



Article

Review of Ethical Implications of AI: Balancing Innovation and Privacy in Digital Societies

Rusul J. Alsaedi^{*1}, Mustafa Radif²

1. Al-Qasim Green University, Babylon 51013, Iraq

2. University of Al-Qadisiyah, Al Diwaniyah, Iraq

* Correspondence: rusul@uoqasim.edu.iq

Abstract: Artificial intelligence (AI) has a big impact on how digital societies are formed in many areas, especially in research, government, and healthcare. AI also has to do with keeping personal information safe. This study looks at the moral issues that come up with AI. It stresses protecting basic rights and encouraging new ideas. This study looks at both sides of AI, including its ability to change things and the worries that come with it, as well as algorithmic decision-making and community surveillance. This study looks at modern ethical frameworks and governance models, stresses global efforts, and adds trust to AI systems. It stresses how important it is to protect users' privacy and calls for ethical AI. This study says that we should promote and improve technology in a way that is fair and focuses on people.

Keywords: AI Systems, Ethics, Digital Societies, Balance, Privacy

1. Introduction

AI has a big impact on the 21st century. The many benefits, especially in medical diagnosis and instruction, are changing businesses and how people live their lives. It is also used to automate tasks related to money and logistics [1]. In digital communities and beyond, the need for AI is becoming more and clearer.

AI has many benefits, but it also raises serious moral questions about fairness and privacy. AI systems sometimes collect a lot of personal information through online behaviors or sensors, which are then used to make sensitive information without explicit consent [2], [3]. This leads to a lot of controversy about how data should be collected, who should collect it, and how it should be regulated, especially when algorithms undermine important rights like freedom of speech and due process [4].

Many AI systems are hard to understand and include "black boxes" that make it hard to get accurate results or challenge them [5]. This makes the ethics of AI more challenging. We ask businesses, civil society groups, and governments to take aggressive steps to make sure that AI development is in line with moral and social principles.

The major goal of this study is to look at the moral effects of AI on digital society, focusing on how to find a balance between privacy and innovation. This article looks into how AI can be both a major threat to human rights and a driver of progress. This report shows the future path of AI growth, which is backed up by frameworks that protect privacy and ethics.

Citation: Alsaedi, R. J., & Radif, M. Review of Ethical Implications of AI: Balancing Innovation and Privacy in Digital Societies. Central Asian Journal of Mathematical Theory and Computer Sciences 2025, 6(4), 889-893.

Received: 30th Jun 2025

Revised: 11th Jul 2025

Accepted: 31st Jul 2025

Published: 31st Aug 2025



Copyright: © 2025 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

(<https://creativecommons.org/licenses/by/4.0/>)

The Two Sides of AI Innovation

AI has the ability to change every part of life in a big way. It can predict things like early disease diagnosis and the transfer of smart technologies. In healthcare, it is used to improve AI-powered diagnostic tools and make it easier to quickly find diseases like cancer and diabetes [6]. In education, it helps a lot with building adaptive AI that meets the demands of students, which makes them more interested and improves their learning results [7]. Artificial intelligence is great at public administration, making decisions, analyzing information, predicting the future, meeting individual needs, and improving response [8].

The technology that makes these systems work also poses a number of risks. Security and law enforcement agencies use a lot of AI to help them make decisions. This has an effect on people's rights and freedoms. People have used surveillance cameras to recognize faces in public places and for law enforcement [9]. The widespread use of AI-powered surveillance technology in China has drawn worldwide criticism for violating human rights [10].

Artificial intelligence (AI) can make people's biases even stronger. The use of algorithms in predictive policing units to predict crimes that disproportionately affect certain groups or minorities shows that the cycles of effective policing and too much policing are still going on. Algorithmic bias in loan approval processes and hiring platforms might cause unfair discrimination based on race, gender, and other personal attributes [11], [12].

Duality: Because of this, AI works to find possible sources of threat. The need comes up here. AI's goal is to make life easier for vulnerable people by reducing pain and risks, protecting marginalized minorities, and upholding democratic values.

2. Materials and Methods

AI Applications and Privacy Issues

As AI and digital technology get better; people are becoming more worried about data privacy. To improve machine learning training, artificial intelligence often combines large amounts of data. This information is often about behavior, personal information, or biometric data. Using and getting data is important for improving algorithms, but it also raises a lot of legal and moral questions.

Many people don't know how key AI applications acquire, share, and analyze data. The ideas of consent for using social media and e-commerce make this possible. Algorithms check user activity from time to time to build a complete profile that is used for content and advertising suggestions. "Surveillance capitalism" is the term used to describe this data and its rise, in which privacy is less important than making money for businesses.

The impacts of commercial actions go beyond what they do. One of the most interesting things about AI is that it can watch people in real time. Cameras have been used to find the faces of suspects in cities, even in quarantine zones, to keep an eye on rising temperatures, or to watch how people act without any legal protections or public input. Without laws about surveillance, these gadgets are a big threat to people's safety and freedom.

Anonymous data stays anonymous, which is a big danger. Even after being taken out of other databases, artificial intelligence may reconstruct anonymous human identities. Destruction provides you the chance to directly protect your data privacy.

Keeping data safe is really important. Artificial intelligence must be responsible for keeping information safe and protecting data because AI systems and technologies are naturally vulnerable to hacking, attacks, and output manipulation. The main job of AI is a

big and hard task. To attain justice, this requires strong rules, constant inspection, following the law, and being open about things.

3. Results and Discussion

Ethics and AI Governance

Because AI is developing so quickly, ethical governance has become a key part of AI responsibility. At first, decisions were made about technologies and access to biometric surveillance, which goes beyond just technical monitoring. This protects personal freedoms and democracy in the fight for social justice.

There are two main philosophical foundations for AI ethics. The socially beneficial method focuses on results, while the ethical approach protects people and their rights no matter what happens. Beneficiaries say that the ethical framework for AI surveillance is bad since it takes away their freedom. To come up with fair rules that take into account the situation, artificial intelligence and its ethical issues must find a way to bring these two points of view together.

The National Authority has been told what the rules are for how to use AI in a moral way. The Principle of Economic Cooperation and Development through Artificial Intelligence stresses important issues such fairness, responsibility, openness, and the strength of rights. The European Commission came up with the proposed AI legislation in 2021. Its goal is to make rules for hazards and make sure that high-risk AI technology used in jobs, law enforcement, and important infrastructure follows stricter and stricter rules [13], [14].

Many businesses have developed rules for AI ethics, which has made the government's dollar work. Microsoft, Google, and other big digital corporations have put out clear rules based on fairness, safety, privacy, and human control. Some detractors also say that autonomous systems generally don't have enough enforcement, which might make them look worse in the eyes of the public. Ethical obligations don't work if people aren't held accountable, and this doesn't stop harm.

To prevent making decisions that are too risky, bidding, human monitoring, and algorithmic transparency should all be given more attention. It is now a moral and legal obligation for technology that don't affect healthcare or criminal justice to be "explainable". Also, systems that use deep learning models still have a big problem: they are hard to understand directly.

There is still not enough global coordination. The UNESCO Recommendation on the Ethics of Artificial Intelligence is a big step toward getting everyone to agree on something. Economic and geopolitical conflicts are still making it hard for the world to agree on how to manage AI [15].

So, along with technology, ethical and legal frameworks must be put in place that is based on open conversation and the public benefit. It is necessary to use an integrative approach that includes sociology, computer science, law, ethics, and community opinions. This is helpful and necessary for building an AI system that serves all parts of society and promotes equality.

Finding a Balance between Privacy and New Ideas

One of the biggest problems with AI is finding a way to preserve people's privacy while yet making technology better. As a result, AI innovation is a huge step forward that brings big economic and societal benefits by changing the way transportation and healthcare work and making them safer and more secure. Also, these benefits often come from collecting personal data and the chance for pluralism [16]. This ends the discussion of how much AI may be used without violating civil liberties and privacy.

Through one of the privacy-preserving methods, that let AI does complicated analysis without giving out or putting data at risk. For example, adding the obfuscation

feature to all data illustrates the detection of generic patterns without giving away user information [17], [18]. Federated learning is another example of this. It trains artificial models on various servers or devices without moving raw data, which helps close information gaps [19].

One key thing to think about is how to use as little data as possible. Systems are made to just collect the data they need to do a certain job. The General Data Protection Regulation (GDPR) of the European Union is based on this idea. It sets tight rules for how personal data can be processed, including identifying the purpose and getting user consent [20].

For consumers to find a balance between privacy and innovation, they need to know how AI systems work with their data and look into any legal or social effects [21]. The creation of AI systems that utilize interpretative reasoning (XAI) to figure out why algorithms make judgments shows that oversight is trustworthy, open, and accountable [22], [23].

For AI to grow and last, people in the community need to trust it. Sometimes, some customers may not want to use technologies that could be helpful to them. So, openness, together with communication and ethical design, is very important for building trust and making people feel like they belong in the community [24], [25].

So, participation and making governance more inclusive are important for keeping up with new ideas and moving society forward. Getting stakeholders, especially those who are less fortunate, involved in the design and use of AI systems reduces harm and the risk of exclusion while improving AI governance frameworks [26].

The statement requires that privacy be included in broad policies that cover technological progress, inclusive governance, and strict rules. Combining AI development with privacy can lead to new ideas that respect human rights and democratic values.

Suggestions for policy and practice

- a. Design and Ethics: Users must think about and include ethical privacy issues at every stage of the AI lifecycle.
- b. Better Regulation: National and international laws can make sure that developers are responsible for the harm caused by AI.
- c. AI systems: Must be easy to understand when they harm rights and freedoms.
- d. Public Engagement: AI's ability to help people learn about and talk about trust and informed conversation.
- e. Diversity through Participation: Include people from underrepresented groups in the process to reduce bias in AI output.

4. Conclusion

This paper shows that the most fundamental ethical challenges of AI in digital society are namely how to protect privacy while yet allowing for new ideas. There are a lot of good things in AI, but there are also critical facts and problems that need to be dealt with. To make sure that AI helps people grow without violating their basic rights, societies need to embrace strong ethical frameworks, privacy-protecting systems, and broad and significant legislation. This is important for a responsible way to create and manage AI.

REFERENCES

- [1] M. Brundage, S. Avin, J. Clark, et al., Using AI for bad things: predicting, stopping, and lessening the damage, Institute for the Future of Humanity, 2018.
- [2] K. Crawford, Atlas of AI: The Political, Economic, and Environmental Costs of AI, Yale University Press, 2021.
- [3] C. Dwork and A. Roth, "The algorithmic basis of differential privacy," Foundations and Trends® in Theoretical Computer Science, vol. 9, no. 3–4, pp. 211–407, 2014.

- [4] V. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, St. Martin's Press, 2018.
- [5] European Commission, "Proposal for a Regulation that sets out clear rules for artificial intelligence (the Artificial Intelligence Act)," 2021.
- [6] EU, "Regulation on the Protection of Personal Data (GDPR)," Regulation (EU) 2016/679, 2016.
- [7] A. G. Ferguson, *The Rise of Big Data Policing: Race, Surveillance, and the Future of Law Enforcement*, NYU Press, 2017.
- [8] L. Floridi and J. Cowls, "A set of five principles that all agree on for AI in society," *Harvard Data Science Review*, vol. 1, no. 1, 2019.
- [9] D. Gunning and D. Aha, "The Explainable Artificial Intelligence (XAI) Program at DARPA," *AI Magazine*, vol. 40, no. 2, pp. 44–58, 2019.
- [10] J. Isaak and M. J. Hanna, "Facebook, Cambridge Analytica, and Privacy Protection: Protecting User Data," *Computer*, vol. 51, no. 8, pp. 56–59, 2018.
- [11] A. Jobin, M. Ienca, and E. Vayena, "The world of AI ethical rules," *Nature Machine Intelligence*, vol. 1, no. 9, pp. 389–399, 2019.
- [12] P. Kairouz, H. B. McMahan, et al., "Federated Learning: Progress and Open Issues," Preprint on Arxiv, arxiv:1912.04977, 2019.
- [13] R. Luckin, W. Holmes, M. Griffiths, and L. B. Forcier, *Intelligence Unleashed: Why AI Should Be Used in Schools*, Pearson, 2016.
- [14] J. Morley, L. Floridi, L. Kinsey, and A. Elhalal, "From What to How: A First Look at AI Ethics Tools, Methods, and Research That Are Open to the Public to Turn Principles into Action," *Science and Engineering Ethics*, vol. 26, no. 4, pp. 2141–2168, 2020.
- [15] P. Mozur, "Inside China's nightmarish dreams: A.I., shame, and a lot of cameras," *The New York Times*, 2018.
- [16] A. Narayanan and V. Shmatikov, "Strongly de-anonymizing large, sparse datasets," *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, pp. 111–125, 2008.
- [17] S. U. Noble, *Algorithms of Oppression: How Search Engines Make Racism Worse*, OECD, NYU Press, 2018.
- [18] F. Pasquale, *The Black Box Society: The Hidden Algorithms That Control Money and Data*, Harvard University Press, 2015.
- [19] N. A. Smuha, "A European way of looking at AI: from moral principles to laws that everyone should follow," *Philosophy & Technology*, vol. 34, no. 3, pp. 491–514, 2021.
- [20] E. Topol, *Deep Medicine: How AI Can Make Healthcare More Human Again*, Basic Books, 2019.
- [21] United Nations Educational, Scientific, and Cultural Organization (UNESCO), "Advice on the moral issues surrounding AI," 2021.
- [22] S. Wachter, B. Mittelstadt, and L. Floridi, "AI for robotics that is clear, understandable, and responsible," *Science Robotics*, vol. 2, no. 6, ean6080, 2017.
- [23] S. Wachter, B. Mittelstadt, and L. Floridi, "There is no right to an explanation of automated decision-making in the General Data Protection Regulation," *International Data Privacy Law*, vol. 7, no. 2, pp. 76–99, 2017.
- [24] J. Whittlestone, R. Nyrop, A. Alexandrova, and S. Cave, "The Role and Limits of Principles in AI Ethics: Moving Toward a Focus on Conflicts," *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, pp. 195–200, 2019.
- [25] Y. Zhou, X. Jin, and C. Zhang, "Using AI in Government: Pros and Cons," *Quarterly Journal of Government Information*, vol. 37, no. 3, 101481, 2020.
- [26] S. Zuboff, *The Age of Surveillance Capitalism: The Battle for a Human Future at the New Frontier of Power*, Public Affairs, 2019.