# Culpability in the Era of Artificial Intelligence in Kenya: An Overview

**Kahungi Natasha Wanjiku***

## Abstract

*The boom of Artificial Intelligence (AI) has brought benefits and challenges alike. One particular concern about the application of AI is the imposition of liability. So far, establishing responsibility in the event that an AI system causes harm has proven difficult for a variety of reasons. Primarily, AI systems are distinct in that they lack transparency, which makes imposing liability difficult. AI also has a sense of autonomy, which makes imposing liability on the programmer, software developer, or user difficult, despite the fact that many liability regimes are human-oriented. This creates a lacuna where the perpetrator of the crime, tort or harm, often the AI system itself, is unpunished. This article examines current liability regimes and highlights their shortcomings in determining culpability. It will also propose various liability regimes with the goal of not only making amends for wrongs committed but also acting as a deterrent.*

## 1.0 Introduction to Artificial Intelligence in Kenya

Artificial Intelligence (AI) has potentially been dubbed the Fourth Industrial Revolution (4IR) marker due to its role in aiding countries and cultures around the world to transition technologically.[188] AI contributes to the 4IR by automating and substituting labour across multiple economies.[189] Remarkably, there is no

* The author is an LLB student at the University of Nairobi Law School as well as an intern at the National Council for Law Reporting (NCLR) and a News Editor at *Jurist*. She is also the Editor-in-Chief of the *University of Nairobi Law Journal*. Among many other interests, the author is passionate about Artificial Intelligence and in particular, the nexus between AI and the Law.

[188] International Labour Organisation, *The Fourth Industrial Revolution, Artificial Intelligence, and the Future of Work in Egypt*, (2021), 8.

[189] David Mhlanga, 'Artificial Intelligence in the Industry 4.0, and Its Impact on Poverty, Innovation, Infrastructure Development, and the Sustainable Development Goals: Lessons from Emerging Economies?' (2021) 13 Sustainability MPDI, 6.

single definition of AI. This is spurred by a number of factors, chief among them the distinctive nature and operation of AI that appears to evolve over time.[190] The European Union (EU), has defined AI as 'a system, whether software or hardware embedded, that exhibits intelligent behavior by gathering, processing, evaluating, and understanding its surroundings and by taking autonomous actions to achieve predefined goals.'[191] This description aptly captures two key characteristics of AI: adaptability, or the capacity to continuously improve performance through experience learning, and autonomy, the capacity to accomplish tasks in an uncontrolled environment.[192]

AI has been critical in actualizing a number of the UN's sustainable development goals (SDGs).[193] These SDGs include, among others, eradicating hunger and poverty (SDGs 1 and 2, respectively), ensuring good health (SDG 3), raising the standard of education (SDG 4), and promoting economic growth (SDG 8).[194] In Kenya, artificial intelligence is being used in the healthcare industry to speed up disease identification and treatment.[195] AI also significantly facilitates digital trading, or e-commerce, through the creation and adaptation of smart contracts and smart loans.[196] AI systems are also employed in the agricultural industry to identify diseases in crops and livestock as well as to evaluate the best options for farmers.[197] In the judicial sector, AI has expedited the delivery of justice through processes such as Online Dispute Resolution and the usage of teleconferencing and e-filing systems.[198] Consequently, AI has demonstrated enormous promise for driving change in Kenya and throughout Africa.

---

[190] University of Helsinki, 'Elements of AI' <https://course.elementsofai.com/1/1> accessed 12 February 2023.
[191] European Parliament Resolution 20 October 2020 with Recommendations to the Commission on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies [2020] A9-0186, Art 4.
[192] University of Helsinki, (n 3).
[193] Arthur Gwagwa, Patti Katchidza, Kathleen Siminyu, Matthew Smith, 'Responsible Artificial Intelligence in Sub Saharan Africa: Landscape and General State of Play' (2021) 5 AI4D <https://ircai.org/wp-content/uploads/2021/03/AI4D_Report_Responsible_AI_in_SSA.pdf> accessed 12 February 2023.
[194] Transforming our world: the 2030 Agenda for Sustainable Development, (adopted on 21 October 2015), UNGA A/RES/70/1, <https://www.refworld.org/docid/57b6e3e44.html> accessed 10 February 2023.
[195] Jackline Akello, *Artificial Intelligence in Kenya*, Padigrim Initiative (2022), 4.
[196] Ibid.
[197] Ibid.
[198] Megha Shawani, 'Alternate Dispute Resolution and Artificial Intelligence; Boom or Bane?' (2020) 2(1) LexForti Legal Journal, 2. AI can be used in ODR systems as a neutral to examine documents or as a neutral in itself to provide optimum solutions to parties.

It is fascinating to note that Sub-Saharan Africa has one of the lowest levels of AI preparedness internationally, despite the pressing need for AI systems.[199] This is in accordance with the 2022 AI Readiness Index. The fundamental purpose of this index is to examine the actions taken by the government to apply AI by looking into three significant sectors; Government, the technology sector and data and infrastructure.[200] According to the survey, Kenya, which now holds the 90th spot, is one of the few African nations that are in the top 100 in the world.[201] Additionally, according to the UN Conference on Trade (UNCTAD), Least Developed Countries (LDC) and developing countries are unprepared to adopt and adapt to the technology revolution.[202] This is due to the fact that LDCs have fewer resources, less advanced technology, and less productive industries, which could effectively impede the achievement of SDGs.[203]

Kenya has arguably taken steps to reap the greatest benefits from AI. In 2018, the government created a Blockchain and Artificial Intelligence Task Force to provide recommendations on how best to exploit AI.[204] The Task Force recommended, among other things, that the Government create laws that support AI while safeguarding human rights.[205] Unfortunately, this has yet to be accomplished, as the main AI-related issues addressed in legislation are data privacy and cybercrime in the Data Protection Act of 2019 and the Computer Misuse and Cybercrimes Act of 2018.[206] Additional suggestions include creating an AI-friendly ecosystem, assessing the hazards of AI, and putting steps in place to mitigate the problem.[207] Notwithstanding Kenya's absence of national legislation to control AI, it is important to remember that Kenya is a signatory to

[199] Annys Rogerson, Emma Hankins et al, *Government AI Readiness Index 2022*, (Oxford Insights, 2022) <https://www.unido.org/sites/default/files/files/2023-01/Government_AI_Readiness_2022_FV.pdf> accessed 12 February 2023.
[200] Ibid.
[201] Ibid.
[202] United Nations Conference on Trade and Development, *Technology and Innovation Report*, (2021) 31.
[203] United Nations Conference on Trade and Development, *The Least Developed Countries*, (2020)
[204] Muthoki Mumo, 'Tech Dream Team to Produce Kenya's Blockchain Roadmap' (*Business Daily*, 28 February 2018) <https://www.businessdailyafrica.com/corporate/tech/Ndemo-taskforce-Kenya-blockchain-roadmap-ICT/4258474-4323074-gjwgqnz/index.html> accessed 13 February 2021.
[205] Distributed Ledgers and Artificial Intelligence Taskforce, *Emerging Digital Technologies for Kenya: Exploration and Analysis*, (2019) <https://www.ict.go.ke/blockchain.pdf> accessed 13 February 2023.
[206] Data Protection Act, 2019 and Computer Misuse and Cybercrimes Act, 2018
[207] Distributed Ledgers and Artificial Intelligence Taskforce, (n 19).

international agreements like the African Union (AU) Convention on Cyber Security and Personal Data Protection, whose scope includes the handling of private information by AI systems.[208]

Despite all of its advantages, AI still confronts significant difficulties. These include bias that worsens gender inequity and problems with data protection.[209] Further discouraging the usage of AI is the idea that its incorporation into many industries may result in job losses.[210] The topic of liability is one particular concern linked with AI that will be the focus and discussion of this article. The main question in this case is, in the event that an AI system malfunctions and causes harm to a third party, who is to be held accountable? A good example is the radiotherapy machine designed by Atomic Energy of Canada Limited, which delivered lethal doses of radiation to cancer patients due to a system malfunction.[211] The liability problem is yet to be determined, as it was asserted that certain hospitals had upgraded the system thus further complicating the issue of culpability.[212] Regrettably, given the continued rise of telemedicine and other industries, this scenario is real and likely to occur in Kenya. Therefore, it is imperative that Kenya and many other African countries should enact legislation imposing liability on various actors in the event of injury caused by an AI system. These policies should be consistent with the Organization for Economic Cooperation and Development's (OECD) five AI principles.[213]

- First, that the development of AI systems should promote democracy, the rule of law, human rights, and diversity.

[208] African Union, African Union Convention on Cyber Security and Personal Data Protection (Adopted on 27 June 2014) AU <https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf> accessed 13 February 2023.

[209] Sheridan Wall and Hilke Schellmann, 'LinkedIn's job matching AI was biased. The company's solution? More AI' *(MIT Technology Review*, 23 June 2021) < https://www.technologyreview.com/2021/06/23/1026825/linkedin-ai-bias-ziprecruiter-monster-artificial-intelligence/> accessed 10 February 2023.

[210] Ibrahim Godofa, 'Artificial Intelligence and Its Future in Arbitration' (2020) 4(1) JCMSD, 10.

[211]Lee Gluyas, Stefanie Day, 'Who is liable when AI fails to perform?' (*CMS*, 2018) <https://cms.law/en/gbr/publication/artificial-intelligence-who-is-liable-when-ai-fails-to-perform> accessed 10 February 2023.

[212] Ibid.

[213] OECD, 'Recommendation of the Council on Artificial Intelligence' (Adopted on 22 May 2019) OECD/LEGAL/0449 <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed on 13 February 2023.

- Second, that AI should be a catalyst for inclusive growth and sustainable development.
- Third, AI systems should be transparent so that people may comprehend them better.
- Fourth, that organizations and people responsible for creating or using AI systems be held accountable when those systems cause harm.
- Fifth, that potential risks associated with AI be continuously assessed and managed.[214]

Yet, imposing culpability is easier said than done. This is due to a variety of factors, including regime diversity and the opaque nature of AI systems.[215] The purpose of this study is to draw attention to the ambiguity around liability in AI in the hopes that it will offer more clarity on the same. To that end, this article will be divided into the following sections: Part 2 explores the obstacles to the imposition of liability. Part 3 concentrates on the types of liability in different jurisdictions and highlight their applicability. Part 4 highlights various culpability determination models and discuss their drawbacks. The liability of AI in the Kenyan setting covered in Part 5. Finally, Part 6 will be set aside for the recommendations and conclusion.

## 2.0 Challenges that hinder the imposition of liability for AI in Kenya and Internationally

Artificial Intelligence (AI) systems in Kenya and elsewhere create a one-of-a-kind environment in which decisions may be far removed from human decision-making, unpredictable, and opaque.[216] This poses a quandary in determining culpability. Another issue that complicates assigning responsibility is whether AI qualifies as a legal person. This section is dedicated to exploring the many problems surrounding responsibility imposition and creating a deeper understanding of the nature of AI.

[215] Nieves Briz and Allison Bender, 'Key challenges of artificial intelligence: Liability for AI decisions' (*Dentons*, 2021) <https://www.businessgoing.digital/key-challenges-of-artificial-intelligence-liability-for-ai-decisions/> accessed 13 February 2023.
[216] Ibid.

Legal personhood is the capacity to exercise rights and perform obligations.[217] Its scope includes the subject of legal responsibility.[218] Legal personhood is extended not only to persons but also to non-human entities such as corporations.[219] Legal personhood for AI is still an illusion in many jurisdictions, where AI has and continues to thrive, including Kenya.[220] This considerably adds to the difficulty in apportioning blame when fully autonomous AI systems inflict harm. Fascinatingly, the EU Parliament, in its Draft Report with Recommendations to the Commission on Civil Law Rules on Robotics, proposed awarding of robots electronic personhood that is critical in holding them liable in case of harm.[221] The motion tabled suggested that robots be allowed to own property, pay taxes and pay damages whenever there is harm occasioned on another.[222] Interestingly, the motion received a lot of backlash from robotics experts, industry leaders law, medical and ethics experts who signed an open letter stating that the recommendations were based on a distorted view of robotics and were inappropriate from an ethical and legal perspective.[223]

A key merit for granting legal personhood to an AI system is that it would make it easier to assign liability in instances where different parties were involved in providing the AI service and isolating responsibility might prove difficult. This would be really helpful when a claimant wishes to identify the agent primarily in control of the risk posed by the AI system, a task that is often very costly.[224] Critics, however, argue that attaining legal personhood might not be the ideal means of establishing liability. Instead, it would create a situation in which Autonomous AI systems, granted legal personality and short-term benefits such

[217] Bryan Garner and Henry Campbell Black, *Black's Law Dictionary* (7th ed, St. Paul Minn: West Group 1999) defines a person at law as; a person is any being whom the law regards as capable of rights and duties.
[218] Ibid.
[219] Visa AJ Kurki, *A Theory of Legal Personhood*, (Oxford University, 2019), 3.
[220] Kenya Copyright Board, 'Copyright in the Age of Artificial Intelligence' (Copyright News) <https://copyright.go.ke/sites/default/files/newsletters/issue-38.pdf> accessed on 10 February 2023.
[221] Committee on Legal Affairs, *Draft Report with Recommendations to the Commission on Civil Law Rules on Robotics* (European Parliament, A8-0005/2017), 18.
[222] Ibid; Raed Alnimer and Eman Naboush, 'The extent of the civil liability of technologies for the infection and the spread of Covid-19' (2022) 25(2) Journal of Legal, Ethical and Regulatory Issues, 1-16.
[223] Valérie Simonart, 'Artificial Intelligence and Legal Personality,' (*Liedekerke*, 5 October, 2022) <https://liedekerke.com/en/insights/artificial-intelligence-and-legal-personality> Accessed 3rd March 2023.
[224] Andrea Bertolini, *Artificial Intelligence and Civil Liability* (European Parliament, PE 621.926), 18.

as the capacity to own and dispose of assets, would effectively control the economy.[225]

Autonomy is a predominant feature of AI, as was previously mentioned. AI systems use machine learning algorithms in order to process data and provide outcomes.[226] This means that as long as they are provided with enough data, they require little to no supervision.[227] AI systems' capacity for independent learning could cause them to make unanticipated and difficult-to-understand conclusions.[228] Typically, the choices should fall within the range of anticipated outcomes, although this is not always the case.[229]

Due to how remote the AI system's decisions are from human oversight, it can be challenging to determine liability when a mishap happens at this stage.[230] In South Africa, for example, restrictions are in place to guarantee that doctors depend on their knowledge to best treat patients, regardless of recommendations from AI systems.[231] This is due to their recognition that AI occasionally has the potential to produce ludicrous and unforeseen outcomes. Yet, this might only be effective in situations where humans still have some influence on AI systems.[232] It would thus be rendered ineffectual when such control is relaxed, like in the case of self-driving cars and fully automated AI systems.[233]

Connectivity to other systems is a key component of how AI functions.[234] In order to learn and operate, AI is significantly dependent on data.[235] For instance, in order for self-driving automobiles to operate effectively, they must communicate with

[225] Valérie Simonart, 'Artificial Intelligence and Legal Personality,' (*Liedekerke*, 5 October, 2022) <https://liedekerke.com/en/insights/artificial-intelligence-and-legal-personality> Accessed 3rd March 2023.
[226] Giangiacomo Olivi and Brendan Graves, 'Dentons Artificial Intelligence Guide 2022: The AI journey—opening our eyes to opportunity and risk' (*Dentons*, 2022) <https://www.businessgoing.digital/dentons-artificial-intelligence-guide-2022-the-ai-journey-opening-our-eyes-to-opportunity-and-risk/> accessed on 11 February 2023.
[227] Michael Da Silva, 'Autonomous Artificial Intelligence and Liability: A Comment on List' (2022) 35 (44) Philosophy & Technology.
[228] Ibid.
[229] Ibid.
[230] Ibid.
[231] Dustee Lee Donnelly, 'First Do No Harm: Legal Principles Regulating the Future of Artificial Intelligence in HealthCare in South Africa' (2022) 25 PER, 2.
[232] Michael Da Silva (n 46).
[233] Michael Da Silva (n 46).
[234] Michael Da Silva (n 46).
[235] Christiane Wendehorst, 'Strict Liability for AI and other Emerging Technologies', (2020) 11(2) JETL 160.

other vehicles, traffic signs, and other traffic signals.[236] This interconnectedness presents a stumbling block in determining culpability since it increases the number of individuals who must be held accountable.[237] The problem is further complicated by the fact that the participants have no control over what the other party does with their data and, as a result, will be reticent to accept responsibility for acts indirectly carried out by them.[238] Also, because there are so many passive participants and AI systems, it might be challenging to identify the source of a defect and who was responsible for the defect.[239]

AI systems are also opaque in the sense that they lack transparency in their operation and performance.[240] Choices made by AI systems are often inexplicable. In addition to using pre-processed data, machine learning algorithms also employ their own methods of trial and error to get outcomes.[241] Because of this, even "reliable" AI systems might not be as transparent as desired.[242] This is known as the "black box nature of AI," and it has a variety of effects on liability.[243]

Fundamentally, AI learning systems are complex and difficult to comprehend, necessitating effort and a technical mind.[244] As a result, legal practitioners and legislators must understand the fundamentals of AI in order to assign blame to the party who made a mistake.[245] Furthermore, in the case of a liability claim, the

[236] Michael Da Silva (n 46).
[237] Christiane Wendehorst, (n 54).
[238] Report from the Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence and other emerging digital technologies* (European Commission, 2019).
[239] Philip Boucher, 'Artificial intelligence: How does it work, why does it matter, and what can we do about it?' (2020) European Parliamentary Research Service.
[240] Matthew Fenech, Nika Strukelj and Olly Buston, *Ethical, social and political challenges of artificial intelligence in health*, (Future Advocacy report for the Wellcome Trust, 2018).
[241] Anirudh V K, 'How Does Artificial Intelligence Learn Through Machine Learning Algorithms?' (*Spiceworks*, 10 February 2022) <https://www.spiceworks.com/tech/artificial-intelligence/articles/how-does-ai-learn-through-ml-algorithms/> accessed 13 February 2023.
[242] Ibid; Yavar Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' (2018) 31(2) Harvard Journal on Law & Tech, 889.
[243] Philip Boucher, 'Artificial intelligence: How does it work, why does it matter, and what can we do about it?' (2020) European Parliamentary Research Service, 19; Yaniv Benhamou & Justine Ferland, 'Artificial Intelligence & Damages: Assessing Liability and Calculating the Damages' in Giuseppina D'Agostino, Aviv Gaon & Carole Piovesan, (eds), *Leading Legal Disruption: Artificial Intelligence and a Toolkit for Lawyers and the Law* (Toronto: Thomson Reuters Canada, 2021) at 8.
[244] Expert Group on Liability and New Technologies, *New Technologies Formation, Liability for Artificial Intelligence and Other Emerging Digital Technologies* (Luxembourg: Publications Office of the European Union, 2019), 52-59.
[245] Ibid.

parties in possession of the data and algorithms that explain how the injury occurred have no incentive to share the information because doing so would expose them to liability.[246] The lack of transparency also makes determining causation difficult. This is because it is difficult to overcome the burden of proof, as the claimant must also demonstrate injury and cause.[247] This overarching principle is too condemning since it will be very challenging for the victims to establish causality where the system is not transparent.[248]

It is also difficult to hold AI systems accountable where AI is being created and used on a global basis.[249] This is due to the fact that different countries have different legal frameworks, ethical dilemmas, and cultural perspectives on AI.[250] So, if an AI system is created across multiple jurisdictions with various responsibility regimes or without any liability regimes at all, a mistake made by the AI system may be challenging to remedy.

## 3.0 Types of liability in AI in Kenya and Internationally

The diversity of liability regimes, as discussed in the previous section, is one impediment to establishing liability for AI defects. It is fascinating to note that most liability regimes rely on the human element to impose liability in the absence of express regulations.[251] This means that the AI system cannot be held liable. Rather, the system's programmer, developer, or user will be held liable for any harm caused by the system. The purpose of this section is to discuss liability regimes and to highlight the relevance of each.

[246] Ibid; Lee Akazaki, 'Failing to Predict the Past: Will Legal Causation Kill Tort Law in Cyberspace?' [2017] Annual Review of Civil Litigation 27
[247] Yavar Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' (2018) 31(2) Harvard Journal of Law & Technology, 922.
[248] Ibid.
[249] Michael Da Silva (n 46).
[250] Ibid.
[251] Leon Wein, 'The Responsibility of Intelligent Artefacts: Towards an Automation Jurisprudence' (1992) 6 Harvard Journal of Law & Technology.

## 3.1 Civil liability in AI

The term "civil liability" describes the legal obligation to make up for damage or loss brought on to another person or piece of property.[252] Civil liability in the context of AI refers to the responsibility of individuals, businesses, or governments for any harm or loss caused by AI systems.[253] As AI systems become more autonomous, the question of who is ultimately responsible for their actions becomes more complicated. Civil liability includes several liability regimes, including contractual liability, tortious liability, products liability, and strict liability.

## 3.2 Contractual Liability in AI

This liability regime is appropriate when the AI system is the subject of a sales contract. Under contract law, a supplier-recipient relationship may include an exclusion clause to exclude liability in the event of a defective AI component.[254] Depending on how the court interprets the exclusion clause, the supplier may or may not be held liable for the faulty AI. Furthermore, claims may be brought before the court for harm suffered by the claimant who relies on the implied term regarding the fitness of the product, i.e., the AI system.[255] Therefore, the implied term must be interpreted by the court in relation to the AI system. In dealing with cases where an AI system that is subject to a contract has caused harm, is a well-established principle that the loss suffered should not be so far off that it is impossible to recover it under contractual liability.[256]

Nonetheless, there are weaknesses in the contractual liability regime. In many jurisdictions, including Kenya, AI is not considered a good under the Sale of Goods Act, which governs contractual transactions involving the sale of goods.[257]

---

[252] Jean-Sebastien Boghetti, 'Civil Liability for Artificial Intelligence: What Should its Basis Be?' (219) SSRN, 1.
[253] Ibid.
[254] Ibid.
[255] Ibid.
[256] Phillip Kelly, Marcus Walsh, Sofia Wyzykiewicz and Simone Young-Alls, 'Man vs Machine: Legal liability in Artificial Intelligence contracts and the challenges that can arise' (*DLA piper*, 6 October 2021) <https://www.dlapiper.com/en/insights/publications/2021/10/man-vs-machine-legal-liability-artificial-intelligence-contracts> accessed 14 February 2023.
[257] Sale of Goods Act, 1979 enacted in the UK Sale of Goods Act, Cap 31 in Kenya do not recognise AI as a good.

In the United Kingdom, for example, in the cases of *St Albans City and District Council* v *International Computers* and *Computer Associates UK Ltd* v *Software Incubator Ltd*, the court determined that computer software does not qualify as a good under the Sale of Goods Act of 1979.[258] This would make it particularly challenging to establish contractual liability under the Act since AI would be similarly classified.[259]

## 3.3 Tortious Liability in AI

This liability regime is frequently used when a claimant has run into some difficulties in proving contractual liability.[260] Under this regime, the claimant may bring a negligence claim in order to impose liability on a party who is not subject to contractual liability.[261] Causation, duty of care and foreseeability must be proven in order to prove negligence.[262] Arguably, the foreseeability component of negligence in the context of AI may be particularly challenging to demonstrate due to the "black box" nature of AI.[263] Nonetheless, if the claimant can establish a causal link between the supplier or developer's conduct and the defect in the AI system that caused harm, the latter may be held liable under the tort of negligence.[264]

[258] *St Albans City and District Council* v *International Computers [1996] 4 All ER 481; Computer Associates UK Ltd* v *Software Incubator Ltd [2018] EWCA Civ 518.*

[259] Phillip Kelly, Marcus Walsh, Sofia Wyzykiewicz and Simone Young-Alls, 'Man vs Machine: Legal liability in Artificial Intelligence contracts and the challenges that can arise' (*DLA piper,* 6 October 2021) <https://www.dlapiper.com/en/insights/publications/2021/10/man-vs-machine-legal-liability-artificial-intelligence-contracts> accessed 14 February 2023.

[260] Phillip Kelly, Marcus Walsh, Sofia Wyzykiewicz and Simone Young-Alls, 'Man vs Machine: Legal liability in Artificial Intelligence contracts and the challenges that can arise' (*DLA piper,* 6 October 2021) <https://www.dlapiper.com/en/insights/publications/2021/10/man-vs-machine-legal-liability-artificial-intelligence-contracts> accessed 14 February 2023; *Winnipeg Condominium Corporation No. 36* v. *Bird Construction Co., [1995] 1 S.C.R. 85* the court noted that establishing the duty of care under the tort of negligence is crucial where there is no contractual relationship between the party that could allow for recovery of damages.

[261] Thomasen Kristen, 'AI and Tort Law' in Florian Martin-Bariteau & Teresa Scassa (eds), *Artificial Intelligence and the Law in Canada* (Toronto: LexisNexis Canada, 2021).

[262] *Donoghue* v. *Stevenson, [1932] A.C. 562 (H.L.) at 580–581* on the duty of care; *Mustapha* v. *Culligan of Canada Ltd* on causation.

[263] Brian Sheppard, 'Warming up to Inscrutability: How Technology Could Challenge Our Concept of Law' (2018) 68:1 UTLJ 36.

[264] Thomasen, Kristen, (n 76).

## 3.4 Product Liability in AI

Product liability is a hybrid system of contractual and tortious liability.[265] It addresses remedies for injuries caused by product defects as well as product misrepresentation.[266] This regime covers negligence, design flaws, manufacturing flaws, failure to warn, and breach of warranty.[267] Manufacturers must create safe products that are used in a way that is reasonably foreseeable, for example, if they want to avoid liability in a negligence case.[268] Thus, if the claimant used this product in a reasonably foreseeable manner and suffered harm as a result, he may argue that the manufacturer was negligent in failing to foresee that specific outcome. Another critical aspect of product liability is strict liability, which is discussed further below.

## 3.5 Strict Liability in AI

Case law demonstrates a global shift away from relying on negligence to define liability and toward the imposition of strict liability regimes.[269] This is supported by the argument belief that consumers have a right to safe products.[270] This type of liability makes the supplier responsible for any product flaws, regardless of negligence or intent. Manufacturers who fail to disclose potential risks associated with their products are primarily subject to strict liability.[271] The test of strict liability was established in the locus classicus case of *Rylands* v. *Fletcher* which states "the person who for his own purposes brings on his lands and collects and keeps there anything likely to do mischief if it escapes, must keep it in at his peril, if he does not do so, is *prima facie* answerable for all the damage which is the natural consequence of its escape."[272] Thus, the ultimate goal of this regime is to ensure that a user who suffers harm as a result of a defective AI system is entitled

[265] John Villasenor, 'Products Liability and Driverless Cars: Issues and Guiding Principles for Legislation' (2014) Washington DC Brookings Institution, 7.
[266] John Villasenor, *Products liability law as a way to address AI harm,* (AI Governance Series, 2019).
[267] Ibid.
[268] Ibid.
[269] Christiane Wendehorst, 'Liability for Artificial Intelligence: The Need to Address Both Safety Risks and Fundamental Rights Risks' in Silja Voeneky, Phillip Kellmeyer, et al (eds), *The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives* (Cambridge Law Handbooks, 2022).
[270] John Villasenor, (n 81).
[271] Ibid.
[272] (1868) LR 3 HL 330.

to a remedy as he does not have to bear the burden of determining precisely where the defect in the AI system is.

## 3.6 Criminal liability in AI

Criminal liability refers to the legal responsibility or culpability of an individual or entity for committing a criminal offense, subject to punishment or sanctions under the law. Two requirements must be met in order to establish criminal liability. The person must first be proven to have committed an act or omission (*actus reus*).[273] Furthermore, *mens rea*, the mental element, is also required to establish liability.[274] Establishing the *actus reus* in the context of AI is relatively easy. However, proving the *mens rea* element of an AI system itself creates a formidable challenge. It is critical to understand that in many jurisdictions, AI is not recognized as a legal person.[275] As a result, AI, like animals, generally lacks the necessary *mens rea* to determine criminal liability.[276] However, it is worth noting that even humans have occasionally displayed behavior that makes determining the mental component difficult.[277] In these situations, the court has imposed liability based on fault.[278]

## 3.7 Fault-based Liability in AI

These Common Law principles refer to the requirement that the claimant demonstrate that the product supplier acted negligently by failing to act in some way that resulted in harm in addition to product defects.[279] A stellar illustration of this would be where a doctor is held liable for failing to look into the recommendations suggested by AI software on treatment administered to patients. In this instance, the medical professional is still responsible for mistakes and

[273] Aryashree Kunhambu and Akshita Rohatgi, 'Artificial intelligence and the shift in liability' (*ipleaders*, 9 September 2021) <https://blog.ipleaders.in/artificial-intelligence-shift-liability/> accessed on 14 February 2023.
[274] Aryashree Kunhambu and Akshita Rohatgi, 'Artificial intelligence and the shift in liability' (*ipleaders*, 9 September 2021) <https://blog.ipleaders.in/artificial-intelligence-shift-liability/> accessed on 14 February 2023.
[275]Aryashree Kunhambu and Akshita Rohatgi, 'Artificial intelligence and the shift in liability' (*ipleaders*, 9 September 2021) <https://blog.ipleaders.in/artificial-intelligence-shift-liability/> accessed on 14 February 2023.
[276] Aryashree Kunhambu and Akshita Rohatgi, 'Artificial intelligence and the shift in liability' (*ipleaders*, 9 September 2021) <https://blog.ipleaders.in/artificial-intelligence-shift-liability/> accessed on 14 February 2023.
[277] Ibid.
[278] Ibid.
[279] Dustee Lee Donelly, (n 46), 20

omissions in treatments that were reasonably foreseeable.[280] Strikingly, this type of liability excludes harm caused by unknown or unforeseeable flaws.[281] The implication of this is that it would be unjust to hold the practitioner liable if the defects were unforeseeable while at the same time, the patient would be left without recourse.

## 4.0 Models of determining Criminal liability in AI in Kenya and Internationally

This section aims to explore three essential models for determining culpability. They are: the perpetration by another AI liability, the natural probable consequence model, and the direct liability model.[282]

### 4.1 The perpetration by another liability of AI

This model promotes the idea that AI can be utilized as a conduit for criminal activity.[283] In this instance, the offender will be held accountable, and AI will be deemed an innocent agent, just as a minor or a person of unsound mind would be under the same circumstances.[284] The model is based on the justification that a person or thing cannot be held accountable if it lacks the freedom to make its own decisions.[285] Because AI systems rely so significantly on the data that is provided to them, they are thought to be incapable of making decisions on their own.[286] This concept integrates the strict liability system, according to which the programmer is held accountable for crimes committed by the system. In addition, the harm caused by the defect will be the responsibility of the user or programmer who should have been able to predict it.[287]

Under this model, the perpetrator could be one of two people: the coder or the end user.[288] When a programmer creates a robot, for instance, and embeds it with

[280] Dustee Lee Donelly, (n 46), 20.
[281] Dustee Lee Donelly, (n 46), 20.
[282] Gabriel Hallevy, 'The Basic Models of Criminal Liability of AI Systems and Outer Circles' (2019) SSRN,1.
[283] Lawrence Solum, 'Legal Personhood for Artificial Intelligences' (1992) 70 NCL REV, 1231.
[284] Gabriel Hallevy, (n 97).
[285] Gabriel Hallevy, 'The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control, (2010) 4(2) (1) Akron Intellectual Property Journal, 179.
[286] Ibid.
[287] Gabriel Hallevy, (n 97), 3.
[288] Gabriel Hallevy, (n 101), 179.

software, and the robot then commits a crime, the programmer will be held accountable for the crime.[289] On the other hand, the user is responsible if the AI system violates the law while being used by the user for personal gain.[290] This master-servant relationship between the AI and the user justifies the imposition of culpability. Although the AI system committed the crime in both instances, satisfying the *actus reus* (or conduct) of criminal culpability, the mental component of the AI system is tasking to determine.[291] Hence, courts do not emphasise the *mens rea* of the system or perpetrators.

This approach is ideal when a user or programmer uses an AI system to commit a crime without making use of any of its further capabilities.[292] Also, it might be applied to outdated AI systems that have not been updated to more recent, sophisticated ones.[293] AI is used as a tool in every one of these situations to commit the crime.[294] Yet, the paradigm would not work if an AI system was fully autonomous and committed a crime on its own.[295]

### *4.2 The natural probable consequence of liability*

The fundamental premise of this paradigm is that the AI system is under the control of its programmer, who had no intention of using the system to perform any crime.[296] Nonetheless, the AI system breaks the law while performing its daily tasks. Users and programmers were not involved in perpetrating the crime and were not aware it had been done.[297] In order to determine culpability, this approach depends on the programmer's or user's ability to foresee.[298] According to this argument, a person is legally responsible when the crime they committed was a logical and likely result of AI's behaviour.[299]

---

[289] Ibid.
[290] Gabriel Hallevy, (n 97), 3.
[291] Lawrence Solum (n 99), 69; George Cross and Cary Debessonet, 'An Artificial Intelligence Application in the Law: CCLIPS, A Computer Program that Processes Legal Information' (1986).1 HIGH TECH. L.J. 329.
[292] Compare with; Andrew Wu, 'From Video Games to Artificial Intelligence: Assigning Copyright Ownership to Works Generated by Increasingly Sophisticated Computer Programs' (1997) 25 AIPLA Q.J, 131.
[293] Ibid.
[294] Ibid.
[295] Gabriel Hallevy, (n 101), 181.
[296] Ibid.
[297] Gabriel Hallevy, (n 97).
[298] Ibid.
[299] Ibid.

Under this theory, the programmer or user must have been acting negligently.[300] It is not necessary for them to know that the crime will be committed; rather, it is sufficient to know that the crime's commission was a logical and likely result of the AI's routine actions.[301] This theory attempts to address the issue of culpability in situations when the programmer or user predicted the conduct of the offence, but it is unable to address the question of whether the AI itself should be held accountable for the offence.[302]

### *4.3 Direct Liability Model*

Direct Liability aims to hold the AI system accountable.[303] The justification for assigning blame is based on the notion that an AI system should be held accountable if it can demonstrate both the *actus reus* and the *mens rea* (or mental) requirements for criminal responsibility.[304] As the *actus reus* (conduct) in criminal proceedings involving AI entails an action or inaction by the system, proving it is quite simple.[305] The actual stumbling block is demonstrating the internal aspect. Liability is subject to the mental elements of knowledge, intent, and negligence.[306] The *mens rea* criterion is deemed to have been met when an AI system exhibits awareness of the external element or was developed with a specific aim or purpose such as to commit a crime.[307] In light of this, there is no justification for not imposing culpability when an AI system determines both the *mens rea* and *actus reus* of the offence.[308] In such a scenario, the AI system's criminal accountability is imposed in addition to that of the programmer or user.[309] Hence, the criminal culpability of AI is not reliant on that of the programmer or user; rather, the

[300] Robert Fine and Gary Cohen, 'Is Criminal Negligence a Defensible Basis for Criminal Liability?' (1966) 16 BUFF L REV. 749; Herbert L.A. Hart, 'Negligence, Mens Rea and Criminal Responsibility' (1961) 29 Oxford Essays in Jurisprudence.
[301] Gabriel Hallevy, (n 97), 6.
[302] Ibid.
[303] Ibid.
[304] Ibid.
[305] Joshua Dressler and Stephen Garvey, *Criminal law: cases and materials* (7th Ed West Academic Publishing 2016).
[306] Gabriel Hallevy, (n 101), 188.
[307] Ibid.
[308] Joshua Dressler and Stephen Garvey, *Criminal law: cases and materials* (7th Ed West Academic Publishing 2016).
[309] Ibid.

programmer or user and AI system may be found jointly accountable as accomplices and abettors.[310]

## 5.0 Liability of AI and the Kenyan Experience

AI has played an important role in the development of various industries across the country. Digital credit, for example, has been a game changer in loan issuance.[311] A study by the University of Nairobi's Institute for Development Studies (IDS), University College London's Institute for Advanced Studies, and Lawyers Hub estimates that at least six million Kenyans have taken out at least one digital loan.[312] In such a case, artificial intelligence is used to automate lending decisions and risk assessments.[313] What happens then if, in the case of a mobile lending app, consumer data is compromised or if, as a result of the AI system's improper creditworthiness assessment, the system leads to over indebtedness or defaults? Who will be held accountable for the harm caused?

Kenyan law is often technology-neutral and applies the same legal standards to AI as it does to other technologies. As such, it lacks AI specific liability regimes.[314] The implication of this is that it creates a challenge in establishing culpability in case an AI system causes harm. Currently, to impose liability, Kenya takes into account several legal systems including; intellectual property law, contract law, tort law, and data protection legislation. Primarily the Constitution of Kenya guarantees the right to a fair hearing and access to justice.[315] Thus, where AI causes harm or damage, those affected can seek redress in court.

Copyright law may be used to safeguard software code and works produced by AI under intellectual property law.[316] Under the Copyright Act, the first owner of the copyright is the author.[317] Generally, an author is identified as a person or legal

[310] Ibid.
[311] Mark Gaffley, Rachel Adams and Ololade Shyllon, *Artificial Intelligence. African Insight A Research Summary of the Ethical and Human Rights Implications of AI in Africa* (HSRC & Meta AI and Ethics Human Rights Research Project for Africa, 2022), 5.
[312] Ibid.
[313] Ibid.
[314] Jackline Akello, (n 8), 5.
[315] Constitution of Kenya 2010, Art 48 and 50.
[316] Copyright Act, Cap 130.
[317] Ibid, S2.

entity that creates the literary work, photograph or computer programme.[318] Consequently, an AI system is not recognized as an author and cannot have any claim under copyright law.[319] The implication of this is that as it cannot claim any rights, it is also not subject to any liabilities. Kenya, like India and Hong Kong have attributed any rights and liabilities relating to AI generated pieces to the person who made the necessary preparations for the creation of the work in question.[320] This may indicate that a user or computer programmer may be held liable where an AI system is in breach of copyright law.

In situations when AI is employed in a contractual relationship, such as when an AI system is used to provide automated customer support, contract law suffices. Liability in such circumstances would most likely be determined by the terms of the parties' contract.[321] As discussed in the previous section, the Sale of Goods Act is silent on whether AI is considered a good.[322] Thus, applying the act to supplier-consumer transactions may present a legal problem. Tort law may apply when AI causes harm or damage, such as when an AI system erroneously prescribes medication for a patient.[323] Depending on the specifics of the situation, liability may be placed on the AI system's owner, software developer or user. In such a case, the claimant ought to establish that there was harm occasioned by the system owing to the negligence of the system owner, manufacturer or developer.[324]

Under the Data Protection Act (DPA), it is the responsibility of data controllers and processors to guarantee that the processing of personal data complies with the law.[325] However, it is unclear who is responsible when an AI system is independently involved in the processing of personal data. One potential problem

[318] Ibid.
[319] Kenya Copyright Board, 'Copyright in the Age of Artificial Intelligence' (Copyright News) <https://copyright.go.ke/sites/default/files/newsletters/issue-38.pdf> accessed on 10 February 2023.
[320] Kenya Copyright Board, 'Copyright in the Age of Artificial Intelligence' (Copyright News) <https://copyright.go.ke/sites/default/files/newsletters/issue-38.pdf> accessed on 10 February 2023.
[321] Supra 72.
[322] Phillip Kelly, Marcus Walsh, Sofia Wyzykiewicz and Simone Young-Alls (n 62).
[323] Thomasen, Kristen, (n 76).
[324] Ibid.
[325] Data Protection Act, 2019.

is that AI systems occasionally make decisions that are hard to justify.[326] If something goes wrong, it may be difficult to assign fault due to this lack of transparency. For instance, it might be challenging to determine who is responsible if an AI system makes a bad choice that hurts a person—the data controller or processor, the AI system, or both.

The DPA mandates that data controllers and processors put in place the necessary organizational and technical safeguards to ensure the security of personal data in order to address this problem.[327] This includes putting in place safeguards to prevent unauthorized or unlawful processing, accidental loss or destruction of personal data, and data damage.[328] It is also worth noting that AI systems are not exempt from the DPA's requirement to obtain data subjects' consent before processing their personal data.[329] Individuals must be informed about the use of AI in the processing of their personal data by data controllers and processors, and their explicit consent must be obtained.[330]

The Consumer Protection Act (CPA) provides for the liability of suppliers and manufacturers of goods and services to consumers.[331] A supplier is defined by the Act as someone who provides goods or services in the course of their business, whereas a manufacturer is someone who makes, assembles, or produces goods. A supplier or manufacturer is liable under the CPA for any harm caused to a consumer by the goods or services provided.[332] This includes damage caused by defective goods or services, a failure to provide adequate instructions or warnings, and a breach of an express or implied warranty.

In the case of AI, liability may arise when a consumer is harmed as a result of an AI system's decision.[333] For example, if an AI-powered recommendation system

[326] Giangiacomo Olivi and Brendan Graves, 'Dentons Artificial Intelligence Guide 2022: The AI journey—opening our eyes to opportunity and risk' (*Dentons*, 2022) <https://www.businessgoing.digital/dentons-artificial-intelligence-guide-2022-the-ai-journey-opening-our-eyes-to-opportunity-and-risk/> accessed on 11 February 2023.
[327] Data Protection Act, 2019.
[328] Data Protection Act, 2019.
[329] Data Protection Act, 2019.
[330] Data Protection Act, 2019.
[331] Consumer Protection Act, 2012.
[332] Ibid.
[333] John Villasenor, (n 81).

recommends a product that harms a consumer, the system's supplier or manufacturer may be held liable under the CPA.[334] However, liability may not arise if the harm caused was not reasonably foreseeable or if the consumer was aware of the risks associated with the product or service's use. Furthermore, liability may be reduced if the supplier or manufacturer can demonstrate that they took reasonable precautions to avoid the harm.[335]

Ultimately, establishing responsibility for AI in Kenya requires a case-by-case analysis that takes into account the specifics of each instance as well as the pertinent legal frameworks. Kenyan legislators are advised to draft specific laws and rules to address the liability issues raised by the use of AI as the technology becomes more widespread.

## 6.0 Recommendations and Conclusion on AI in Kenya

Kenya must adopt an AI liability regime that is consistent with the ever-changing nature of AI. To address these issues, a greater emphasis on transparency and accountability in the development and deployment of AI systems is required.[336] This is done to reduce the black-box nature of AI. Consequently, developers must work to make AI systems more transparent so that people can understand how they make decisions. Legislators should develop a liability framework for AI that takes a human-centric approach, in line with the European Commission's recommendations.[337] This legal framework should be based on transparency, accountability, and human rights protection.[338] Additionally, there needs to be a greater emphasis on international coordination, so that there is a unified approach to the development and deployment of AI.[339]

[334] Ibid.
[335] Ibid.
[336] Richard Roovers, 'Transparency and Responsibility in Artificial Intelligence A call for explainable AI' (*Deloitte*, 2019).
[337] Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, Building Trust in Human-Centric Artificial Intelligence, (Brussels COM 168 Final, 2019).
[338] Tambiama Madiega, *Artificial intelligence liability directive* (European Parliamentary Research Service, 2023).
[339] Ibid.

Kenya's legal system must distinguish between accountability for AI as a technology and accountability for AI as an individual. According to this paper, the legal personhood of AI may be the key to establishing civil liability.[340] This is due to the fact that granting legal personhood imposes obligations on the AI. When an AI system violates its obligations and causes harm, the judicial system may award restitution to the victim by holding the AI system liable.[341] Damages can only be awarded if AI is able to own property, which is only possible if AI attains legal personhood.[342] Furthermore, granting AI systems legal personhood may help to circumvent the issue of imposing liability on fully autonomous AI systems. Thus, there is a need to sufficiently address the legal status of AI before assigning liability.

It is critical to note that in discussing the liability of AI, one has to consider the issue of enforcing court orders and what happens when the AI system fails to comply with the court order. Ideally, courts may hold AI systems in contempt and may order the system to pay fines or impose other sanctions. In doing so, the courts may consider factors such as the intent of the AI, the extent to which the AI's behaviour was foreseeable etc. Thus, holding AI in contempt requires a nuanced approach to balancing its autonomous and adaptable nature.

This article recognizes that no single type of liability can govern the use of AI as AI is dynamic and has infiltrated many aspects of human life. As a result, it proposes integrating various liability regimes to govern the imposition of AI liability. In particular, when drafting regulations to impose criminal liability, consideration should be given to the three models mentioned above: natural consequence, direct liability, and perpetration by another liability.

Legislators should also take into account the concept of joint liability.[343] Under such a liability regime, the developer and user, the developer and AI system, or

[340] Committee on Legal Affairs, *Draft Report with Recommendations to the Commission on Civil Law Rules on Robotics* (European Parliament, A8-0005/2017), 18.
[341] Ibid.
[342] Ibid.
[343] Amanda Leiu, 'Artificial Intelligence ('AI'): Legal Liability Implications' (*Burges and Salmon*, 30 January 2020) < https://www.burges-salmon.com/news-and-insight/legal-updates/commercial/artificial-intelligence-legal-liability-implications> accessed 11 February 2023.

the user and AI system, can be held liable for any harm caused.[344] Furthermore, legislators should enact an adapted duty of care, such as additional obligations on AI system suppliers to monitor and maintain those systems in order to control for unexpected outcomes due to machine learning.[345] The implication of this revised duty of care is that AI systems will cause less harm as they are actively maintained. However, if the AI system causes harm as a result of system flaws, the system operator or supplier will be held liable.

The purpose of this article was to explore the various liability regimes for AI while outlining the difficulties in imposing responsibility in Kenya. As stated, the opaque, adaptable, and autonomous nature of AI systems creates a particularly unique situation that makes imposing liability difficult. In addition to the models for imposing liability, this paper has highlighted various forms of liability that are essential in ensuring that harms caused by AI are remedied. Since AI is so flexible, these liability regimes cannot function in isolation. Therefore, it is urgent for legislators to pass integrated liability regimes to guarantee that harm caused by AI systems is not left unattended. Legislators should work to make sure that these liability regimes serve to both remedy the harm already done and prevent further harm. After all, an ounce of prevention is worth a pound of cure in the AI context too.

[344] Ibid.
[345] Tambiama Madiega, *Artificial intelligence liability directive* (European Parliamentary Research Service, 2023).

## 7.0 BIBLIOGRAPHY

**Books**

Benhamou, Y & Ferland J, 'Artificial Intelligence & Damages: Assessing Liability and Calculating the Damages' in Giuseppina D'Agostino, Aviv Gaon & Carole Piovesan, (eds), *Leading Legal Disruption: Artificial Intelligence and a Toolkit for Lawyers and the Law* (Toronto: Thomson Reuters Canada, 2021) at 8.

Dressler J and Garvey S, *Criminal law: cases and materials* (7th Ed West Academic Publishing 2016).

Kristen, T, 'AI and Tort Law' in Florian Martin-Bariteau & Teresa Scassa (eds), *Artificial Intelligence and the Law in Canada* (Toronto: LexisNexis Canada, 2021).

Kurki ,V, *A Theory of Legal Personhood*, (Oxford University, 2019), 3.

Villasenor, J, *Products liability law as a way to address AI harm,* (AI Governance Series, 2019).

Wendehorst, C, 'Liability for Artificial Intelligence: The Need to Address Both Safety Risks and Fundamental Rights Risks' in Silja Voeneky, Phillip Kellmeyer, et al (eds), *The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives* (Cambridge Law Handbooks, 2022).

**Journal Articles**

Akazaki, L, 'Failing to Predict the Past: Will Legal Causation Kill Tort Law in Cyberspace?' [2017] Annual Review of Civil Litigation 27.

Alnimer, R and Naboush E, 'The extent of the civil liability of technologies for the infection and the spread of Covid-19' (2022) 25(2) Journal of Legal, Ethical and Regulatory Issues, 1-16.

Bathaee, Y, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' (2018) 31(2) Harvard Journal on Law & Tech, 889.

Boghetti, J, 'Civil Liability for Artificial Intelligence: What Should its Basis Be?' (219) SSRN, 1.

Boucher, P, 'Artificial intelligence: How does it work, why does it matter, and what can we do about it?' (2020) European Parliamentary Research Service.

Cross, G and Debessonet C, 'An Artificial Intelligence Application in the Law: CCLIPS, A Computer Program that Processes Legal Information' (1986).1 HIGH TECH. L.J. 329.

Donnelly D, 'First Do No Harm: Legal Principles Regulating the Future of Artificial Intelligence in HealthCare in South Africa' (2022) 25 PER, 2.

Fine, R and Cohen G, 'Is Criminal Negligence a Defensible Basis for Criminal Liability?' (1966) 16 Buff el Rev 749

Godofa, I, 'Artificial Intelligence and Its Future in Arbitration' (2020) 4(1) JCMSD.

Hallevy, G, 'The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control, (2010) 4(2) (1) Akron Intellectual Property Journal, 179.

Hallevy, G, 'The Basic Models of Criminal Liability of AI Systems and Outer Circles' (2019) SSRN,1.

Mhlanga, D, 'Artificial Intelligence in the Industry 4.0, and Its Impact on Poverty, Innovation, Infrastructure Development, and the Sustainable Development Goals: Lessons from Emerging Economies?' (2021) 13 Sustainability MPDI, 6

Shawani, M, 'Alternate Dispute Resolution and Artificial Intelligence; Boom or Bane?' (2020) 2(1) LexForti Legal Journal, 2.

Sheppard, B, 'Warming up to Inscrutability: How Technology Could Challenge Our Concept of Law' (2018) 68:1 UTLJ 36

Silva, M, 'Autonomous Artificial Intelligence and Liability: A Comment on List' (2022) 35 (44) Philosophy & Technology.

Solum, L, 'Legal Personhood for Artificial Intelligences' (1992) 70 NCL REV, 1231.

Wein, L, 'The Responsibility of Intelligent Artefacts: Towards an Automation Jurisprudence' (1992) 6 Harvard Journal of Law & Technology.

Wendehorst C, 'Strict Liability for AI and other Emerging Technologies', (2020) 11(2) JETL 160.

Wu, A, 'From Video Games to Artificial Intelligence: Assigning Copyright Ownership to Works Generated by Increasingly Sophisticated Computer Programs' (1997) 25 AIPLA Q.J, 131

Villasenor, J, 'Products Liability and Driverless Cars: Issues and Guiding Principles for Legislation' (2014) Washington DC Brookings Institution, 7.

**Treaties and conventions**

African Union, African Union Convention on Cyber Security and Personal Data Protection (Adopted on 27 June 2014) AU <https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf> accessed 13 February 2023.

OECD, 'Recommendation of the Council on Artificial Intelligence' (Adopted on 22 May 2019) OECD/LEGAL/0449 <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed on 13 February 2023.

Transforming our world: the 2030 Agenda for Sustainable Development, (adopted on 21 October 2015), UNGA A/RES/70/1, <https://www.refworld.org/docid/57b6e3e44.html> accessed 11 October 2022.

United Nations Conference on Trade and Development, *Technology and Innovation Report*, (2021) 31.

United Nations Conference on Trade and Development, *The Least Developed Countries*, (2020)

**Reports**

Akello J, *Artificial Intelligence in Kenya*, Padigrim Initiative (2022), 4.

Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, Building Trust in Human-Centric Artificial Intelligence, (Brussels COM 168 Final, 2019).

Committee on Legal Affairs, *Draft Report with Recommendations to the Commission on Civil Law Rules on Robotics* (European Parliament, A8-0005/2017), 18.

Distributed Ledgers and Artificial Intelligence Taskforce, *Emerging Digital Technologies for Kenya: Exploration and Analysis,* (2019) <https://www.ict.go.ke/blockchain.pdf> accessed 13 February 2023.

European Parliament Resolution 20 October 2020 with Recommendations to the Commission on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies [2020] A9-0186, Art 4.

Expert Group on Liability and New Technologies, *New Technologies Formation, Liability for Artificial Intelligence and Other Emerging Digital Technologies* (Luxembourg: Publications Office of the European Union, 2019), 52-59

Fenech M, Strukelj N and Buston O, *Ethical, social and political challenges of artificial intelligence in health*, (Future Advocacy report for the Wellcome Trust, 2018).

Gaffley M, Adams R and Shyllon O, *Artificial Intelligence. African Insight A Research Summary of the Ethical and Human Rights Implications of AI in Africa* (HSRC & Meta AI and Ethics Human Rights Research Project for Africa, 2022), 5

International Labour Organisation, *The Fourth Industrial Revolution, Artificial Intelligence, and the Future of Work in Egypt*, (ILO 2021).

Madiega T, *Artificial intelligence liability directive* (European Parliamentary Research Service, 2023).

Report from the Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence and other emerging digital technologies* (European Commission, 2019).

Rogerson A, Hankins E et al, *Government AI Readiness Index 2022*, (Oxford Insights, 2022) <https://www.unido.org/sites/default/files/files/2023-01/Government_AI_Readiness_2022_FV.pdf> accessed 12 February 2023.

**Websites and blogs**

Anirudh V K, 'How Does Artificial Intelligence Learn Through Machine Learning Algorithms?' (*Spiceworks*, 10 February 2022) <https://www.spiceworks.com/tech/artificial-intelligence/articles/how-does-ai-learn-through-ml-algorithms/> accessed 13 February 2023.

Briz N and Bender A, 'Key challenges of artificial intelligence: Liability for AI decisions' (*Dentons*, 2021) <https://www.businessgoing.digital/key-challenges-of-artificial-intelligence-liability-for-ai-decisions/> accessed 13 February 2023.

Gluyas L, Day S, 'Who is liable when AI fails to perform?' (*CMS*, 2018) <https://cms.law/en/gbr/publication/artificial-intelligence-who-is-liable-when-ai-fails-to-perform> accessed 10 February 2023.

Gwagwa A, Katchidza P, Siminyu K, Smith M, 'Responsible Artificial Intelligence in Sub Saharan Africa: Landscape and General State of Play' (2021) 5 AI4D <https://ircai.org/wp-content/uploads/2021/03/AI4D_Report_Responsible_AI_in_SSA.pdf> accessed 12 February 2023.

Kelly P, Walsh M, Wyzykiewicz S and Young-Alls S, 'Man vs Machine: Legal liability in Artificial Intelligence contracts and the challenges that can arise' (*DLA piper*, 6 October 2021) <https://www.dlapiper.com/en/insights/publications/2021/10/man-vs-machine-legal-liability-artificial-intelligence-contracts> accessed 14 February 2023.

Kenya Copyright Board, 'Copyright in the Age of Artificial Intelligence' (Copyright News) <https://copyright.go.ke/sites/default/files/newsletters/issue-38.pdf> accessed on 10 February 2023.

Kunhambu A and Rohatgi A, 'Artificial intelligence and the shift in liability' (*ipleaders*, 9 September 2021) <https://blog.ipleaders.in/artificial-intelligence-shift-liability/> accessed on 14 February 2023.

Leiu A, 'Artificial Intelligence ('AI'): Legal Liability Implications' (*Burges and Salmon*, 30 January 2020) < https://www.burges-salmon.com/news-and-insight/legal-updates/commercial/artificial-intelligence-legal-liability-implications> accessed 11 February 2023.

Mumo M, 'Tech Dream Team to Produce Kenya's Blockchain Roadmap' (*Business Daily*, 28 February 2018) <https://www.businessdailyafrica.com/corporate/tech/Ndemo-taskforce-Kenya-blockchain-roadmap-ICT/4258474-4323074-gjwgqnz/index.html> accessed 13 February 2021.

Roovers R, 'Transparency and Responsibility in Artificial Intelligence A call for explainable AI' (*Deloitte*, 2019).

Olivi G and Graves B, 'Dentons Artificial Intelligence Guide 2022: The AI journey—opening our eyes to opportunity and risk' (Dentons, 2022) <https://www.businessgoing.digital/dentons-artificial-intelligence-guide-2022-the-ai-journey-opening-our-eyes-to-opportunity-and-risk/> accessed on 11 February 2023

Wall S and Schellmann H, 'LinkedIn's job matching AI was biased. The company's solution? More AI' *(MIT Technology Review*, 23 June 2021) < https://www.technologyreview.com/2021/06/23/1026825/linkedin-ai-bias-ziprecruiter-monster-artificial-intelligence/> accessed 10 February 2023.

Walsh A, 'Saudi Arabia grants robot citizenship' (*DW*, 28 October 2017) <https://www.dw.com/en/saudi-arabia-grants-citizenship-to-robot-sophia/a-41150856> accessed 10 February 2023.

**LEGISLATION**

Constitution of Kenya 2010, Art 48 and 50.

Computer Misuse and Cybercrimes Act, 2018

Copyright Act, Cap 130.

Consumer Protection Act, 2012.

Data Protection Act, 2019.

Sale of Goods Act, Cap 31.

**CASE LAW**

St Albans City and District Council v International Computers [1996] 4 All ER 481.

Computer Associates UK Ltd v Software Incubator Ltd [2018] EWCA Civ 518.

Winnipeg Condominium Corporation No. 36 v. Bird Construction Co., [1995] 1 S.C.R. 85.

Donoghue v. Stevenson, [1932] A.C. 562 (H.L.) at 580–581.

Mustapha v. Culligan of Canada Ltd 2008 SCC 27 (CanLII), [2008] 2 SCR 114.

Rylands v Fletcher (1868) LR 3 HL 330.

## OTHER SOURCES

Garner B and Black H, Black's Law Dictionary (7th ed, St. Paul Minn: West Group 1999)

University of Helsinki, 'Elements of AI' <https://course.elementsofai.com/1/1> accessed 12 February 2023.