

18

Technology, AI & Digital Freedom

Mr. Aleem Khan^{1*} & Dr. Ravi Shankar Sharma²

^{1,2}Assistant Professor, S.S. Jain Subodh P.G. College, Jaipur.

*Corresponding Author: aleem.khan@live.com

Abstract

Digital technologies and artificial intelligence (AI) are transforming how people communicate, learn, work, access public services and participate in society. These technologies create opportunities for innovation, accessibility, economic growth and knowledge sharing. However, they also raise concerns regarding privacy, surveillance, algorithmic discrimination, misinformation and unequal access to digital resources. Digital freedom refers to the ability of individuals to participate in digital environments while enjoying privacy, freedom of expression, equal opportunities and control over their personal information. This chapter examines the relationship between technology, AI and digital freedom, highlighting major opportunities, challenges and ethical responsibilities. It argues that technological progress should be accompanied by transparency, accountability, cybersecurity, inclusion and meaningful human oversight. Drawing on international frameworks, including UNESCO's Recommendation on the Ethics of Artificial Intelligence and the National Institute of Standards and Technology's AI Risk Management Framework, the chapter proposes principles for developing a fair, inclusive and rights-respecting digital society.

Keywords: Artificial Intelligence, Digital Freedom, Data Privacy, Human Rights, Digital Inclusion, Algorithmic Bias, Cybersecurity, AI Ethics, Accountability, Digital Governance.

Introduction

Technology has become an essential part of modern life. Smartphones, computers, social media, online education, digital payments and cloud computing have changed how individuals interact with the world. Artificial intelligence has further accelerated this transformation by enabling machines to analyse information, recognise patterns, generate content and assist in decision-making.

AI can support education, healthcare, scientific research, business operations and public administration. At the same time, its growing influence raises important questions about individual freedom, privacy and social responsibility. For example, automated systems may influence the information people see, the services they receive and the opportunities available to them.

Digital freedom is therefore not simply about having access to the internet. It also involves the ability to use digital services safely, express opinions, protect personal information, access reliable knowledge and challenge unfair decisions. The United Nations Global Digital Compact emphasises international cooperation to create an inclusive, open, safe and secure digital environment [1].

This chapter explores how technology and AI can promote digital freedom while examining the safeguards necessary to protect human rights and individual autonomy.

Understanding Technology, AI and Digital Freedom

Technology refers to the tools, systems and processes developed to solve problems and perform tasks. Artificial intelligence is a branch of computing concerned with systems that perform tasks such as prediction, classification, language processing and content generation.

Digital freedom is the ability to participate meaningfully in digital life while retaining fundamental rights and personal agency. It includes several important dimensions:

- **Freedom of Expression:** The ability to communicate ideas and opinions online within rights-respecting legal frameworks.
- **Privacy and Data Protection:** The ability to understand and exercise appropriate control over the collection and use of personal information.
- **Digital Inclusion:** Access to affordable connectivity, devices, accessible services and digital skills.
- **Fairness and Accountability:** Protection against unjust discrimination and access to mechanisms for challenging consequential decisions.
- **Security and Autonomy:** Protection from cyber threats, manipulation and excessive monitoring.

These dimensions are interconnected. Internet access alone cannot guarantee freedom if users are subjected to intrusive surveillance or discriminatory automated decisions. A responsible digital society must therefore combine technological innovation with effective safeguards.

Opportunities Created by AI and Digital Technology

- **Education and Knowledge**

Digital platforms provide educational resources to learners regardless of geographical location. AI-powered tools can assist with language translation, personalised explanations, accessibility and research. They may help teachers prepare learning materials and provide students with additional learning support.

However, AI-generated information can contain errors. Students and educators should verify important claims, protect personal information and use AI to support rather than replace independent thinking.

- **Healthcare and Public Services**

AI can assist healthcare professionals in analysing medical information, identifying patterns and supporting research. Digital public services can simplify administrative procedures and reduce the need for physical visits.

Nevertheless, decisions affecting health, welfare or legal rights require appropriate professional oversight, understandable explanations and opportunities to correct errors.

- **Economic Growth and Employment**

Businesses can use AI to improve productivity, analyse market trends and automate repetitive tasks. Digital platforms also enable entrepreneurs to reach wider audiences and provide services online.

However, automation may change job requirements and displace some tasks. Governments, educational institutions and employers should promote digital skills, retraining and opportunities for workers to adapt.

- **Accessibility and Participation**

Assistive technologies, speech recognition, captions and translation tools can help people with disabilities or language barriers participate in digital environments. Online platforms can also support civic engagement and community collaboration.

These benefits depend on affordable access, accessible design and the inclusion of diverse communities in technology development.

Challenges to Digital Freedom

- **Privacy and Surveillance**

Digital platforms may collect personal information such as location, browsing behaviour and communication preferences. Excessive collection or unauthorised use of this information can threaten privacy and personal autonomy.

Privacy protection should be integrated into system design through data minimisation, secure storage, clear privacy notices and appropriate limits on data

retention. UNESCO's AI ethics recommendation emphasises protecting privacy and personal data throughout the AI life cycle [2].

- **Algorithmic Bias and Discrimination**

AI systems learn from data and human design decisions. If their training data contain historical inequalities or inadequately represent certain groups, their outputs may produce unfair results.

For example, an automated recruitment system could disadvantage qualified applicants if it relies on biased historical hiring data. Developers should test systems for unequal error rates, document limitations and provide procedures for reviewing harmful decisions.

- **Misinformation and Synthetic Content**

AI tools can generate realistic but inaccurate text, images, audio and video. Such content may mislead people, damage reputations and reduce trust in reliable information.

Digital literacy, fact-checking, responsible platform policies and appropriate content-provenance measures can help individuals evaluate online information critically.

- **Lack of Transparency and Accountability**

Some AI systems are difficult to understand, even for their users. When an automated system affects employment, education, credit or public benefits, affected individuals should receive suitable explanations and have access to meaningful review.

The NIST AI Risk Management Framework identifies trustworthiness characteristics such as validity, safety, security, transparency, explainability, privacy and fairness [3].

- **Digital Inequality**

People may be excluded from digital opportunities because of income, disability, geographical location, language or limited digital skills. Unequal access can widen existing social and economic inequalities.

Affordable connectivity, accessible public services, digital education and multilingual resources are important for reducing this divide.

Principles for Protecting Digital Freedom

A rights-respecting digital environment requires practical safeguards throughout the development and use of technology.

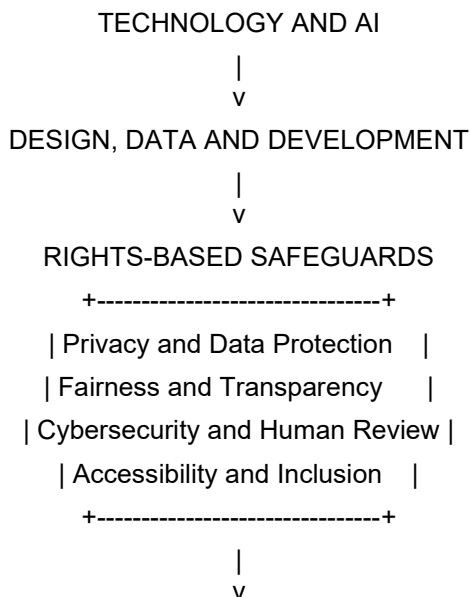
- **Privacy by Design:** Organisations should collect only necessary information, explain its purpose and protect it against unauthorised access.

- **Transparency:** Users should be informed when AI is used in consequential contexts and should receive explanations appropriate to the importance of the decision.
- **Fairness:** AI systems should be tested for bias before deployment and monitored for unequal outcomes after implementation.
- **Human Oversight:** Automated systems should not eliminate meaningful human review where significant rights or interests are affected.
- **Security:** Developers and organisations should use secure development practices, access controls, software updates and appropriate incident-response procedures.
- **Inclusion and Accessibility:** Digital services should accommodate different abilities, languages, income levels and levels of digital literacy. Alternative access arrangements should be considered for essential services.
- **Accountability:** Organisations should identify who is responsible for system performance, investigate complaints and provide suitable remedies when harm occurs.

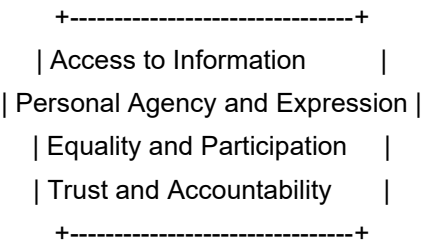
These principles align with international efforts to promote responsible AI and inclusive digital cooperation [1–3].

Figure 1: A Rights-Centred Framework for Digital Freedom

The following diagram illustrates how safeguards connect technological development with positive social outcomes.



DIGITAL FREEDOM OUTCOMES



FEEDBACK, AUDITS AND IMPROVEMENT

+----> Continuous Review

Source: Author’s conceptual framework informed by UNESCO [2] and NIST [3].

Table 1: Major Risks to Digital Freedom and Possible Safeguards

Risk	Possible impact	Recommended safeguard
Privacy violations	Loss of control over personal information	Data minimisation and secure storage
Algorithmic bias	Unfair treatment or exclusion	Bias testing and independent audits
Misinformation	Confusion and reduced public trust	Media literacy and fact-checking
Opaque AI decisions	Difficulty understanding or challenging outcomes	Clear explanations and human review
Digital inequality	Unequal access to opportunities	Affordable connectivity and digital education
Cybersecurity threats	Data theft and service disruption	Secure development and incident response

Source: Author’s synthesis based on UNESCO [2] and NIST [3].

Responsibilities of Governments, Organizations and Individuals

Governments should establish effective legal protections for privacy, equality, freedom of expression and due process. Regulatory measures should be proportionate to the risks involved and supported by appropriate oversight.

Technology companies should explain how their systems operate, minimise unnecessary data collection, test for bias and provide accessible complaint procedures. Organisations adopting AI should assess its likely impact before deployment and monitor its performance over time.

Educational institutions should develop digital literacy, critical thinking, cybersecurity awareness and responsible AI-use practices. Students should learn to verify generated information and distinguish reliable evidence from unsupported claims.

Individuals can use strong passwords, multi-factor authentication, software updates and privacy settings to improve their digital security. Nevertheless, personal precautions cannot replace the responsibilities of organisations that design and operate digital systems.

Table 2: Translating Digital Freedom Principles into Practice

Principle	Practical action	Expected benefit
Privacy	Limit unnecessary data collection	Greater personal control
Transparency	Explain AI use and important decisions	Improved understanding
Fairness	Test systems across relevant user groups	Reduced discriminatory outcomes
Accountability	Establish complaint and review procedures	Clear responsibility
Inclusion	Provide accessible and affordable services	Broader participation
Human oversight	Enable review of consequential decisions	Better protection of rights

Source: Author's recommendations informed by international AI governance frameworks [1–3].

Conclusion

Technology and artificial intelligence offer significant opportunities to improve education, healthcare, economic participation, accessibility and communication. However, these benefits are not automatic. Poorly governed systems can undermine privacy, reinforce discrimination, spread misinformation and exclude people who lack digital access or skills.

Digital freedom must therefore be treated as a fundamental consideration in the design, regulation and use of technology. Privacy, transparency, fairness, cybersecurity, accessibility and meaningful human oversight should be incorporated throughout the AI life cycle. Governments, businesses, educational institutions, researchers and individuals all have responsibilities in achieving these objectives.

International frameworks provide useful guidance, but their principles must be translated into effective laws, institutional policies and everyday practices. Ultimately, successful digital transformation should not be measured only by technological capability or economic efficiency. It should also be assessed by whether people can participate safely, make informed choices, protect their rights and challenge decisions that affect their lives.

The central goal is to ensure that technology remains a tool for human empowerment. AI should strengthen human agency rather than replace individual judgment or diminish fundamental freedoms.

References

1. United Nations. (2024). *Global Digital Compact*. In *Pact for the Future* (A/RES/79/1). <https://www.un.org/en/summit-of-the-future/global-digital-compact>
2. UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*. United Nations Educational, Scientific and Cultural Organization. <https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence>
3. Tabassi, E. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.AI.100-1>
4. United Nations General Assembly. (1948). *Universal Declaration of Human Rights*. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>
5. Organisation for Economic Co-operation and Development (OECD). (2019, updated 2024). *OECD AI Principles*. <https://oecd.ai/en/ai-principles>.

