). Artificial intelligence for cybersecurity: Threats, attacks and mitigation. In *Artificial Intelligence for Societal Issues* (pp. 3-25). Cham: Springer International Publishing.

Chandra, R., & Sanjaya, K. (2023, January). Punishing the unpunishable: a liability framework for artificial intelligence systems. In the International Conference on Digital Technologies and Applications (pp. 55-64). Cham: Springer Nature Switzerland

Chaudhary, G. (2020). Artificial intelligence: the liability paradox. ILI Law Review.

Coeckelbergh, M. (2020). Artificial intelligence, responsibility attribution, and a relational justification of explainability. *Science and engineering ethics*, *26*(4), 2051-2068.

D'Alfonso, G. (2022). Intelligenza artificiale e responsabilità civile. Prospettive di regolamentazione europea.

Dimitrova, R. (2022). Criminal liability associated with artificial intelligence entities under the Bulgarian Criminal law. In *2022 XXXI International Scientific Conference Electronics (ET)* (pp. 1-5). IEEE.

Gautam, A., Piplani, R., Soni, P., & Singh, R. (2025). Psychological perspective of white-collar crimes. *International Journal of Interdisciplinary Approaches in Psychology*, *3*(1), 57-66.

Gredka-Ligarska, I. (2024). Employer as an AI System Operator and Tortious Liability for Damage Caused by AI Systems: European and US Perspectives. *The Chinese Journal of Comparative Law*. https://doi.org/10.1093/cjcl/cxae015.

Greene, D., & Shenoy, J. (2022). How do anti-discrimination laws affect firm performance and financial policies? Evidence from the post-World War II period. *Management Science*, *68*(5), 3813-3833.

Greiman, V. A. (2022). Cyber Law and Regulation. In *Cyber Security: Critical Infrastructure Protection* (pp. 59-78). Cham: Springer International Publishing.

Grimm, C. M., Smart, W. D., & Hartzog, W. (2018, December). An Education Model of Reasonable and Good-Faith Effort for Autonomous Systems. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 117-121).

Hallevy, G. (2010). The criminal liability of artificial intelligence entities-from science fiction to legal social control. *Akron Intell. Prop. J.*, *4*, 171.

Härkänen, M., Haatainen, K., Vehviläinen-Julkunen, K., & Miettinen, M. (2021). Artificial intelligence for identifying the prevention of medication incidents causing serious or moderate harm: an analysis using incident reporters' views. *International Journal of Environmental Research and Public Health*, *18*(17), 9206.

Heim, T. N. (2023). Global governance and regulation of cybersecurity: Towards coherence or fragmentation?.

Huriye, A. Z. (2023). The ethics of artificial intelligence: examining the ethical considerations surrounding the development and use of AI. American *Journal of Technology*, *2*(1), 37-44.

Ivanova, P., & Antonova, K. (2022). The Use Of Artificial Intelligence: Challenges For Employment. *Education, Science And Digital Innovations-Sinergy For Professional Way 2021, Round table proceedings*, (1), 44-51.

Jiarawattanakul, K. (2023, October 7). *The Technological Advancement of Artificial Intelligence*. LinkedIn. Retrieved April 11, 2024, from https://www.linkedin.com/pulse/technological-advancement-artificial-intelligence-jiarawattanakul/

Kamalova, G. G. (2020). Some issues of criminal liability in the field of application of artificial intelligence and robotics systems. *Bulletin of Udmurt University. Economics and Law Series , 30* (3), 382-388

Kandpal, N., Singhal, N., Lavaniya, H. V., Jain, R., Singh, R., & Gaur, A. (2025). Utilizing artificial intelligence and machine learning for enhanced recycling efforts. In *AI Technologies for Enhancing Recycling Processes* (pp. 65-82). IGI Global Scientific Publishing https://doi.org/10.4018/979-8-3693-7282-1.ch004

Kaur, A., Maheshwari, S., & Tripathi, N. (2022). AI, Privacy Breaches and Ethical Transgressions: An Integrative Theoretical Framework. In *Academy of Management Proceedings* (Vol. 2022, No. 1, p. 12024). Briarcliff Manor, NY 10510: Academy of Management.

Kelley, S., Ovchinnikov, A., Hardoon, D. R., & Heinrich, A. (2022). Anti-discrimination Laws, AI, and Gender Bias: A Case Study in Non-mortgage Fintech Lending. *Manufacturing*

& Service Operations Management 0 (0). https://doi. org/10.1287/msom.

Kharitonova, Y. S., Savina, V. S., & Pagnini, F. (2022). Civil Liability in the Development and Application of Artificial Intelligence and Robotic Systems: Basic Approaches. *Perm U. Herald Jurid. Sci.*, *58*, 683.

Khisamova, Z. I., & Begishev, I. R. (2019). Criminal liability and artificial intelligence: theoretical and applied aspects. *All-Russian Journal of Criminology , 13* (4), 564-574.

Kirpichnikov, D., Pavlyuk, A., Grebneva, Y., & Okagbue, H. (2020). Criminal liability of the artificial intelligence. In *E3S web of conferences* (Vol. 159, p. 04025). EDP Sciences.

Krassadaki, E., & Matsatsinis, N. (2023). Career options and necessary technical skills in AI. In *Handbook of Research on Artificial Intelligence, Innovation and Entrepreneurship* (pp. 350-366). Edward Elgar Publishing.

Laacke, S. (2023). Bias and epistemic injustice in conversational AI. *The American Journal of Bioethics*, *23*(5), 46-48.

Leavy, S., O'Sullivan, B., & Siapera, E. (2020). Data, power and bias in artificial intelligence. *arXiv preprint arXiv:2008.07341*.

Llorca, D. F., Charisi, V., Hamon, R., Sánchez, I., & Gómez, E. (2023). Liability regimes in the age of AI: a use-case driven analysis of the burden of proof. *Journal of Artificial Intelligence Research*, *76*, 613-644.

Luo, Q., Yu, Y., Liu, J., & Benslimane, A. (2021). Automatic detection for privacy violations in Android Applications. *IEEE Internet of Things Journal*, *9*(8), 6159-6172.

Macrae, C. (2022). Learning from the failure of autonomous and intelligent systems: Accidents, safety, and sociotechnical sources of risk. *Risk analysis*, *42*(9), 1999-2025.

Mahmud, H., & Jahankhani, H. (2021). Hacking Artificial Intelligence (AI) Engines for Organised Crime and Inciting Chaos. *Information Security Technologies for Controlling Pandemics*, 387-414.

Malhotra, S., Arora, G., & Bathla, R. (2023, May). Detection and Analysis of Fraud Phone Calls using Artificial Intelligence. In *2023 International Conference on Recent Advances in Electrical, Electronics & Digital Healthcare Technologies (REEDCON)* (pp. 592-595). IEEE.

Martsenko, N. (2022). Civil liability for damage caused by artificial intelligence. *Proceedings. Series: Law*, (12), 34-39.

Matyuk, Y. S. (2022). Legal Regulation of Artificial Intelligence: Foreign Practices. Russian Journal of Legal Studies (Moscow), 9(2), 107-115.

McCauley, L. (2007). AI Armageddon and the Three Laws of Robotics. *Ethics and Information*

Technology, 9, 153-164. https://doi.org/10.1007/s10676-007-9138-2.

McGregor, S. (2021, May). Preventing repeated real world AI failures by cataloging incidents: The AI incident database. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 35, No. 17, pp. 15458-15463).

Min, A. (2023). Artificial Intelligence And Bias: Challenges, Implications, And Remedies. Journal of Social Research, 2(11).

More, A., Mahajan, M., & Gholap, H. AI and IOT Based Road Accident Detection and Reporting System.

Nasim, S. F., Ali, M. R., & Kulsoom, U. (2022). Artificial intelligence incidents & ethics a narrative review. *International Journal of Technology, Innovation and Management (IJTIM)*, *2*(2), 52-64.

Nerantzi, E., & Sartor, G. (2024). 'Hard AI Crime': The Deterrence Turn. *Oxford Journal of Legal Studies*, 44, 673 - 701. https://doi.org/10.1093/ojls/gqae018.

Oh, J. (2023). Legal relations related to Artificial Intelligence. *Law Research Institute Chungbuk National University*. https://doi.org/10.34267/cbstl.2023.14.2.143.

Panchbhai, A. V., Nemane, D. V. V., & Sonule, D. V. B. (2022). Product Liability Law in India-a Critique. *Journal of Positive School Psychology*, 561-567.

Pandey, A., Bhatraju, A., Markam, S., & Bhatt, D. (2022, November). Adversarial Fraud Generation for Improved Detection. In *Proceedings of the Third ACM International Conference on AI in Finance* (pp. 123-129).

Pappadà, R., & Pauli, F. (2022). Discrimination in machine learning algorithms. *arXiv preprint arXiv:2207.00108*.

Plachkinova, M. (2022). US Cybersecurity Laws and Regulations: Current Trends and Recommendations for Improvement. In *Global Perspectives on Information Security Regulations: Compliance, Controls, and Assurance* (pp. 1-21). IGI Global.

Ponce, A. (2021). The AI Regulation: entering an AI regulatory winter? Why an ad hoc directive on AI in employment is required. *Why an ad hoc directive on AI in employment is required (June 25, 2021). ETUI Research Paper-Policy Brief*.

Poon, N. C., & Sung, J. J. (2019). Self-driving cars and AI-assisted endoscopy: Who should take the responsibility when things go wrong?. *Journal of Gastroenterology & Hepatology*, *34*(4).

Rádi, V. G. (2023, May). Comparative Analysis of the AI Regulation of the EU, US and China from a Privacy Perspective. In 2023 46th MIPRO ICT and Electronics Convention (MIPRO) (pp. 1446-1451). IEEE.

Rickardo, G., & Meiriele, S. (2023). Artificial Intelligence: Its Impact on Employability. *World Journal of Advanced Research and Reviews*, *18*(3), 198-203.

Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, *4*, 100005.

Rozenshtein, A. Z. (2023). *A Comparative Perspective on AI Regulation*. Lawfare. Retrieved April 13, 2024, from https://www.lawfaremedia.org/article/a-comparative-perspective-on-ai-regulation

Santoni de Sio, F., & Van den Hoven, J. (2018). Meaningful human control over autonomous systems: A philosophical account. *Frontiers in Robotics and AI*, *5*, 15.

Saud, A. (2024). Criminal Liability about the Use of Artificial Intelligence: Investigating the Actus Reus Element of AI-driven Technology. *American Journal of Law, 6*(1), 1-25.

Sawant, S., Raisinghani, D., Vazirani, S., Zawar, K., & Giri, N. (2023). Nirbhaya Naari: An artificial intelligence tool for detection of crime against women. In *Intelligent Systems and Human Machine Collaboration: Select Proceedings of ICISHMC 2022* (pp. 29-45). Singapore: Springer Nature Singapore.

Shin, D., & Shin, E. Y. (2023). Data's Impact on Algorithmic Bias. *Computer*, *56*(6), 90-94.

Shirokova, E. S., & Fedulin, A. M. (2022). On the Issue of Liability for Harm Caused by the Actions of Drones Using Artificial Intelligence. In *Proceedings of the Fifth International Scientific Conference "Intelligent Information Technologies for Industry"(IITI'21)* (pp. 664-671). Springer International Publishing.

Siboni, G., & Sivan-Sevilla, I. (2019). Regulation in Cyberspace.

Singh, R., Soni, P., & Kerie, A. (2025). Social Engineering Attacks: Detection and Prevention. *Securing the Digital Frontier: Threats and Advanced Techniques in Security and Forensics*, 269-290. https://doi.org/10.1002/9781394268917.ch12

Singh, R., Soni, P., & Kumar, A. (2022). Cyber abuse of women at workplace. *Women at work: a holistic outlook*, 119-127.

Sipior, J., Ward, B., Rusinko, C., & Lombardi, D. (2023). Bias in Using AI for Recruiting: Legal Considerations. *Information Systems Management*, 41, 399 - 412. https://doi.org/10.1080/10580530.2023.2294453.

Slootmaeckers, K. (2023). Anti-discrimination policies: From the margins to differentiated politicisations. In *Coming in* (pp. 73-97). Manchester University Press.

Socatiyanurak, V., Klangpornkun, N., Munthuli, A., Phienphanich, P., Kovudhikulrungsri, L., Saksakulkunakorn, N., ... & Tantibundhit, C. (2021). Law-u: Legal guidance through artificial intelligence chatbot for sexual violence victims and survivors. *IEEE Access*,

9, 131440-131461.

Soni, P., Shruti, K. M., Srivastav, S., & Singh, R. (2025). From Fun to Fear: Unveiling the Nexus of Cyberbullying and Online Gaming. *International Journal of Interdisciplinary Approaches in Psychology*, *3*(7), 103-112. https://doi.org/10.61113/ijiap.v3i7.1103

Soni, P., Singh, R., & Kumar, A. (2023). Cyberbullying and Cyber Victimization: Dreadful Psychological Impact on Adolescents. *Mental Health and Well-being—New Paradigms*, 19.

Stefański, K. (2022). The Issue of the Subjectivity of Artificial Intelligence Acting for an Employer. *Studia z Zakresu Prawa Pracy i Polityki Społecznej*, *29*(2), 95-103.

Streich, G. (2022). (Re-) configuring federal cybersecurity regulation: from critical infrastructures to the whole-of-the-nation. *Ind. L. Rev.*, *55*, 733.

Sumodiningrat, A., & Nabila, J. A. (2022). Against Discrimination. *Journal of Contemporary Sociological Issues*, *2*(2), 116-135.

Tao, X., Li, L., & He, J. (2022, November). Research on discrimination and regulation of artificial intelligence algorithm. In *2nd International Conference on Artificial Intelligence, Automation, and High-Performance Computing (AIAHPC 2022)* (Vol. 12348, pp. 79-84). SPIE.

Thomas, R. J. (2023, September 25). *AI Law & Regulation: A Synopsis of the Global Perspective*. Medium. Retrieved April 13, 2024, from https://medium.com/version-1/ai-law-regulation-a-synopsis-of-the-global-perspective-8ad720c6bca2

Vojtuš, F., Kordík, M., & Dražová, P. (2022, October). Artificial Intelligence and the criminal responsibility-challenges, obstacles and possible solutions. In 2022 Al Qatawneh, I. S., Moussa, A. F., Haswa, M., Jaffal, Z., & Barafi, J. (2023). Artificial Intelligence Crimes.

Walters, K., & Markazi, D. M. (2021). Insights from people's experiences with ai: Privacy management processes. In *Diversity, Divergence, Dialogue: 16th International Conference, iConference 2021, Beijing, China, March 17–31, 2021, Proceedings, Part I 16* (pp. 33-38). Springer International Publishing.

Walz, A., & Firth-Butterfield, K. (2019). Implementing ethics into artificial intelligence: A contribution, from a legal perspective, to the development of an AI governance regime. *Duke L. & Tech. Rev.*, *18*, 176.

Wemmers, J. A. (2012). Victims Rights are Human Rights: The importance of recognizing victims as persons. *Temida, June.*

Windl, M., Winterhalter, V., Schmidt, A., & Mayer, S. (2023, April). Understanding and mitigating technology-facilitated privacy violations in the physical world. In

Vol. 4, Issue 3 March 2026 ISSN: 2584-0142

Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (pp. 1-16).

Zech, H. (2021). Liability for AI: public policy considerations. *ERA Forum*, 22, 147 - 158. https://doi.org/10.1007/s12027-020-00648-0.

Zhang, C. (2023). Towards societal impact of AI. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 37, No. 13, pp. 15463-15463).

Zhang, Q., Wallbridge, C. D., Jones, D. M., & Morgan, P. (2021). The blame game: Double standards apply to autonomous vehicle accidents. In *International Conference on Applied Human Factors and Ergonomics* (pp. 308-314). Cham: Springer International Publishing.