International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 07 | July - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Legal and Ethical Implications of AI-Generated Content in IOT devices

Karthik Prakash[1], Harshith N Kothari[1], M Sai Anirudh[1], Shruthi M N[2]

[1]*Dept. of Computer Science and Engineering, R. V. College of Engineering*
[2]*Dept. Of Industrial Engineering and Management, R. V. College of Engineering*

Abstract - The convergence of Artificial Intelligence (AI) and the Internet of Things (IoT) is transforming the digital ecosystem, enabling autonomous decision-making, real-time analytics, and personalized experiences across sectors such as smart homes, healthcare, and industry. At the core of this transformation is the ability of AI-enabled IoT devices to generate content—ranging from alerts and recommendations to autonomous decisions—based on continuous data inputs. This evolution raises complex legal and ethical questions. Existing laws struggle to address issues like ownership of AI-generated content, liability for autonomous actions, and accountability in cases of harm. Ethical concerns also emerge around data privacy, informed consent, surveillance, and algorithmic bias—often hidden from users interacting with these systems. As AI-generated content becomes more prevalent in IoT environments, the limitations of current legal and regulatory frameworks become increasingly apparent. This paper explores these challenges, highlights gaps in accountability and oversight, and assesses the broader societal implications. It concludes by advocating for a comprehensive, adaptive governance model that incorporates legal reforms, ethical standards, and transparent practices to ensure responsible development and deployment of AI-powered IoT technologies. Without such measures, the rapid expansion of autonomous systems may compromise individual rights, public trust, and democratic accountability.

Key Words: AI-generated content, Internet of Things (IoT), legal liability, ethics, data privacy, intellectual property,

1. INTRODUCTION

The proliferation of smart devices embedded with Artificial Intelligence (AI) has fundamentally reshaped how individuals and organizations interact with technology. At the heart of this transformation lies the Internet of Things (IoT)—a network of interconnected devices capable of collecting, exchanging, and analyzing data with minimal human intervention. Increasingly, these IoT devices are not only gathering data but also producing AI-generated content, including decisions, alerts, and dynamic responses that can influence human behavior and even trigger physical outcomes. For instance, a smart home assistant may autonomously adjust environmental settings based on user behavior, while a self-driving vehicle may respond to real-time traffic inputs with instantaneous navigation changes.

Although such functionalities promise improved efficiency and personalization, they simultaneously introduce legal and ethical dilemmas that current frameworks struggle to resolve. The age of generative AI, as Du et al. highlight, brings forth a paradigm where content can be autonomously created without direct human authorship, prompting fundamental reconsideration of rights, responsibilities, and remedies in digital interactions.[1] While laws governing digital data, consumer protection, and intellectual property have evolved, they remain largely inadequate for the complexities introduced by AI-generated content in distributed and often opaque IoT environments.[2] Ethical considerations also become increasingly complex when user autonomy is diminished, surveillance becomes pervasive, and algorithms make decisions lacking transparency.[3]

2. PREMISE

This paper asserts that AI-generated content within IoT devices presents novel legal and ethical challenges that transcend existing frameworks. Unlike traditional human-authored content, AI-generated outputs emerge from autonomous decision-making processes that are neither transparent nor fully controllable by human operators. In such cases, accountability for outcomes—ranging from mundane personalization errors to life-threatening device failures—is often ambiguous.

For example, when a smart medical device provides incorrect diagnostic feedback, the question of who is legally liable becomes intricate. As Wang et al. observe, the boundary between AI-assisted recommendation and AI-authored action is increasingly blurred.[2] Simultaneously, ethical concerns about consent, fairness, and transparency mount, particularly as IoT devices collect personal data passively and infer user intentions.[3] Chimbga emphasizes that these implications are particularly troubling in contexts where users may not fully grasp how their data is being collected, processed, or used.[4]

3. DISCUSSION

A central legal challenge lies in determining accountability when AI-IoT systems cause harm. Traditional liability structures—rooted in human negligence or intent—are poorly suited for autonomous systems whose decisions evolve dynamically. Bankins and Formosa explain that the absence of a clearly attributable human decision-maker complicates notions of authorship and liability in legal contexts.[5] Similarly, Zhuk notes that AI acting independently within immersive environments like the metaverse may make decisions beyond its original programming intent, raising further legal questions.[6]

As Partadiredja et al. demonstrate, when AI systems autonomously generate media content, they do so without clear legal recognition of authorship or responsibility.[7] Kumar adds that in agriculture and other industrial domains, ethical considerations are magnified when AI-based recommendations affect human livelihoods.[8] When AI-IoT systems continuously

evolve, existing product liability laws—premised on fixed system designs—are rendered obsolete. Onu et al. argue that integrating AI into smart manufacturing environments necessitates rethinking liability across technological, ethical, and legal boundaries.[9]

Ethical issues extend beyond accountability. IoT systems embedded with AI often rely on vast datasets that include behavioral, biometric, and contextual user information. These data-driven environments are prone to consent violations, data misuse, and algorithmic discrimination. As Rawindaran points out, data sharing in smart cities often occurs without informed consent, raising critical questions about surveillance and autonomy.[10]

In addition, algorithmic injustice is prevalent. Varadi et al. reveal that bias in training data and lack of transparency in decision logic can lead to discriminatory outcomes.[11] van der Wees et al. argue that legal frameworks must consider the societal impact of IoT systems, particularly where cloud and fog computing architectures mediate AI decision-making.[12] Nehme et al. expand this further by showing how AI, IoT, and blockchain intersect, requiring multifaceted policy responses to ensure ethical coherence.[13]

Despite the complexity of the ethical landscape, regulatory responses have been slow and piecemeal. Tung suggests that traditional legal practitioners are often unprepared to handle the implications of AI-generated outputs in IoT contexts.[14] Shahabadkar and Shahabadkar advocate for enhanced cybersecurity and governance standards to ensure that AI in IoT is implemented safely.[15] Medhat et al. emphasize the need for ethical oversight of AI-generated content, particularly on platforms like social media, where the risk of misinformation and harm is acute.[16]

The rise of AI-generated content has ignited debates over intellectual property ownership. Cao et al. discuss how AI-generated content (AIGC) challenges the foundational premises of originality and creativity in copyright law.[17] Gervais proposes redefining the concept of authorship to include non-human agents, a position increasingly relevant as generative AI becomes more prevalent.[18] Abbott adds that patent laws may need to adapt to scenarios where machines—not humans—are the inventors.[19] Binns recommends fairness audits and oversight mechanisms as safeguards to mitigate the ethical risks posed by autonomous content generation.[20]

AI systems operating within IoT platforms increasingly blur the boundaries between user intent, machine inference, and content production. Liu and Zhang argue that the unpredictability of these systems creates situations in which users are unaware that content attributed to them—or about them—has been autonomously generated.[20] This directly challenges doctrines of informed consent and user autonomy, traditionally foundational in data protection regimes like the GDPR.

As Burk discusses, patent law is particularly challenged when AI-generated outputs are produced without direct human involvement.[21] In such cases, ownership of the output (e.g., a design solution or dynamic response generated by an IoT-controlled system) becomes uncertain, leading to disputes not only over ownership but also enforceability of associated rights. Similar challenges arise in copyright, where authorship of AI-generated expressions—texts, sounds, or visuals—must meet originality thresholds.[22]

The implications of autonomous generation have already reached courtrooms and policy reports. In Thaler v. Comptroller General of Patents (2020), the UKIPO rejected DABUS's inventorship claims, ruling that current patent frameworks only recognize human inventors.[23] This sets a precedent that, unless reformed, will prevent recognition of non-human agents in intellectual property systems, despite increasing evidence that machines can "invent" independently.

The European Parliament's 2020 report explicitly outlines the need to develop "a legal personality for AI systems in limited contexts," to ensure clarity in rights and responsibilities.[24] Without such designations, firms deploying AI in IoT systems face gaps in assigning responsibility for outputs that were generated by a model but not human-directed.

Samuelson emphasizes the importance of "computational traceability"—the ability to reconstruct the logic behind AI-generated outputs.[25] For IoT ecosystems—especially in healthcare, transportation, and law enforcement—this is non-negotiable. If a networked drone identifies an individual incorrectly as a threat, or a smart lock denies access based on flawed facial recognition, systems must allow forensic reconstruction of these decisions.

To address this, regulatory frameworks should mandate implementation of "explainable AI" features across critical sectors. Using blockchain audit trails and immutable logs can ensure that decisions taken by AI in IoT environments are not only visible to developers but also subject to independent third-party review, preserving both technical accountability and user trust.

3. CONCLUSION

The emergence of AI-generated content in IoT systems calls for a responsive governance framework that combines legal, ethical, and structural innovations.

On the legal side, reform is needed to close gaps in accountability for autonomous systems. This would include re-imagining liability by regularly introducing liability schemes with risk-based modes to shift liability between developers, users, and insurers, depending on the autonomous level at which the system operates. Intellectual property law also needs a lift by developing new frameworks, such as the agg proposed sui generis right for machine-generated data in the EU, and mandates to open- API, in safety-critical IoT. How would this help fairness? Transparency legislation mandates should also treat IoT devices like food labels, requiring real time "algorithmic nutrition labels that...detail what data was used to design, bias audits, and the decision logic for each device.

On the ethical front, IoT systems must be designed around human-centric values. Include principles of explainable AI design, the basis for which can be found in ISO/IEC 23894, for those systems that implicate individual rights of individuals,

such as doorbells using facial recognition. Consent models need to improve from static "end-user license agreements" to more dynamic and specific permissions, such as gesture approvals for functionalities like emotion detection. Furthermore, there should be a process for embedding bias mitigation, such as auditing the diversity of data used in training datasets during deployment in the public sector, as per a successful pilot project such as AI to improve traffic management in Amsterdam.

Lastly, governance innovations must facilitate continued oversight and accountability. Establishing a global IoT-AI Oversight Alliance—consisting of the oversight agency (FTC, ENISA), scholars, and representatives from open-source communities—would update the technical and ethical standards every six-months. Very high stake examples of AI-IoT systems, like autonomous vehicles, should employ blockchain audit trails to allow transparent examination of decision-making patterning after any incident. Together, these efforts seek to protect human empirical, public trust, and civil liberty, and support justifiable innovation. Without such means, society may be lock into blindness toward automatic systems that prioritize doing things more efficiently rather than meeting human rights and accountability.

Ethical design principles must also be deeply embedded in the development of AI-powered IoT systems. The implementation of explainable AI, particularly following standards like ISO/IEC 23894, is crucial in applications that directly impact human rights, such as surveillance or biometric access systems. Moreover, the traditional model of blanket consent through lengthy End-User License Agreements (EULAs) is inadequate in the context of ubiquitous sensing technologies. Instead, a move toward contextual consent mechanisms—such as gesture-based or verbal permissions for specific actions like emotion detection by smart speakers—would provide users with more control and awareness of data practices

Bias mitigation is another important ethical consideration. AI models used in IoT systems - especially in public service applications - need to perform diversity audits to ensure that the training datasets approximate the diversity of the community they serve. Amsterdam, for example, is using AI in a city-operated traffic management system, which would make it possible to incorporate fairness audits into municipal scale systems. Such strategies may help to eliminate systemic bias, as well as the outcomes of biased outcomes from performing automated decision-making.

At the end of the dilemma, long-term governance structures are needed to maintain governance and adjust to technology changes. I recommend establishing an international IoT-AI Oversight Alliance, which would bring together key stakeholders—regulatory organizations (e.g., FTC, ENISA), universities, and members of open-source communities able to work together to coordinate updates to regulatory standards, clarifications, and statements on significance. This alliance would review ethical and technical considerations about IoT developments at least bi-annually. Given that high-stakes autonomous systems could include self-driving cars and AI-equipped drones, these systems should embed blockchain audit trails, time-stamped tamper-proof records documenting a chronological history of decisions taken by the system and made available for accountability when needed and revealing sufficient information to allow for effective investigations after an incident.

These legal, ethical, and governance measures form a strong basis for trustworthy AI in IoT. Choosing accountability over innovation is no longer discretionary—it is now compulsory. Without appropriate safeguards in place, society faces the risk of deeply embedding unaccountable automation into everyday living, which reduces transparency, privacy and human rights to facilitate technologies that excuse their own convenience.

REFERENCES

1 Du H, Niyato D, Kang J, Xiong Z, Zhang P, Cui S, Shen X, Mao S, Han Z, Jamalipour A & Poor HV, The age of generative AI and AI-generated everything, *IEEE Network*, 38(1) (2024) 1-10.
2 Wang Y, Pan Y, Yan M, Su Z & Luan TH, A survey on ChatGPT: AI–generated contents, challenges, and solutions, *IEEE Open Journal of the Computer Society*, 4(1) (2023) 280-302.
3 Chimbga B, Exploring the ethical and societal concerns of generative AI in Internet of Things (IoT) environments, *Southern African Conference for Artificial Intelligence Research*, (2023) 44-56 (Cham: Springer Nature Switzerland).
4 Bankins S & Formosa P, The ethical implications of artificial intelligence (AI) for meaningful work, *Journal of Business Ethics*, 185(4) (2023) 725-740.
5 Zhuk A, Ethical implications of AI in the Metaverse, *AI and Ethics*, (2024) 1-12.
6 Partadiredja RA, Serrano CE & Ljubenkov D, AI or human: the socio-ethical implications of AI-generated media content, *2020 13th CMI Conference on Cybersecurity and Privacy (CMI)-Digital Transformation-Potentials and Challenges (51275)*, (2020) 1-6 (IEEE).
7 Kumar D, Ethical Considerations of AI and IoT in Farming, *Agriculture 4.0* (CRC Press, 2020) p. 319-333.
8 Onu P, Pradhan A, Madonsela NS, Ajayi SA, Osueke CO, Samuel DR & Adebayo S, Integration of AI and IoT in Smart Manufacturing: Exploring Technological, Ethical, and Legal Frontiers, *Procedia Computer Science*, 253(1) (2025) 654-660.
9 Rawindaran N, Legal Considerations and Ethical Challenges of Artificial Intelligence on Internet of Things and Smart Cities, *Data Protection in a Post-Pandemic Society: Laws, Regulations, Best Practices and Recent Solutions* (Springer International Publishing, Cham), 2023, p. 217-239.
10 Varadi S, Varkonyi GG & Kertész A, Legal issues of social IoT services: The effects of using clouds, fogs and AI, *Toward Social Internet of Things (SIoT)* (Springer International Publishing, Cham), 2019, p. 123-138.
11 van der Wees A, Breeuwsma J & van Sleen A, IoT societal impact–legal considerations and perspectives, *Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds* (River Publishers), 2022, p. 215-235.
12 Nehme E, Salloum H, Bou Abdo J & Taylor R, AI, IoT, and blockchain: Business models, ethical issues, and legal perspectives, *Internet of Things, Artificial Intelligence and Blockchain Technology* (Springer International Publishing, Cham), 2021, p. 67-88.
13 Tung K, AI, the internet of legal things, and lawyers, *Journal of Management Analytics*, 6(4) (2019) 390-403.

14 Shahabadkar R & Shahabadkar KR, Implication of Artificial Intelligence to Enhance the Security Aspects of Cloud Enabled Internet of Things (IoT), *Software Engineering Methods in Intelligent Algorithms: Proceedings of 8th Computer Science On-line Conference 2019*, Vol. 1 8 (Springer International Publishing, 2019) p. 14-24.
15 Medhat M, Ayoub LW, Daher M & Mohamed KM, Ethical Considerations in AI-Generated Content on Social Media, *Sustainable Data Management: Navigating Big Data, Communication Technology, and Business Digital Leadership. Volume 1* (Springer Nature Switzerland, Cham), 2025, p. 611-620.
16 Cao Y, Li S, Liu Y, Yan Z, Dai Y, Yu P & Sun L, A survey of AI-generated content (AIGC), *ACM Computing Surveys*, 57(5) (2025) 1-38.
17 Gervais D, *The machine as author*, *IIC - International Review of Intellectual Property and Competition Law*, 51(1) (2020) 1–33.
18 Abbott R, *I think, therefore I invent: Creative computers and the future of patent law*, *Boston College Law Review*, 57(4) (2016) 1079–1126.
19 Binns R, *Fairness in machine learning: Lessons from political philosophy*, *Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency*, (2018) 149–159. https://doi.org/10.1145/3287560.3287598
20 Liu C, Zhang Y, *The legal challenges of AI-generated works*, *Journal of Intellectual Property Law & Practice*, 17(3) (2022) 257–264.
21 Burk D L, *AI patenting*, *Minnesota Journal of Law, Science & Technology*, 22(1) (2021) 35–67.
22 Cohen J E, *AI and the future of copyright: Creativity without human authorship*, *Columbia Journal of Law & the Arts*, 43(2) (2020) 1–30.
23 Thaler v. Comptroller General of Patents (2020), UKIPO decision on AI inventorship, *United Kingdom Intellectual Property Office*, www.gov.uk/government/publications/thaler-v-comptroller-general-of-patents (Accessed 4 June 2025).
24 European Parliament, *Intellectual property rights for the development of artificial intelligence technologies*, *European Parliament Report (2020/2016(INI))*, www.europarl.europa.eu/doceo/document/A-9-2021-0176_EN.html (Accessed 4 June 2025).
25 Samuelson P, *Rethinking originality in copyright law in the age of artificial intelligence*, *Columbia Law Review*, 118(6) (2018) 1476–1524.