

Artificial Intelligence, Robotics, and the Transformation of Forensic Law in Cameroon

NGONDA Yusi Roger¹

¹ Ph.D. Fellow in Law, University of Bangui, Central African Republic

Correspondence: NGONDA Yusi Roger, Ph.D. Fellow in Law, University of Bangui, Central African Republic.

doi:10.63593/LE.2788-7049.2026.09.001

Abstract

Artificial intelligence and robotics are no longer features of science fiction. They are reshaping the way justice is investigated, prosecuted, and administered in legal systems around the world, including in Cameroon. This article examines that transformation through a critical and grounded lens, asking not merely what these technologies can do, but whether the law as it currently stands in Cameroon is ready to govern what they do. The article finds that Cameroon currently lacks dedicated legislation governing artificial intelligence and robotics in forensic or judicial contexts. This regulatory vacuum creates serious risks: evidence produced by AI systems lacks clear admissibility standards, liability for errors by autonomous systems is legally indeterminate, and protections for the rights of accused persons are inadequate in the face of automated decision-making. The doctrine of *res ipsa loquitur* and the concept of legal personhood for AI entities are examined as possible bridges between existing jurisprudence and emerging technological realities. The article concludes by proposing a multi-pronged governance pathway for Cameroon: the enactment of dedicated AI legislation with specific forensic provisions, the establishment of interdisciplinary regulatory bodies, the development of clear liability frameworks for autonomous systems, and the integration of ethical AI principles of fairness, transparency, and accountability into Cameroon's legal culture.

Keywords: artificial intelligence, forensic law, robotics, legal liability, *res ipsa loquitur*

1. Introduction

The relentless advancement of “Artificial Intelligence” (AI) and “Robotics” has propelled society into an era of unparalleled technological sophistication.¹ Artificial Intelligence and robotics are transforming forensic law by introducing innovative methods for solving crimes and enhancing the efficiency of the justice system. Forensic law, which involves the application of scientific and technological principles to legal cases, has greatly benefited from the integration of AI and robotics. These technologies facilitate faster, more accurate data analysis, reduce human error, and improve decision-making processes in legal and forensic contexts.² The question thus, what therefore is Artificial Intelligence (AI)? There are many official definitions of what Artificial Intelligence systems are, provided both by independent organisations and by national legislators in some cases; we would take as a starting reference the definition provided by the expert group appointed by the European Commission in 2019 (AI HLEG): per this Commission, “Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best

¹ Chidiogo U., et al. (2024). Legal Challenges of Artificial Intelligence and Robotics: A Comprehensive Review. *Computer Science and Information Technology Research Journal*, 5(3), 544.

² Chen Y., et al. (2021). Enhancing Forensic Accuracy through Deep Learning. *Journal of AI Applications*, 18(4), 45–60.

action(s) to take to achieve the given goal.¹

AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)".² This is a very comprehensive definition, providing both a notion of AI as a field of study and of the products of its implementation that can be taken into account for regulatory purposes.

Thus, when talking about AIs one can refer to software running either in a simple computer — or in a computer network or in a more complex physical architecture — that is, the hardware component - made up of such as sensors, computer vision devices, and so on. The former might be defined as generic 'AI algorithms' or 'software agents' while the latter might be called "robot agents". Either way, prior to software or hardware, the core element of both these technologies is data on which — at least for the new generation the AI systems are built and trained. For what concern robots and robotics, there are several industrial applications especially in heavy industries — both for logistics and manufacturing.³ There are also interesting uses of robots for educational and recreational purposes as well as to assist vulnerable people, for example, people suffering from dementia or autism.⁴ In addition, some robots are able to provide surgical assistance for high-precision operations.⁵

The aim of this overview is to help understand both to clarify the notion of 'artificial intelligence systems' and which of these computational artefacts are most likely to be of interest for the scope of attributing an autonomous legal personality. More specifically, the common property of the technologies we are concerned with is ability to deliberate according to evaluations that are, to some extent, independent of those of the designer. In a sense, AIs have a degree of epistemic and practical authority over their own behaviour.⁶ What are we referring to when we talk about Artificial Intelligence? We can both describe a scientific field and a series of technologies somehow derived from it. An attempt was made to circumscribe the AI technologies under consideration in this work to the so-called Artificial Intelligence systems (AIs), although this notion still suffers from some vagueness. A more detailed identification of the specific AI systems relevant to our research question will be attempted in next sections, using not only factors relating to the technical components, but also that of the social context in which systems operate.

AI as a branch of knowledge studies the way in which human intelligence, or some of its characteristics, can be reproduced in artificial objects. Even though nowadays these artefacts are mostly computer based, nothing prevents the same goals from being pursued on hybrid systems in the future. A broad enough, and often cited, definition was proposed by the leading AI scientist John McCarthy, according to whom AI: "is the science and engineering of making intelligent machines, especially intelligent computer programs."⁷ It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to

¹ AI HLEG. (2019). A definition of AI: main capabilities and disciplines, European Commission, <https://ec.europa.eu/digital-inglemarket/en/news/definitionartificial-intelligence-main-capabilities-and-scientific-disciplines>. A more concise definition is the one provided by the Organisation for Economic Co-operation and Development (OECD), in the 2019 recommendation of the Council on Artificial Intelligence: "An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy" (OECD. LEGAL/0440).

² *Ibid.*

³ Yongjun Xu, et al. (2021). Artificial intelligence: A Powerful Paradigm for Scientific Research. *The Innovation Review*, 2(1), 1-20.

⁴ Wood J., et al. (2012). Developing Kaspar: A Humanoid Robot for Children with Autism. *International Journal of Social Robotic*, 13(3-4), 500.

⁵ *Ibid.*

⁶ Omohundro Stephen. (2008). The Basic AI Drives: Artificial General Intelligence. *Frontiers in Artificial Intelligence and Applications*, 171(1-3), 483-492.

⁷ MacCarthy, J. (2007). What is Artificial Intelligence? Available at <http://jmc.stanford.edu/articles/whatisai.html> (Lastly Accessed on 16/04/2026).

methods that are biologically observable”.¹

More and more often humans, in different activities as users of a self-driving vehicles, consumers making a contract with a bot, physicians supported by a diagnostic system interact with artificial entities that play an active role in such activities. These entities process information and make choices between epistemic and practical alternatives, make changes in the digital or physical world, and engage in communication. Their action appears to be autonomous, in the sense that it is not preprogramed by a human designer as a specific response to the particular circumstances of the concrete situation. It is up to such systems to process the available information, using learning and inferential algorithms, and to make assessments and decisions accordingly.² An additional complexity is owed to the fact that each such an agent may be part of a dense network of agents, sharing information and making coordinated decisions.

This raises a set of issues pertaining to legal liabilities, as well as to accountability and moral responsibility. Who is to be asked to explain and justify the behaviour of such a system? Who may be subject to blame or adverse consequences in case such behaviour turns out to be harmful? Who is to be subject to legal penalties, including damages as well as administrative fines or criminal punishment, when such a behaviour violates applicable legal rules? Is it the owner, the user, the programmer, the manager of the development team, the person tasked with testing and debugging? What happens if an action cannot be traced back to any particular human?³

The harmful behaviour of AI systems can engender obligations for the human agents involved, such as users, owners, and developers. Artificial agents can also participate in legally relevant interactions, producing effects in the sphere of their owners as well as that of human third parties. Their use can produce legal effects, that is, contractual rights and obligations, for their users (for example, vendors in electronic commerce) by virtue of their ability to interact with other subjects (human and electronic) entering into legal transactions. Equally remarkable is the capacity of some AIs to generate creative works — paintings, songs, novels, etc. — prompting the European Parliament to consider whether AI-generated artworks and inventions might be protected by copyright.⁴

One of the most significant contributions of AI to forensic law is the ability to process large datasets rapidly. Machine learning algorithms, a subset of AI, can analyze complex forensic data, including DNA sequences, fingerprints, and voice patterns, with remarkable accuracy. These systems have been shown to outperform traditional methods in terms of speed and precision, leading to breakthroughs in cold cases and more efficient criminal investigations.⁵ AI-powered tools also enable predictive analysis in forensic investigations. By analyzing historical data, these systems can predict crime patterns, identify high-risk areas, and even suggest potential suspects. For example, crime-mapping tools equipped with AI algorithms have helped law enforcement agencies allocate resources more effectively and prevent crimes before they occur.⁶

Digital forensics has been revolutionized by AI systems that can extract, analyze, and correlate digital evidence from various sources, such as mobile phones, computers, and online platforms. Automated tools can identify anomalies in digital footprints, detect cybercrimes, and recover deleted files, thereby providing critical evidence in court proceedings.⁷ These advancements are crucial in an era where cybercrime is becoming increasingly prevalent. Facial recognition technology, powered by AI, is another transformative tool in forensic law. This technology can identify individuals in real-time, aiding in the identification of suspects and missing persons. However, concerns regarding privacy and ethical implications have prompted calls for stricter regulations to ensure its responsible use.⁸

¹ Each AI system poses a negative impact on privacy for the individual at multiple levels. Depending on how it is applied, facial recognition AI systems can essentially create “dragnet biometric databases” that impact both criminal and law-abiding citizens. If applied in a live video feed, then any expectations of privacy or anonymity in public are essentially eroded by the capabilities of a facial recognition system. Since there are no current limitations or regulations imposed on this type of technology, law enforcement agencies are not required to submit warrants or justification before usage. For this reason, many municipalities have taken it upon themselves by banning the usage of facial recognition by public agencies within their jurisdiction.

² MacCarthy, J. (2007). *Op. Cit.*, note 12.

³ Trahan J. (2008). The Distinction Between Persons & Things: An Historical Perspective. *Journal of Civil Law Studies*, 1(6), 341-360.

⁴ *Ibid.*

⁵ Roberts D., et al. (2022). Autonomous Robotics in Forensic Evidence Collection. *Journal of Autonomous Systems*, 19(2), 168.

⁶ Smith, J., et al. (2021). AI Applications in DNA Evidence Analysis. *Journal of Forensic Bioinformatics*, 9(2), 48.

⁷ *Ibid.*

⁸ Brown, H., et al. (2021). Role of Robotics in Post-Disaster Forensic Investigations. *Disaster and Forensic Science Review*, 10(3), 312.

Robotics has also found its way into forensic investigations, particularly in crime scene analysis. Robots equipped with cameras and sensors can navigate hazardous environments, collect evidence, and preserve the integrity of crime scenes.¹ This capability is especially valuable in cases involving biohazards, explosives, or other dangerous conditions.² In addition to crime scene analysis, robotics plays a role in automating repetitive tasks in forensic laboratories. For instance, robotic systems can automate the process of DNA extraction and analysis, thereby reducing the workload for forensic scientists and minimizing the risk of contamination or human error.³

AI has proven invaluable in analyzing audio and video evidence. Algorithms can enhance low-quality recordings, identify speakers, and detect manipulated audio or video files. These capabilities are essential in cases where the authenticity of evidence is contested.⁴ Natural Language Processing (NLP), a branch of AI, has enhanced the analysis of textual evidence. NLP systems can process large volumes of documents, emails, and social media posts to identify relevant information and establish connections between suspects and criminal activities. This capability has been particularly useful in cases involving financial crimes and organized crime networks.⁵ AI has also improved the accuracy of forensic pathology. Machine learning algorithms can assist in determining causes of death by analyzing medical images and autopsy reports. These systems provide valuable insights, especially in complex cases where traditional methods may fall short.⁶

The integration of AI and robotics in forensic law has implications for the courtroom as well. AI systems can simulate crime scenes, reconstruct events, and present evidence in a more comprehensible manner for judges and juries.⁷ Virtual reality (VR) tools, powered by AI, allow for immersive reconstructions of crime scenes, enhancing the understanding of evidence. Despite these advancements, the use of AI in forensic law is not without challenges. One major concern is the potential for bias in AI algorithms, which can lead to wrongful convictions or unequal treatment under the law. Ensuring fairness and transparency in AI systems remains a critical priority for developers and policymakers.⁸ Another challenge is the admissibility of AI-generated evidence in court. Legal frameworks must evolve to address questions of reliability, accuracy, and accountability associated with AI tools. Establishing clear guidelines for the use of AI in forensic investigations is essential for its acceptance in legal contexts.⁹

The ethical implications of AI and robotics in forensic law are also a topic of debate. Issues such as privacy, consent, and surveillance require careful consideration to balance the benefits of these technologies with the rights of individuals. Collaboration between technologists, forensic experts, and legal professionals is crucial for the successful integration of AI and robotics in forensic law. Interdisciplinary efforts can ensure that these technologies are developed and implemented in ways that align with legal standards and ethical principles.¹⁰ Training and education are equally important. Forensic professionals must be equipped with the skills to understand and operate AI and robotic systems effectively. Continuous professional development programs can help bridge the gap between technological advancements and practical applications.¹¹ Looking ahead, the potential of AI and robotics in forensic law is immense. Emerging technologies such as quantum computing and advanced neural networks promise even greater capabilities for solving crimes and administering justice.

However, the pace of technological progress must be matched by efforts to address legal, ethical, and social challenges.¹² The role of AI and robotics in forensic law extends beyond solving crimes to preventing them. Predictive policing, enhanced surveillance, and real-time data analysis can create safer communities and more efficient legal systems. The future of forensic law will likely see even greater reliance on these technologies to

¹ Lee J., et al. (2023). Training Forensic Scientists in AI and Robotics: A New Paradigm. *Journal of Forensic Education*, 7(1), 17.

² *Ibid.*

³ Jones A., et al. (2020). Predictive Analytics in Law Enforcement: Applications and Limitations. *Criminal Justice Technology*, 15(2), 25.

⁴ Patterson, S., et al. (2022). Cybersecurity Challenges in AI-Driven Forensic Investigations. *Computers & Security*, 115, 102738. <https://doi.org/10.1016/j.cose.2022.102738>

⁵ Miller B., et al. (2020). Robotics in Forensic Anthropology: A Case Study. *Journal of Forensic Robotics*, 13(3), 190.

⁶ *Ibid.*

⁷ *Ibid.*

⁸ Wilson D., et al. (2023). Public Perception of AI and Robotics in Forensic Law. *Journal of Criminal Justice Ethics*, 14(1), 79.

⁹ *Ibid.*

¹⁰ *Ibid.*

¹¹ *Ibid.*

¹² *Ibid.*

achieve justice and maintain public trust.¹ Robotics, on the other hand, has been instrumental in augmenting forensic practices by performing tasks such as scene reconstruction and evidence retrieval with precision.² This technological integration promises enhanced efficiency and accuracy in solving criminal cases.

The rise of AI-powered tools in forensic law has also brought new approaches to predicting criminal behaviors and identifying suspects. Predictive analytics tools assess patterns in crime data to provide law enforcement with insights into potential criminal activities.³ Additionally, facial recognition technologies, enabled by AI, have gained prominence in suspect identification, providing results with unprecedented speed and reliability. Despite these advancements, concerns over privacy and bias in AI algorithms persist, raising ethical and legal challenges.⁴ These concerns necessitate critical appraisals of AI applications within forensic law.

Robotics in forensic investigations provides unique capabilities for handling hazardous environments and collecting evidence in conditions unsafe for humans. Robots equipped with sensors and imaging tools facilitate investigations in disaster zones or chemically hazardous crime scenes.⁵ However, the deployment of robotics in forensic contexts remains limited due to high costs and the need for specialized training. This indicates a gap in the widespread adoption of robotics technologies in forensic law. Legal frameworks and governance structures surrounding the use of AI and robotics in forensic law are still developing. Policymakers and judicial bodies are working to establish regulations to govern the use of these technologies in a manner consistent with legal and ethical principles.⁶ The legal community must address questions of accountability, particularly when errors occur in forensic analyses conducted by AI or robotics systems.

Moreover, the integration of AI and robotics into forensic law requires robust interdisciplinary collaborations. This includes partnerships between technologists, legal practitioners, and forensic scientists to ensure the technologies align with the evidentiary standards of the legal system. According to recent studies, the lack of standardized protocols for incorporating AI and robotics into forensic processes hampers their effectiveness and acceptance in legal proceedings.⁷ There is no one-size-fits-all approach to addressing liability and regulatory issues associated with the new growing technology. The solution is to have the correct balance between encouraging innovation and entrepreneurship and also on addressing real safety and privacy concerns.⁸ As new technologies, among other things self-driving cars, drones, augmented and virtual reality as well as the internet of things (IoT)⁹, get more and more popular, rules and laws governing the new technology need to keep up.¹⁰

The liability of AI and robotics in forensic law raises complex legal questions, as existing frameworks struggle to address the actions of autonomous systems and the potential for bias and lack of transparency. While AI can enhance forensic capabilities, the potential for misuse and the need for accountability require careful consideration and adaptation of legal approaches. The question on who becomes liable if a privately owned robot destroys property or authorities' AI-system giving the wrong answer or decision that causes harm is very necessary. Now and especially in the future, the liable party in AI-related accidents is not so clear anymore, which means that the answer to the question "who is liable and under what circumstances is unclear".

The main issue is that if, for instance, a self-driven car collides with another vehicle, who then can be held liable,

¹ *Ibid.*

² Brown, R., et al. (2022). Robotics and Automation in Crime Scene Investigations: Challenges and Opportunities. *Forensic Science International*, 324, 112.

³ *Ibid.*

⁴ Chen Y., et al. (2021). *Op.Cit.*

⁵ Wang S., et al. (2022). *Op.Cit.*

⁶ Anderson B., et al. (2023). Ethical Implications of AI in Forensic Law: A Critical Analysis. *Journal of Legal Studies in Technology*, 12(4), 48.

⁷ Greenfield, A., et al. (2021). Standardization in AI-Powered forensic Processes. *Science and Justice*, 61(3), 288.

⁸ Silverman, S., et al. (2018). Torts of the Future II: Addressing the Liability and Regulatory Implications of Emerging Technologies. US Chamber for Commerce Institute for Legal Reform, p. 6. Available at [Instituteforlegalreform.com/research/torts-of-the-future-ii-addressing-the-liability-and-regulatory-implications-of-emerging-technologies/](https://www.instituteforlegalreform.com/research/torts-of-the-future-ii-addressing-the-liability-and-regulatory-implications-of-emerging-technologies/) (Lastly Accessed on the 22/04/2026).

⁹ Internet of Things (IoT), "IoT comprises devices and objects whose state can be altered via Internet, with or without the active involvement of individuals. The term goes beyond devices traditionally connected to the Internet, like laptops and smartphones, by including all kinds of objects and sensors that permeate the public space, the workplaces and home."

¹⁰ Gluyas, L., et al. (2018). Who Is Liable When AI Fails to Perform? CMS Cameron McKenna Nabarro Olswang LLP.

considering that instead of a human being, the car was driven by an algorithm.¹ As there is no human driver, the responsible party needs to be established somewhere else, and it could be the owner or the manufacturer of the car, the software designer or at some point maybe even the AI itself. In addition, no one can be blamed without reasons or applicable law, so there is a need for suitable reasoning to hold the party in question liable, and the legislations need to be updated to recognise the liable party regarding the more recent technology. These same aspects are also examined by the point of view of international law and treaties, especially regarding state jurisdiction and responsibility.²

Each AI system poses a negative impact on privacy for the individual at multiple levels. Depending on how it is applied, facial recognition AI systems can essentially create “dragnet biometric databases” that impact both criminal and law-abiding citizens. If applied in a live video feed, then any expectations of privacy or anonymity in public are essentially eroded by the capabilities of a facial recognition system.³ Since there are no current limitations or regulations imposed on this type of technology, law enforcement agencies are not required to submit warrants or justification before usage. For this reason, many municipalities have taken it upon themselves by banning the usage of facial recognition by public agencies within their jurisdiction due to the dangers involved. Facial recognition AI systems are not the only systems with privacy issues. Both predictive risk assessment and predictive policing AI systems have the ability to chip away at privacy expectations and alter Fourth Amendment expectations. As described by **Justice Sotomayer**, the “mosaic theory” could be applied to AI systems in a similar manner to GPS surveillance, as the power of data has grown to the point where intimate details of a person’s habits and preferences can be accurately inferred.⁴ Against this backdrop there, there is the need to establish establishing the liability of AI and robots for forensic and other technological interventions in the situation of misleading conclusive investigations.

2. Regulation Framework of Artificial Intelligence and Robotics in Forensic Investigation in Cameroon

According to the Oxford Advance Learner’s Dictionary, the word regulation carries different meanings. It might be ‘a rule or directive made and maintained by an authority’, in a more strictly governmental sense. However, it might also have a broader sense, meaning ‘the action or process of regulating or being regulated’.⁵ Thus, while regulation has a broader definition, which is the set of parameters and rules that act as a guidance to behaviours, it has numerous connotations that can be used in the most variable ways. The existence of different meanings to regulation, altogether with the different existing personal views about politics and government intervention may cause certain difficulties in understanding it. These difficulties, consequently, have the potential to result in confusion while defining regulation and using the best term for each circumstance.⁶ Therefore, it is indispensable to delimit how the word “regulation” is employed in the context.

The liability of Artificial Intelligence (AI) and Robotics in forensic law raises complex questions about accountability, as traditional legal frameworks struggle to address actions of non-human agents. While Artificial Intelligence (AI) can enhance forensic capabilities, the potential for misuse and harm necessitates a careful examination of who is liable when AI systems act in ways that violate the law. The growth of Artificial Intelligence has been significant within several industrial sectors and is anticipated to grow even more in the

¹ An AI Algorithm refers to a specific set of rules or instructions that a computer system follows to perform tasks that typically require human intelligence. These tasks can include learning, reasoning, problem-solving, perception, and language understanding. Key Characteristics of AI Algorithms; AI algorithms can learn from data. They improve their performance over time by analysing patterns and making predictions based on past experiences; They can adapt to new information or changes in the environment, allowing them to remain effective as conditions evolve; AI algorithms can automate complex decision-making processes, often faster and more accurately than humans; Many AI algorithms can handle vast amounts of data and perform computations that are infeasible for humans to do manually. The Common Types of AI Algorithms: These algorithms enable systems to learn from data. Examples include linear regression, decision trees, and neural networks. A subset of machine learning, these algorithms use neural networks with many layers (deep neural networks) to process complex data structures, such as images and sounds. These algorithms are designed to understand, interpret, and generate human language. Examples include sentiment analysis and machine translation. These algorithms learn by interacting with an environment, receiving feedback in the form of rewards or penalties based on their actions.

² Donald Z. (2000). *Someone to Watch over Me? Privacy and Governance Strategies for CCTV and Emerging Surveillance Technologies*. Master’s Thesis, Naval Postgraduate School. <https://calhoun.nps.edu/handle/10945/4167>. (Lastly Accessed on 16/04/2026).

³ WCPO Statement in Response to New York Times Article Wrongfully Accused by an Algorithm, June 24, 2020. WCPO Press Release. Detroit, MI: County of Wayne, 2020. Woodward, J., et al. (2003). *Biometrics: A Look at Facial Recognition*. Santa Monica, CA: RAND Corporation. <https://apps.dtic.mil/dtic/tr/fulltext/u2/a414520.pdf>.

⁴ *Ibid*.

⁵ The Oxford English Dictionary. (2005). 7th Ed., Oxford, Oxford University Press.

⁶ Barack O. (2012). What Is Regulation? *Yale Journal on Regulation Online*, 30(1), 3-10.

upcoming days.¹ Since, these commercial organizations are looking to adopt the features of artificial intelligence, robotics, and machine learning, it is necessary to stay aware of the laws and regulations associated with these technologies.

Regulations related to the activities of Artificial Intelligence is a phenomenon that governs the policies and laws integrated to the public sector who nurtures, and modulates Artificial Intelligence. A robust debate is evident if Artificial Intelligence can be held liable in the scenario of a machine learning application or robotic automation goes wrong. Regulations behind AI are a complex terrain, but countries like U.S, and other European nations have embraced with regulations considering both the ethical and physical consequences of these technologies.² European Union is one of the major regulatory bodies who are associated with activities and frameworks of laws and regulations connected to Artificial Intelligence. One of the major regulations stated by the European Union is General Data Protection Regulation (GDPR), that enables in protecting the valuable and personal information of the users enhancing the parameters of both safety and privacy of data.

The rapid integration of artificial intelligence (AI) and robotics into forensic law necessitates a robust institutional framework and legal infrastructure. This chapter examines the global, regional, and national institutions and legal instruments regulating AI and robotics in forensic applications. It highlights gaps, overlaps in existing frameworks, and offers insights into their inadequacy in addressing emerging challenges.

2.1 Reasons for Regulation of Artificial Intelligence (AI) and Robotics

Regulation of AI and robotics in forensic investigations is crucial to ensure fairness, accountability, and ethical use, addressing concerns about bias, privacy, and the potential for misuse, while also maintaining the integrity of forensic processes and the role of human experts.³

2.1.1 Ethical Concerns and Potential for Bias

AI algorithms can perpetuate and amplify existing biases present in training data, leading to unfair or discriminatory outcomes in forensic investigations. “Black box” AI systems can be difficult to understand, making it hard to determine how they arrive at their conclusions, which is crucial for ensuring accountability and trust in the forensic process. Biometric data collection and analysis, a common application of AI in forensics, raise significant privacy concerns that need to be addressed through regulation.⁴

2.1.2 Ensuring Reliability and Admissibility of AI-Generated Evidence

Current legal frameworks may not be adequate to address the reliability and admissibility of AI-generated evidence, necessitating the development of new legal standards. AI systems used in forensic investigations must meet rigorous forensic standards for accuracy, reliability, and validity. Over-reliance on AI could undermine the role of human forensic experts, potentially leading to a decline in critical thinking and judgment.⁵

2.1.3 Addressing Potential for Malicious Use

AI and robotics can be used for malicious purposes, such as cyberattacks, the creation of fake news, or the manipulation of video evidence, which can undermine trust in the justice system. Criminals and terrorist groups could leverage AI and robotics to create new digital, physical, or political threats, requiring law enforcement to be prepared to address these challenges. The use of AI and robotics in law enforcement can have a significant social impact, potentially affecting public trust and perceptions of law enforcement agencies.⁶

2.1.4 Ensuring Fairness and Equity

¹ M. Saračević M., A. Selimi., Š. Plojović. (2019). Some Specific Examples of Attacks on Information Systems and Smart Cities Applications, in Hassanien A., Elhoseny M. (eds) *Cybersecurity and Secure Information Systems*. Netherlands, Springer, 45.

² Koos S. (2021). Artificial Intelligence as Disruption Factor in the Civil Law: Impact of the use of Artificial Intelligence in Liability, Contracting, Competition Law and Consumer Protection with Particular Reference to the German and Indonesian Legal Situation. *Yuridika*, 36(1), 235-262.

³ G. Makam. (2023). Criminal Liability of Robots- A Critical Analysis of the Legal Framework in the US, UK, and Europe. O. P. Jindal Global University, Jindal Global Law School (JGLS). Available at SSRN: <https://ssrn.com/abstract=4649764> or <http://dx.doi.org/10.2139/ssrn.4649764> (Lastly Accessed on 07.04.2025).

⁴ Thiruma Valavan. (2023). AI Ethics and Bias: Exploratory Study on the Ethical Considerations and Potential Biases in AI and Data Driven Decision making in Banking, with Focus on Fairness, Transparency and Accountability. *World Journal of Advanced Research and Reviews*, 20(2), 197-206.

⁵ Rwertembula, V. (2024). Legal and Practical Challenges for the Admissibility of Artificial Intelligence. *Evidence in Criminal Proceedings in Mainland Tanzania, East African Journal of Law and Ethics*, 7(1), 136-148.

⁶ *Ibid.*

Unequal access to AI tools between well-funded and underfunded agencies can exacerbate existing disparities in forensic capabilities and potentially widen gaps in justice.¹ Ensuring that AI systems are trained on diverse datasets is crucial to prevent bias and ensure fairness in forensic investigations.

2.1.5 Keeping Pace with Technological Advancements

Law enforcement agencies need to continuously monitor the evolving technology landscape to ensure preparedness for new threats and opportunities related to AI and robotics. Law enforcement agencies should identify and share their needs in terms of AI and robotics to facilitate the development of relevant technologies and projects. Collaboration between law enforcement, researchers, and policymakers is essential to address the challenges and opportunities presented by AI and robotics in forensic investigations.²

2.2 Legal Framework on Artificial Intelligence and Robotics

2.2.1 International Legal Framework

The international legal framework on AI and Robotics seeks to address several key areas such as, Establishing who is responsible when AI systems cause harm or make decisions that lead to negative outcomes, ensuring that AI and robotic systems are safe for users and society, including regulations for testing and compliance, Promoting ethical guidelines for the development and deployment of AI technologies, focusing on fairness, transparency, and non-discrimination, Protecting individuals' privacy rights in the context of data collection and processing by AI system, Ensuring that AI technologies respect and promote human rights, including avoiding biases that could lead to discrimination, Addressing the legal implications of using AI in military applications, particularly concerning autonomous weapon systems, Fostering collaboration among countries to develop harmonized regulations and standards for AI and robotics, and Addressing the socio-economic implications of AI and robotics on the workforce, including job displacement and the need for reskilling. Overall, the framework aims to balance innovation with the protection of fundamental rights and societal interests. However, there are no binding international conventions specifically dedicated to AI or Robotics. This is a significant gap in international law, reflecting the rapidly evolving nature of the technology and the difficulty of achieving consensus among nations on how to regulate it.

a) United Nations Convention on the Use of Electronic Communications in International Contracts

UN Convention called "United Nations Convention on the Use of Electronic Communications in International Contracts", provides a general principle for AI liability. The Convention posits that a person, who can be a natural person or a legal entity, on whose behalf a computer was programmed should ultimately be liable for any message generated by the machine. So even though that convention is not about AI liability per se, there are some excellent principles for it.³

As a whole, Article 12 states:

"A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract."

The meaning of the article is opened up in the Electronic Communications Convention Explanatory note section 213, according to which:

"Article 12 is an enabling provision and should not be misinterpreted as allowing for an automated message system or a computer to be made the subject of rights and obligations. Electronic communications that are generated automatically by message systems or computers without direct human intervention should be regarded as 'originating' from the legal entity on behalf of which the message system or computer is operated. Questions relevant to agency that might arise in that context are to be settled under rules outside the Convention."

As can be seen from this note, electronic systems cannot be held liable, meaning that computers are not seen as legal persons by international law, and so only natural and legal persons can be held responsible or at least they should ultimately be the responsible party. This is because of the general rule that the user of the tool is responsible, as the tool does not have its own will. This is not usually a problem in situations where the owner has acted intentionally or otherwise very carelessly or if the AI product would have had a defect on it in

¹ Ibid.

² NCSL. (2024). Keeping Pace with Rapid Changes in Technology and Communication, National Conference of States Legislatures. Available at <https://www.ncsl.org/> (Lastly Accessed on 26th April, 2025).

³ Article 12 of the United Nations Convention on the Use of Electronic Communications in International Contracts.

manufacturing. The problem might be, however, in events where the AI itself has caused harm, particularly when talking about fully autonomous robots.

The proposal of the UN Convention on the Use of Electronic Communications in International Contracts states that “general principles of agency law (for example, principles involving limitation of liability as a result of the faulty behaviour of the agent) could not be used in connection with the operation of such systems.” Hence, according to the proposal, it could be understood that a robot, as a machine, should be viewed as a tool. Therefore, the user or the manufacturer would be the responsible party when a robot makes a mistake.

b) United Nations Educational Scientific and Cultural Organisation Recommendation on Ethics of Artificial Intelligence 2021¹

UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) is a non-binding but influential framework that aims to provide a global ethical foundation for the development and deployment of Artificial Intelligence (AI). It covers areas such as transparency, accountability, privacy, and human oversight.

Key aspects include:

- **Human Rights Framework:** Emphasis on ensuring AI aligns with human rights, fundamental freedoms, and ethical principles.
- **Multi-stakeholder Approach:** Calls for collaboration among governments, the private sector, civil society, and academia.
- **Areas of Application:** Addresses ethical concerns in areas like education, culture, communication, and information.
- **Monitoring and Evaluation:** Encourages member states to monitor and evaluate the impact of AI technologies.

The UNESCO Recommendation provides a wide range of specific recommendations, organised around key values and principles. The recommendation emphasizes the following core values and principles, which should guide the development and use of AI: Respect for Human Dignity, Human Rights, and Fundamental Freedoms: AI systems should not be used in ways that violate human rights or undermine human dignity. Environment and Ecosystem Flourishing: AI should be developed and used in a sustainable way that protects the environment and promotes biodiversity. Ensuring Diversity and Inclusiveness: AI systems should be designed and used in ways that promote diversity and inclusivity, and avoid discrimination. Living in Peaceful, Just and Interconnected Societies: AI should be used to promote peace, justice, and social cohesion.²

c) The Organisation for Economic Co-operation and Development (OECD) Principles on Artificial Intelligence (2019)

The OECD (Organisation for Economic Co-operation and Development) Principles on AI, adopted in 2019. They are a set of non-binding guidelines intended to promote trustworthy AI that benefits people and the planet. The overall aim of the OECD Principles on AI is to foster the responsible stewardship of trustworthy AI systems, promoting innovation while safeguarding human rights, democratic values, and sustainable development. More specifically, the principles seek to:

- **Promote AI that is Beneficial to People and the Planet:** Encourage the development and use of AI that contributes to inclusive growth, sustainable development, and well-being.
- **Foster Trust in AI:** Build public trust in AI systems by ensuring that they are transparent, explainable, and accountable.
- **Address the Risks of AI:** Identify and mitigate the potential risks associated with AI, such as bias, discrimination, privacy violations, and job displacement.
- **Encourage International Cooperation:** Facilitate international cooperation on AI policy and governance to promote a common understanding and avoid fragmentation.
- **Provide Guidance to Stakeholders:** Offer practical guidance to governments, businesses, researchers, and civil society organizations on how to develop and use AI responsibly.

The Specific Provisions of the OECD contain five Value-Based Principles and Five Recommendations. The OECD Principles consist of five value-based principles for responsible stewardship of trustworthy AI and five recommendations for national policies and international co-operation.

¹ Formerly known as the UNESCO Recommendation on the Ethics of Artificial Intelligence.

² UNESCO. (2021). UNESCO's Recommendation on the Ethics of Artificial Intelligence, Paris, France.

Value-Based Principles for Responsible Stewardship of Trustworthy AI:¹

These principles are intended to guide the development and use of AI systems in a way that aligns with human values and promotes the common good.

a. AI should benefit people and the planet by driving inclusive growth, sustainable development and well-being

The AI should be used to address societal challenges, such as poverty, inequality, climate change, and healthcare, while promoting economic growth and improving the quality of life for all. Implication: Encourages AI applications in areas like renewable energy, precision agriculture, and personalized medicine.²

b. AI systems should be designed in a way that respects human rights, fundamental freedoms, and democratic values³

The AI should not be used to discriminate against individuals or groups, violate privacy, or undermine democratic processes. Promotes the development of AI systems that are fair, transparent, and accountable.

c. AI systems should be transparent and explainable

Users should be able to understand how AI systems work and why they make certain decisions. This includes providing access to information about the data used to train AI systems and the algorithms they employ. Encourages the development of explainable AI (XAI) techniques and the implementation of transparency mechanisms.⁴

d. AI systems should be robust, secure, and safe throughout their lifecycle

AI systems should be designed to be reliable, resilient, and resistant to attacks. They should also be regularly tested and monitored to ensure that they are functioning as intended. Emphasizes the importance of cybersecurity, data security, and safety engineering in the development of AI systems.⁵

e. AI actors should be accountable for the proper functioning of AI systems

There should be clear lines of responsibility for the design, development, and deployment of AI systems. This includes establishing mechanisms for redress when AI systems cause harm. Promotes the development of legal and ethical frameworks that address liability for AI-related incidents.⁶

2.2.1.1 National Policy Recommendations (Recommendations for Governments)⁷

These recommendations provide guidance to governments on how to create an enabling environment for the responsible development and use of AI

a. Invest in AI research and development

Governments should invest in basic and applied research on AI, as well as in the development of AI infrastructure and talent. Supports public funding for AI research, scholarships for AI students, and the creation of AI hubs and centers of excellence.⁸

b. Foster a digital ecosystem for AI

Governments should promote access to data, infrastructure, and talent that are necessary for the development and deployment of AI. Encourages open data initiatives, the development of high-speed internet access, and the promotion of digital literacy.⁹

c. Shape an enabling policy environment for AI

Governments should create a regulatory environment that supports innovation while mitigating the risks of AI. This includes addressing issues such as data privacy, algorithmic bias, and liability. Promotes the development of

¹ Section 1 on the OECD Recommendation of the Council on Artificial Intelligence.

² *Ibid*, Section1(1).

³ *Ibid*, Section1(2).

⁴ *Ibid*, Section1(3).

⁵ Section 1(4) on the OECD Recommendation of the Council on Artificial Intelligence.

⁶ *Ibid*, Section1(5).

⁷ *Ibid*, Section 2.

⁸ *Ibid*, Section 2(1).

⁹ *Ibid*, Section 2(2).

AI-specific regulations, as well as the adaptation of existing laws to address the challenges posed by AI.¹

d. Build human capacity and prepare for labour market transformation

Governments should invest in education and training programs to prepare workers for the changing labour market. Supports lifelong learning, reskilling initiatives, and the development of new curricula that focus on AI-related skills.²

e. International co-operation for trustworthy AI

Governments should work together to promote a common understanding of AI ethics and governance, and to avoid fragmentation of the global AI ecosystem. Encourages the development of international standards for AI, the sharing of best practices, and collaboration on AI research.³

The OECD Principles on AI provide a comprehensive framework for promoting the responsible development and use of AI. While non-binding, they have been influential in shaping AI policy and governance around the world. They emphasize the importance of aligning AI with human values, promoting trust in AI systems, and addressing the risks associated with this transformative technology. The principles serve as a valuable guide for governments, businesses, and other stakeholders who are working to ensure that AI benefits people and the planet.

d) United Nations and Artificial Intelligence Governance

The United Nations (UN) has been increasingly focused on the governance of artificial intelligence (AI) to ensure that its development and deployment align with global values and human rights. Here are some key objectives and specific provisions related to AI governance:

The objectives of AI governance among others include:

- **Promote Human Rights:** Ensure that AI technologies respect and promote human rights, including privacy, non-discrimination, and freedom of expression.
- **Sustainable Development:** Align AI initiatives with the Sustainable Development Goals (SDGs), leveraging AI for economic growth, education, health, and environmental sustainability.
- **Global Cooperation:** Foster international collaboration in AI research and development, addressing cross-border challenges and sharing best practices.
- **Ethical Standards:** Establish ethical frameworks to guide the responsible development and use of AI, ensuring transparency, accountability, and fairness.
- **Risk Mitigation:** Identify and mitigate risks associated with AI, including bias, misinformation, and potential job displacement.

The specific provisions of the United Nation on AI governance include;

- **Multi-stakeholder Approaches:** Encourage participation from governments, private sector, civil society, and academia in shaping AI governance frameworks.
- **Regulatory Frameworks:** Develop guidelines and policies that govern AI technologies, including data protection laws and regulations on AI applications in critical sectors.
- **Capacity Building:** Support member states in building capacity for AI governance, including training for policymakers and stakeholders on ethical AI practices.
- **Monitoring and Accountability:** Implement mechanisms for monitoring AI deployment and its impacts, ensuring accountability for misuse or harmful consequences.
- **Research and Development:** Promote research on the societal impacts of AI and invest in initiatives that prioritize human-centric AI technologies.

There are 5 underlying principles under the United Nation and Artificial Intelligence Governance. These principles are as follows:

- AI should be governed inclusively, by and for the benefit of all;⁴
- AI must be governed in the public interest;⁵

¹ Section 2(3) on the OECD Recommendation of the Council on Artificial Intelligence.

² *Ibid*, Section 2(4).

³ *Ibid*, Section 2(5).

⁴ Guiding principle 1 of the United Nations and Artificial Intelligence Governance.

- AI governance should be built in step with data governance and the promotion of data commons;¹
- AI governance must be universal, networked and rooted in adaptive multi-stakeholders' collaboration;²
- AI governance should be anchored in the Charter of the United Nations, International human rights law and other agreed international commitments such as Sustainable development Goals.³

The UN's approach to AI governance aims to create a balanced framework that maximizes the benefits of AI while minimizing risks, ensuring that technology serves humanity as a whole.

e) The Vienna Convention on Road Traffic (Vienna, 8 November 1968)

The Vienna Convention on Road Traffic was adopted in 1968 to establish uniform traffic rules and promote road safety internationally. It serves as a framework for countries to harmonize their traffic regulations and improve cross-border vehicle operation.⁴ The objective of this Convention is to reduce accidents and improve safety for all road users, create common traffic laws to facilitate international road traffic and encourage collaboration among countries in traffic management and road safety among others.

While the original convention does not specifically address AI and robotics, several areas within its framework are relevant to the integration of these technologies by stating guidelines for the technical requirements of vehicles, which can include autonomous and AI-driven systems; Provisions regarding the responsibilities of drivers may need updating to account for automated driving systems and the role of AI; Adaptations for AI systems that communicate with traffic signals and infrastructure to improve traffic flow and safety; Regulations concerning the collection and use of data from autonomous vehicles, ensuring privacy and security; Addressing liability in accidents involving automated vehicles, especially in determining the accountability of manufacturers, software developers, and users; Guidelines for the safe testing and deployment of AI-driven vehicles on public roads.

The auto industry is already designing driverless cars, powered by Artificial Intelligence. Despite its imminent deployment, fully autonomous cars are still not allowed, due to the Vienna Convention on Road Traffic, ratified by most European states.⁵ According to this convention, a car needs a human driver to be allowed in the streets. The Regulation No. 79 of the UN/ECE also does not authorise autonomous steering systems. Moreover, many countries, in their national laws, require the driver to always have his hands on the steering wheel, and even require the human driver to be in primary control.

As AI and robotics continue to evolve in the transportation sector, the Vienna Convention may require amendments or supplementary protocols to effectively govern these technologies while maintaining safety and efficiency on the roads.

2.2.2 Regional Legal Instruments

The main regional instrument relevant to this work is the Bangui Agreement of 1977 (Revised in 1999) on Intellectual Property. Cameroon's intellectual property regime is primarily governed by the Bangui Agreement of 1977, revised in 1999, which is administered by the African Intellectual Property Organization.⁶ Cameroon is a member of OAPI, and the Bangui Agreement serves as the basis for IP⁷ protection within the country.

The overarching objectives of the intellectual property framework administered by OAPI and applicable in Cameroon include:

- Protecting Intellectual Creations: To provide legal protection for various forms of intellectual property, such as patents, trademarks, industrial designs, and copyrights.
- Promoting Innovation and Creativity: To incentivize innovation and creativity by granting exclusive rights to creators and inventors, allowing them to benefit from their intellectual endeavours.
- Encouraging Investment: To foster investment in research and development by providing a secure legal framework for protecting intellectual assets.

⁵ *Ibid*, Guiding Principle 2.

¹ *Ibid*, Guiding Principle 3.

² *Ibid*, Guiding principle 4.

³ Guiding principle 5 of the United Nations and Artificial Intelligence Governance

⁴ The Vienna Convention on Road Traffic (Vienna, 8 November 1968) 1042 U.N.T.S. 17, entered into force 21 May 1977, Articles 8 & 13.

⁵ *Ibid*.

⁶ Abbreviated formerly as OAPI.

⁷ IP refers in the context of this work refers to as Intellectual Property.

- **Facilitating Technology Transfer:** To promote the transfer of technology and knowledge by encouraging the disclosure and commercialization of inventions.
- **Harmonizing IP Laws:** To harmonize intellectual property laws across OAPI member states, creating a consistent and predictable legal environment.
- **Contributing to Economic Development:** To contribute to economic growth and development by promoting innovation, attracting investment, and facilitating trade.

While the Bangui Agreement doesn't explicitly address AI (as it predates the current AI boom), several areas of IP law are highly relevant to AI-related inventions, creations, and technologies:

a. Patents

Patents protect new inventions.¹ AI-related inventions, such as novel algorithms, AI architectures, or AI-enhanced devices, can be patented if they meet the patentability criteria (novelty, inventiveness/non-obviousness, and industrial applicability). The challenges here may include Patenting AI inventions can be complex, difficult to assess whether an AI invention is truly "inventive" or simply a routine application of existing techniques. Software Patentability, that software patentability is often subject to stricter scrutiny than hardware patents, AI-Generated Inventions, A key debate, can an AI itself be listed as an inventor on a patent? Most jurisdictions (including those guided by the Bangui Agreement's principles) currently require human inventors.

b. Copyright²

Copyright protects original works of authorship, such as software code, databases, and creative content. Copyright in AI-Generated Works as a challenge may bring about a major question as to who owns the copyright to works created by AI? Is it the programmer, the user, or the AI itself (which is generally not recognized)? Many jurisdictions are grappling with this. If the AI is merely a tool used by a human, copyright likely vests in the human author. However, if the AI operates more autonomously, then the situation is less clear. Another challenge here is training Data. Copyright issues can arise from the use of copyrighted material to train AI systems. Fair use or exceptions for research may apply, but this is a complex area.

c. Trade Secrets³

Trade secrets protect confidential information that gives a business a competitive edge. AI algorithms, training data, and other proprietary AI-related information that may be protected as trade secrets. Trade secret protection does not require registration and can last indefinitely, as long as the information remains confidential. The major challenge here is Trade Secrets are vulnerable to misappropriation. Once the information is disclosed, it loses its trade secret status.

d. Industrial Designs⁴

Industrial designs protect the ornamental or aesthetic aspects of an article. This could be relevant to the design of AI-powered devices or robots.

The challenges generally with the Bangui Agreement on IP are enormous. Some of them include, Lack of Specific AI Provisions. The Bangui Agreement does not specifically address AI, which creates uncertainty about how existing IP laws apply to AI-related inventions and creations. Another challenge is enforcement difficulties. Enforcing IP rights in AI can be difficult due to the complexity of AI systems, the global nature of the technology, and the challenges of detecting infringement. In addition, there is adaptability issues. The IP system needs to adapt to the rapid pace of innovation in AI to ensure that it effectively protects and incentivizes creativity and investment. Again, there is human Authorship/Inventorship Requirement. The current IP system is largely based on human creation. The increasing autonomy of AI raises questions about whether and how AI can be recognised as an author or inventor.

The intellectual property framework in Cameroon, based on the Bangui Agreement, provides a foundation for protecting AI-related inventions and creations. Patents, copyrights, and trade secrets are all potentially relevant to AI. However, the lack of specific AI provisions in the existing IP laws creates uncertainty and highlights the need for further legal developments. As AI becomes more prevalent, Cameroon (and OAPI as a whole) may need to adapt its IP system to address the unique challenges posed by AI, particularly in areas such as AI-generated

¹ Article 1(4) of the Revised Bangui Agreement.

² *Ibid.*

³ *Ibid.*

⁴ *Ibid.*

works, data protection, and the definition of inventorship. This may involve updating the Bangui Agreement or issuing guidelines on how existing IP laws apply to AI-related innovations.

2.2.3 The National Legal Framework on Artificial Intelligence and Robotics in Cameroon

It should be noted that there is no specific national law in Cameroon regulating Artificial Intelligence and Robotics. There are existing laws that touches aspects that are somewhat related to AI regulation.

a) The Law No. 2010/021 of 21 December 2010 on the Protection of Persons with regard to the Processing of Personal Data

Cameroon has been proactive in developing its legal framework for data protection, particularly with the increasing importance of data privacy in the context of digital technologies like AI. Here is an overview of the law on data protection in Cameroon, focusing on its general objectives and provisions relevant to AI. The primary legal framework governing data protection in Cameroon is the Law No. 2010/021 of 21 December 2010 on the Protection of Persons with regard to the Processing of Personal Data. This law shall herein after referred simply to as “The Data Protection Law”.

The general objectives of the Data Protection Law in Cameroon include:

- **Protection of Privacy:** To safeguard the privacy of individuals by regulating the collection, processing, storage, and dissemination of personal data.
- **Rights of Data Subjects:** To establish and protect the rights of individuals (data subjects) regarding their personal data.
- **Regulation of Data Processing:** To provide a legal framework for the lawful processing of personal data by public and private entities.
- **Promotion of Transparency:** To ensure transparency in data processing activities, allowing individuals to know how their data is being used.
- **Accountability:** To hold data controllers and processors accountable for their data processing activities and to establish mechanisms for redress in case of violations.
- **Compliance with International Standards:** To align national data protection practices with international standards and best practices.¹

While the Data Protection Law does not explicitly mention AI, several provisions are relevant to the use of AI technologies, particularly concerning the processing of personal data. Here are some key provisions related to AI:

i. Consent:

Personal data must be collected and processed only with the consent of the data subject, except in specific cases defined by law. This means that for AI systems that process personal data, obtaining informed consent is essential.²

ii. Purpose Limitation:

Data collected for a specific purpose must not be processed in a manner incompatible with that purpose. This is particularly relevant for AI systems that utilize personal data for machine learning and predictive analytics, as they must adhere to the original purpose for which the data was collected.³

iii. Data Minimization:

Data controllers should only collect personal data that is necessary for the intended purpose. AI systems should therefore be designed to minimize the amount of personal data processed.⁴

iv. Data Security:

Data controllers are required to implement appropriate technical and organizational measures to ensure the security of personal data. This includes protecting data used in AI systems from unauthorized access, breaches, and cyberattacks.⁵

¹ Section 1 The Law No. 2010/021 of 21 December 2010 on the Protection of Persons with regard to the Processing of Personal Data.

² *Ibid*, Section 5.

³ Article 6 of Law No. 2010/021 of 21 December 2010 on the Protection of Persons with regard to the Processing of Personal Data.

⁴ *Ibid*, Article 7.

⁵ *Ibid*, Article 8.

v. Rights of Data Subjects:

The law grants data subjects' various rights, including:

- Right to Access: Individuals have the right to access their personal data.
- Right to Rectification: Individuals can request the correction of inaccurate personal data.
- Right to Erasure: Individuals can request the deletion of their personal data under certain conditions.
- Right to Object: Individuals can object to the processing of their personal data, particularly in cases of automated decision-making.¹

vi. Data Protection Impact Assessments (DPIAs):

While not explicitly stated in the law, the use of AI systems that process personal data may necessitate conducting DPIAs to assess the impact of data processing activities on individuals' privacy and rights.

vii. Cross-Border Data Transfers:

The law regulates the transfer of personal data outside Cameroon, requiring that adequate protection measures are in place to ensure that data subjects' rights are upheld. This is particularly relevant for AI systems that may operate across borders.²

viii. Establishment of a National Data Protection Authority:

The law establishes a data protection authority responsible for overseeing compliance, promoting awareness, and enforcing data protection rights. This authority plays a crucial role in ensuring that AI systems processing personal data adhere to the legal framework.

Cameroon's Data Protection Law provides a comprehensive framework for the protection of personal data, with several provisions that are relevant to the development and deployment of AI systems. While the law does not specifically address AI technologies, the principles of data protection, including consent, purpose limitation, data minimization, and security, are essential for ensuring that AI is used responsibly and ethically. As AI continues to evolve, there may be a need for further legal developments in Cameroon to address the unique challenges and ethical considerations associated with AI technologies.

b) Law No. 2010/012 of 21 December 2010 Relating to Cybersecurity and Cybercrime in Cameroon

The primary legislation concerning cybersecurity in Cameroon is Law No. 2010/012 of 21 December 2010 Relating to Cybersecurity and Cybercrime in Cameroon. This law establishes a legal framework to combat cybercrime, protect critical infrastructure, and promote cybersecurity.

The overarching goals of the Cybersecurity Law in Cameroon include:

- Combating Cybercrime: To define and criminalize various cyber offenses, such as hacking, fraud, identity theft, and cyberterrorism.
- Protecting Critical Infrastructure: To ensure the security and resilience of critical information infrastructure, including government networks, financial systems, and essential services.
- Promoting Cybersecurity: To encourage the adoption of cybersecurity best practices and promote awareness among citizens and organizations.
- Facilitating Investigation and Prosecution: To provide law enforcement agencies with the necessary powers and tools to investigate and prosecute cybercrimes effectively.
- International Cooperation: To foster cooperation with other countries and international organizations in the fight against cybercrime.³

While the Cybersecurity Law does not explicitly mention AI (as it predates the widespread adoption of AI technologies), several provisions can be interpreted as relevant to the security of AI systems and the misuse of AI for cybercrime:

i. Offenses Against Information Systems:

The law defines various cyber offenses, such as unauthorized access to computer systems, data interference, and system interference. AI systems, if compromised, could be used to commit these offenses. For example, a hacked

¹ *Ibid*, Articles 9-12.

² Article 14 of Law No. 2010/021 of 21 December 2010 on the Protection of Persons with regard to the Processing of Personal Data.

³ Section 1 of Law No. 2010/012 of 21 December 2010 Relating to Cybersecurity and Cybercrime in Cameroon.

AI system could be used to launch denial-of-service attacks or steal sensitive data.¹

ii. Data Protection and Privacy (Related to Law No. 2010/021, as mentioned before):

While the Cybersecurity Law mainly focuses on criminal aspects, it intersects with data protection principles. AI systems often process large amounts of data, including personal data. Breaches of AI systems could lead to violations of data protection laws, resulting in penalties for the organization responsible for the AI.

iii. Critical Infrastructure Protection (Implied):

Although not explicitly stated, AI is increasingly being used in critical infrastructure, such as power grids, transportation systems, and healthcare. The provisions aimed at protecting critical infrastructure could be interpreted to include measures to secure AI systems used in these sectors.

iv. Digital Evidence (Provisions related to investigation):

The law empowers law enforcement agencies to collect and use digital evidence in cybercrime investigations. This is relevant to AI-related incidents, where digital evidence from AI systems may be crucial in determining the cause of the incident and identifying the perpetrators. For example, log files from an AI-powered security system could be used to investigate a security breach.²

v. Cyberterrorism and National Security (Articles addressing threats to national security):

The law addresses cyberterrorism and other cyber activities that threaten national security. AI systems, if misused, could be employed for malicious purposes, such as spreading disinformation, launching cyberattacks against government institutions, or disrupting critical services. The Cybersecurity Law does not specifically address the unique challenges posed by AI, such as the potential for algorithmic bias, the difficulty of attributing responsibility for AI-related incidents, and the need for specialized expertise in AI forensics. This aspect brings about some limitations such as;

- **Enforcement Challenges:** Enforcing cybersecurity laws against AI-related cybercrimes can be challenging due to the complexity of AI systems, the difficulty of tracing malicious activities, and the lack of trained personnel.
- **Adaptability:** Given the rapid evolution of AI technologies, the existing cybersecurity law may need to be updated to address emerging threats and vulnerabilities.

Cameroon's Cybersecurity Law provides a general legal framework for combating cybercrime and protecting critical infrastructure. While the law does not explicitly address AI, several provisions can be interpreted as relevant to the security of AI systems and the misuse of AI for malicious purposes. However, there is a need for further legal developments to address the unique challenges posed by AI, particularly in areas such as liability, algorithmic bias, and AI forensics. As AI becomes more prevalent, it is essential for Cameroon to adapt its legal and regulatory framework to ensure that AI is used responsibly and securely.

c) Law No. 2011/012 of 6 May 2011 on Consumer Protection in Cameroon

The primary legislation protecting consumers in Cameroon is Law No. 2011/012 of 6 May 2011 on Consumer Protection in Cameroon. This law aims to safeguard the rights of consumers and promote fair trade practices.³ The overarching goals of the Consumer Protection Law in Cameroon include:

- **Protecting Consumer Rights:** To define and protect the fundamental rights of consumers, such as the right to safety, information, choice, and redress.
- **Promoting Fair Trade Practices:** To ensure that businesses engage in fair and ethical trade practices, avoiding deceptive, misleading, or abusive conduct.
- **Ensuring Product Safety:** To establish standards for product safety and quality, protecting consumers from hazardous or defective goods and services.
- **Providing Redress Mechanisms:** To provide consumers with effective mechanisms for resolving disputes and seeking redress when their rights have been violated.
- **Promoting Consumer Education:** To educate consumers about their rights and responsibilities, enabling them to make informed purchasing decisions.

While the Consumer Protection Law does not explicitly mention AI (reflecting its enactment before AI's widespread consumer use), several provisions can be applied to AI-related products and services:

¹ *Ibid*, Sections 14 - 24 of Law.

² Section 7 of Law No. 2010/012 of 21 December 2010 Relating to Cybersecurity and Cybercrime in Cameroon.

³ Article 1 of Law No. 2011/012 of 6 May 2011 on Consumer Protection in Cameroon.

Right to Information

The law guarantees consumers the right to accurate, clear, and complete information about goods and services. This is crucial for AI products. For instance, consumers should be informed about: the capabilities and limitations of an AI-powered product; how the AI system collects and uses data; potential biases or risks associated with the AI system and the level of human oversight involved (if any).¹

Product Safety and Quality

The law ensures that goods and services meet reasonable standards of safety and quality. This is particularly important for AI systems used in safety-critical applications, such as self-driving vehicles or medical devices. Consumers should be protected from harm caused by defective or malfunctioning AI systems.²

Liability for Defective Products (General principles applied)

Although the law doesn't have explicit clauses on AI liability, general product liability principles can be applied. Manufacturers and providers of AI products could be held liable for damages caused by defects in their products, even if those defects are due to algorithmic errors or unforeseen behaviour of the AI system.

Misleading or Deceptive Practices

The law prohibits businesses from engaging in deceptive or misleading practices. This is relevant to AI, where companies might overstate the capabilities of their AI products or fail to disclose important limitations. For example, claiming that an AI system is "100% accurate" when it is known to have a certain error rate would be a violation of this provision.³

Protection Against Unfair Contract Terms

This article protects consumers from unfair or abusive contract terms. AI-related contracts (e.g., terms of service for an AI-powered platform) must be fair and transparent, avoiding clauses that unduly favour the service provider or limit the consumer's rights.⁴

Right to Redress

Consumers have the right to seek redress (For example, compensation, repair, replacement) if they have been harmed by a defective product or service. This applies to AI as well. If an AI system causes financial loss, physical harm, or other damages, consumers should have access to effective mechanisms for seeking compensation.⁵

Challenges and Limitations of the consumer protection law in relation to Artificial intelligence and robotics are enormous such as lack of AI-Specific Provisions: The law does not explicitly address the unique challenges posed by AI. This makes it difficult to apply the law to complex AI-related scenarios; secondly, enforcing consumer protection laws against AI-related violations can be challenging due to the technical complexity of AI systems and the difficulty of determining causality; awareness and education, as many consumers may not be aware of their rights in relation to AI products and services. Increased consumer education is needed to promote informed decision-making.

Cameroon's Consumer Protection Law provides a foundation for protecting consumers from harm caused by defective or misleading AI products and services. While the law needs to be updated to explicitly address the unique challenges posed by AI, existing provisions can be applied to promote transparency, accountability, and fairness in the AI marketplace. As AI becomes more pervasive, it is essential for Cameroon to strengthen its consumer protection framework to ensure that consumers are adequately protected from the risks associated with this transformative technology. This might involve developing new regulations specifically tailored to AI or issuing guidelines on how existing consumer protection laws apply to AI-related products and services.

d) Law No 2016/007 of 12 July 2016 relating to the Cameroon Penal Code

The Code is a crucial legal instrument that defines criminal offenses and the corresponding penalties.⁶ The Code clearly established that all persons who commit an offence in the country will be subjected to the provisions of

¹ Article 4 of Law No. 2011/012 of 6 May 2011 on Consumer Protection in Cameroon.

² *Ibid.* Article 6.

³ Article 8 of Law No. 2011/012 of 6 May 2011 on Consumer Protection in Cameroon.

⁴ *Ibid.*, Article 9.

⁵ *Ibid.*, Article 11.

⁶ Section 21 of the Penal Code classifies offences into Felonies, Misdemeanours and simple offences.

the law.¹ It relates to the relevance of AI evidence in criminal proceedings by framing the context within which crimes are defined and prosecuted. AI evidence can play a significant role in clarifying offenses, supporting investigations, and establishing intent, all of which are essential for fair judicial outcomes.²

The Code outlines specific offenses that AI evidence may help to clarify or prove, such as fraud, cybercrime, or other related offenses. AI-generated evidence, like data analysis or predictive algorithms, can be directly relevant in establishing elements of these crimes.³ AI may well be used as digital evidence for proving offenses committed under the Penal Code. Given that the Penal Code addresses various crimes that may involve technology (e.g., theft, fraud), AI evidence can be crucial in investigations. For instance, AI tools used for digital forensics may analyze electronic communications or financial transactions to uncover criminal activity.⁴

In so far as the question of intent and mental state is concerned,⁵ AI evidence plays a critical role clarifying offenses, supporting investigations, and establishing intent, all of which are essential for establishing the guilt or innocence of the accused. In many offenses, establishing the intent of the accused is crucial. AI systems can analyze behavior patterns or historical data, providing insights into the accused's actions and intentions, thus making AI evidence relevant to determining guilt.⁶

AI technologies can assist law enforcement agencies in collecting and processing evidence related to crimes defined in the code. This includes identifying suspects through data analysis, which can help ensure that relevant evidence is presented in court. The Code emphasizes the rights of individuals accused of crimes. AI evidence must be presented in a way that ensures fairness and does not infringe on these rights, thereby affecting its relevance in judicial proceedings.

3. The Setbacks in Artificial Intelligence Regulatory Framework

Artificial Intelligence (AI) regulatory setbacks refer to the challenges and obstacles faced in creating or enacting effective laws and guidelines for Artificial Intelligence and Robotics. Some of these challenges will be discussed in the subsequent paragraphs below.

3.1 Bias in Data and Algorithms

AI algorithms are only as unbiased as the data they are trained on, and this can lead to biased outcomes. The data used to train AI algorithms can be personal, including historical discrimination and societal prejudices. Partial data can lead to narrow results, which can have severe consequences in the legal industry. For example, AI algorithms that predict case outcomes may be biased against specific demographics, leading to unfair results. Similarly, AI algorithms used for document review may only accept relevant information if it fits preconceived notions of what is essential. AI algorithms are only as unbiased as the data they are trained on. If the data used to train AI algorithms is biased, the algorithms will also be limited. In the legal industry, this can lead to discriminatory outcomes in cases, which can perpetuate systemic biases and injustice.⁷ Ensuring that the data used to train AI algorithms is representative and unbiased is crucial to address this issue.

3.2 Limited Scope

Another legal limitation is that AI is often only adequate for specific legal tasks. For example, AI-powered legal research tools may be excellent at finding relevant case law. Still, they may need to provide a different level of insight into the nuances of legal precedent than a human legal researcher could. Similarly, while AI-powered document review tools can be very effective at analysing large volumes of documents, they may need to be able to identify the same level of detail and nuance as a human reviewer.⁸

3.3 Lack of Context

¹ *Ibid.* Section 1(1).

² Handa, S et al. (2024). Role of AI in Admissibility of Electronic Evidence. *International Journal of Research Publication and Reviews*, 5(11), 1323-1238.

³ Dunsin, D., et al. (2024). A comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response. Available at <<https://www.sciencedirect.com>> (Lastly accessed 28th March 2025).

⁴ Quezada, K., et al. (2021). Legal Challenges in Bringing AI Evidence to the Criminal Courtroom. *East African Journal of Law and Ethics*, 4(2), 1-20.

⁵ Section 74 of the Penal Code.

⁶ Dory A. (2020). Courts and Artificial Intelligence. *International Journal for Court Administration*, 11(2), 1-10.

⁷ Ishan A. (2023). Revolutionising the Legal Industry: The Intersection of Artificial Intelligence and Law. *International Journal of Law Management & Humanities*, 6(3), 1083.

⁸ Ishan A. (2023). *Op. Cit*, note 205.

AI algorithms can only work with the data they are given, and they may only sometimes be able to understand the context in which that data is presented. This can be particularly problematic in legal contexts, where the meaning of a term or phrase can vary depending on the specific legal context. With a human understanding of that context, AI algorithms may be able to analyse and interpret legal documents accurately.¹

3.4 Lack of Transparency

One of the significant drawbacks of AI in law is the need for more transparency in how AI algorithms make decisions. AI algorithms are often considered black boxes, meaning it is difficult to understand how they arrived at a particular conclusion. This lack of transparency can make it challenging to identify and correct errors or biases in the system. Moreover, it can make it difficult for legal professionals to explain the reasoning behind a particular decision to their clients.²

3.5 Cost and Accessibility

While AI technology can help reduce costs in the legal industry, it can also be expensive to implement. Small law firms and individual practitioners may not have the resources to invest in AI technology, making it less accessible to those who need it most. Moreover, AI-powered legal services may not be available in all areas or for all legal issues, further limiting accessibility.

3.6 Data Security

Another significant drawback of using AI in the legal industry is the potential for data breaches and other security concerns. Legal professionals handle sensitive and confidential information, and any data breaches could have severe legal and financial consequences. AI tools used in the legal industry must be adequately secured, and appropriate security measures must be implemented to protect sensitive data.³

3.7 Ethical Concerns

There are several ethical concerns associated with using AI in law. For example, AI algorithms may be used to predict the likelihood of a person committing a crime, which raises questions about privacy and the presumption of innocence. Similarly, using AI in hiring decisions may lead to discriminatory outcomes. The legal industry must carefully consider these ethical concerns when implementing AI technology.⁴

3.8 The Almost Complete Absence of Local Laws on AI and Robotics in Cameroon

Within the context of laws enacted in Cameroon, there is not specific laws purposely on the regulation of Artificial intelligence and Robotics, given that the concept is still new. This has rendered liability of AI and Robotics almost impossible. Some provisions could be inferred from the law on Data Protection, Consumer Protection as well as the Cyber Security laws. However, imputing criminal liability is will be challenging since there is no clear legal provisions on AI and Robotics.

4. Conclusion and Recommendations

This article has attempted to do something simple but necessary: to ask honestly whether Cameroon's legal system is equipped to handle the arrival of artificial intelligence and robotics in the domain of forensic law. The answer, on the evidence reviewed, is that it is not-at least not yet. This is not a criticism of Cameroon's legal tradition, which is rich and adaptive. It is rather a recognition that the country stands at a genuinely historic crossroads, and that the choices made now about how to govern these technologies will shape the quality of justice for years to come. Based on the above findings, the following recommendations were made:

▪ Collaboration of Legal Expert and Academia

Collaborating with legal experts and academic institutions is essential for the effective development of AI regulations. Here are some recommendations for fostering this collaboration:

Create task forces that include legal experts, AI researchers, ethicists, and industry leaders to address the complexities of AI regulation. Encourage university-led research projects that focus on the implications of AI technologies, ensuring that findings are accessible to policymakers. Organize events that bring together stakeholders from law, technology, and academia to discuss regulatory challenges and solutions.

Create interdisciplinary courses that combine law, ethics, and AI technology, preparing future professionals to navigate regulatory landscapes. Involve legal experts and academics in public consultations to gather diverse

¹ *Ibid.* p. 1084.

² *Ibid.*

³ *Ibid.* p. 1328.

⁴ *Ibid.* p. 1329.

perspectives on proposed regulations. Collaborate on developing guidelines that outline best practices for AI development and deployment, ensuring compliance with legal standards. Work with international bodies to harmonize AI regulations, ensuring that legal frameworks can adapt to global technological advancements.

By leveraging the expertise of legal professionals and academic institutions, regulators can create a more robust and adaptable framework for AI governance, fostering innovation while protecting public interests.

▪ **Establish Platforms for Regulatory Discuss & Knowledge sharing**

Establishing a platform for regulatory discussion and knowledge sharing on AI can facilitate collaboration among stakeholders and enhance the development of effective regulations. Ensure accessibility for diverse users, including policymakers, legal experts, technologists, and the public, create topic-specific forums for in-depth discussions on various aspects of AI regulation, include a repository of research papers, case studies, and legal documents related to AI. Invite members from academia, industry, government, and civil society to join the platform. Form panels of experts to address specific regulatory challenges and provide insights.

Host regular webinars featuring experts discussing current trends and challenges in AI regulation, through the organisation of workshops for hands-on collaboration on regulatory frameworks and best practices. Encourage sharing of real-world case studies to illustrate the impact of regulations. Develop and disseminate best practice guidelines for AI development and governance.

Implement tools for gathering feedback from users regarding regulatory proposals and platform functionality. Allow users to comment on discussions and documents, fostering a collaborative atmosphere. Partner with universities for research contributions and to involve students in regulatory discussions. Engage with AI companies to understand practical implications and challenges of regulations. Regularly assess the platform's effectiveness in facilitating discussions and knowledge sharing. Adaptation be prepared to evolve the platform based on user feedback and changing regulatory landscapes. By establishing a comprehensive platform for regulatory discussion and knowledge sharing, stakeholders can work collaboratively to navigate the complexities of AI regulation, ensuring that policies are informed, effective, and adaptable to future developments.

▪ **Advocating for the Creation and Adoption of legal Frameworks and Ethical considerations**

Advocating for the creation and adaptation of legal frameworks and ethical considerations involves promoting the development and modification of laws and guidelines that govern the use of technology, particularly AI. Advocating for the development of new laws that specifically address the unique challenges posed by AI technologies. Promoting standards that ensure AI systems are safe, transparent, and accountable.

Encouraging revisions to current laws to better reflect the realities of AI and its impact on society. Supporting legal frameworks that can evolve with technological advancements, ensuring they remain relevant and effective.

Highlighting the importance of ethical principles in the development and deployment of AI, such as fairness, privacy, and non-discrimination. Advocating for the inclusion of diverse perspectives in ethical discussions, ensuring that various societal interests are represented.

Raising awareness about the implications of AI technologies and the need for robust legal and ethical frameworks. Engaging with lawmakers and regulators to advocate for policies that prioritize ethical considerations in AI development.

Overall, advocating for the creation and adaptation of legal frameworks and ethical considerations aims to ensure that AI technologies are developed and used responsibly, protecting public interests while fostering innovation.

▪ **The Application of the Application of Res Ipsa Loquitur for Criminal Liability**

Res ipsa loquitur is useful in dealing with cases where there are multiple successive inexplicable failures which cannot in themselves be readily explained. It remains to be seen whether the principles of *res ipsa loquitur* will be used by modern courts to conclude that the car (or other automated device), not the driver/operator, is at fault. Defendants will argue that the doctrine should not apply when it is unreasonable to infer that the accident was caused by a design or manufacturing defect, or when the accident in question is not one ordinarily seen with design defects.

A classic example of the application of this was in the US case of *Adam v. Toyota Motor Corporation*,¹ where Toyota found that for no particular reason, many of its high-end Lexus model cars simply accelerated – despite

¹ *Adams v. Toyota Motor Corp.* [2017], No. 15-2507, decided by the Eighth Circuit in 2017. This case arose from an accident that resulted in fatalities and injuries, leading to a lawsuit against Toyota for various claims related to unintended acceleration in Toyota Camrys. The jury found Toyota to be 60 percent at fault for the collision. The court addressed several issues, including the admissibility of evidence regarding similar incidents and the sufficiency of evidence for design defect claims against Toyota. Ultimately, the court affirmed some decisions, reversed others, and remanded for further proceedings.

the intervention of their drivers. Despite much investigation, the cause of these failures could not be pinpointed. Toyota took the step of settling 400 pending cases against it after an Oklahoma jury applied the doctrine of *res ipsa loquitur* and awarded the plaintiffs in that case \$3m in damages.

Another notable case is *Toyota Motor Corporation V. Reactive Surfaces Ltd (2020)*,¹ decided by the Federal Circuit in 2020. This case involved an appeal by Toyota regarding the Patent Trial and Appeal Board's decision that certain claims of a patent were unpatentable as obvious. The court affirmed the Board's decision, supporting the finding that the patent claims were indeed obvious based on prior art.²

▪ Establish Legal Personhood Framework

Develop laws that define the legal status of AI and robots, outlining liability in cases of harm. A further legal status scenario, halfway between continuing to treat AIs as cognitive tools and assigning them some form of individual personality, is to integrate them into a distinct legal entity, for example, companies or corporations. In this way, from the theoretical point of view, AIs would not properly accord the status of independent legal actors, nor would they be merely objects under the direct control of the user, but would be conceived more as part of a shared cognitive system in which human and computer minds interact as part of a collective body. This would allow some of the features of legal personality to be derived, without radical dogmatic breaks: "It is worth noting here that this solution is more realistic since it may be easier to accept that a company has personality, intention, and other subjective states clearly more apparent than that of an electronic agent alone". From the pragmatic viewpoint, the core of this insight is essentially to apply bundles of company law rules to AIs, for Example, the regulatory framework for Limited Liability Companies (Ltd), as a way of settling their reception by the legal system and governing their powers and liabilities. Replicating the legal status of the type of corporate legal entities would make it possible to extract the functional dimension of legal personality so-as-to ensure the ownership of legal positions directly in the hands of the AIs.³

References

- Anderson B., et al. (2023). Ethical Implications of AI in Forensic Law: A Critical Analysis. *Journal of Legal Studies in Technology*, 12(4), 48.
- Barack O. (2012). What Is Regulation? *Yale Journal on Regulation Online*, 30(1), 3-10.
- Brown, H., et al. (2021). Role of Robotics in Post-Disaster Forensic Investigations. *Disaster and Forensic Science Review*, 10(3), 312.
- Brown, R., et al. (2022). Robotics and Automation in Crime Scene Investigations: Challenges and Opportunities. *Forensic Science International*, 324, 112.
- Chen Y., et al. (2021). Enhancing Forensic Accuracy through Deep Learning. *Journal of AI Applications*, 18(4), 45-60.
- Chidiogo U., et al. (2024). Legal Challenges of Artificial Intelligence and Robotics: A Comprehensive Review. *Computer Science and Information Technology Research Journal*, 5(3), 544.
- Donald Z. (2000). *Someone to Watch over Me? Privacy and Governance Strategies for CCTV and Emerging Surveillance Technologies*. Master's Thesis, Naval Postgraduate School. <https://calhoun.nps.edu/handle/10945/4167>. (Lastly Accessed on 16/04/2026).
- Dory A. (2020). Courts and Artificial Intelligence. *International Journal for Court Administration*, 11(2), 1-10.
- Dunsin, D., et al. (2024). A comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response. Available at <<https://www.sciencedirect.com>> (Lastly accessed 28th March 2025).
- G. Makam. (2023). Criminal Liability of Robots- A Critical Analysis of the Legal Framework in the US, UK, and Europe. O. P. Jindal Global University, Jindal Global Law School (JGLS). Available at SSRN: <https://ssrn.com/abstract=4649764> or <http://dx.doi.org/10.2139/ssrn.4649764> (Lastly Accessed on 07.04.2025).
- Gluyas, L., et al. (2018). Who Is Liable When AI Fails to Perform? CMS Cameron McKenna Nabarro Olswang LLP.
- Greenfield, A., et al. (2021). Standardization in AI-Powered forensic Processes. *Science and Justice*, 61(3), 288.

¹ *Motor Corporation V. Reactive Surfaces Ltd (2020)*, LLP, No. 18-1906,

² *Bibbs v. Toyota Motor Corp. - Case Law - VLEX 899577722 - 815 S.E.2d 850,304 Ga. 68.*

³ Turner, J. (2018). *Robot Rules: Regulating Artificial Intelligence*. Springer, 86.

- Handa, S et al. (2024). Role of AI in Admissibility of Electronic Evidence. *International Journal of Research Publication and Reviews*, 5(11), 1323-1238.
- Ishan A. (2023). Revolutionising the Legal Industry: The Intersection of Artificial Intelligence and Law. *International Journal of Law Management & Humanities*, 6(3), 1083.
- Jones A., et al. (2020). Predictive Analytics in Law Enforcement: Applications and Limitations. *Criminal Justice Technology*, 15(2), 25.
- Koos S. (2021). Artificial Intelligence as Disruption Factor in the Civil Law: Impact of the use of Artificial Intelligence in Liability, Contracting, Competition Law and Consumer Protection with Particular Reference to the German and Indonesian Legal Situation. *Yuridika*, 36(1), 235-262.
- Lee J., et al. (2023). Training Forensic Scientists in AI and Robotics: A New Paradigm. *Journal of Forensic Education*, 7(1), 17.
- M. Saračević M., A. Selimi., Š. Plojović. (2019). Some Specific Examples of Attacks on Information Systems and Smart Cities Applications, in Hassanien A., Elhoseny M. (eds) *Cybersecurity and Secure Information Systems*. Netherlands, Springer, 45.
- MacCarthy, J. (2007). What is Artificial Intelligence? Available at <http://jmc.stanford.edu/articles/whatisai.html> (Lasty Accessed on 16/04/2026).
- Miller B., et al. (2020). Robotics in Forensic Anthropology: A Case Study. *Journal of Forensic Robotics*, 13(3), 190.
- NCSL. (2024). Keeping Pace with Rapid Changes in Technology and Communication, National Conference of States Legislatures. Available at <https://www.ncsl.org> (Lasty Accessed on 26th April, 2025).
- Omohundro Stephen. (2008). The Basic AI Drives: Artificial General Intelligence. *Frontiers in Artificial Intelligence and Applications*, 171(1-3), 483-492.
- Patterson, S., et al. (2022). Cybersecurity Challenges in AI-Driven Forensic Investigations. *Computers & Security*, 115, 102738. <https://doi.org/10.1016/j.cose.2022.102738>
- Quezada, K., et al. (2021). Legal Challenges in Bringing AI Evidence to the Criminal Courtroom. *East African Journal of Law and Ethics*, 4(2), 1-20.
- Roberts D., et al. (2022). Autonomous Robotics in Forensic Evidence Collection. *Journal of Autonomous Systems*, 19(2), 168.
- Rwertembula, V. (2024). Legal and Practical Challenges for the Admissibility of Artificial Intelligence. *Evidence in Criminal Proceedings in Mainland Tanzania, East African Journal of Law and Ethics*, 7(1), 136-148.
- Silverman, S., et al. (2018). Torts of the Future II: Addressing the Liability and Regulatory Implications of Emerging Technologies. US Chamber for Commerce Institute for Legal Reform, p. 6. Available at <https://www.instituteforlegalreform.com/research/torts-of-the-future-ii-addressing-the-liability-and-regulatory-implications-of-emerging-technologies/> (Lasty Accessed on the 22/04/2026).
- Smith, J., et al. (2021). AI Applications in DNA Evidence Analysis. *Journal of Forensic Bioinformatics*, 9(2), 48.
- The Oxford English Dictionary. (2005). 7th Ed., Oxford, Oxford University Press.
- Thiruma Valavan. (2023). AI Ethics and Bias: Exploratory Study on the Ethical Considerations and Potential Biases in AI and Data Driven Decision making in Banking, with Focus on Fairness, Transparency and Accountability. *World Journal of Advanced Research and Reviews*, 20(2), 197-206.
- Trahan J. (2008). The Distinction Between Persons & Things: An Historical Perspective. *Journal of Civil Law Studies*, 1(6), 341-360.
- Turner, J. (2018). *Robot Rules: Regulating Artificial Intelligence*. Springer, 86.
- UNESCO. (2021). UNESCO's Recommendation on the Ethics of Artificial Intelligence, Paris, France.
- Wilson D., et al. (2023). Public Perception of AI and Robotics in Forensic Law. *Journal of Criminal Justice Ethics*, 14(1), 79.
- Wood J., et al. (2012). Developing Kaspar: A Humanoid Robot for Children with Autism. *International Journal of Social Robotic*, 13(3-4), 500.
- Yongjun Xu, et al. (2021). Artificial intelligence: A Powerful Paradigm for Scientific Research. *The Innovation Review*, 2(1), 1-20.

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).