

# Research report IMZMUN 2025



**IMZ** | MODEL  
UNITED  
NATIONS

**Human Rights in the Digital Age:  
Ensuring Equity and Privacy**

version 2025.03

## Table of content

1. Introduction .....	3
2. Digital Access and Equity .....	4
3. Privacy in the Digital Era .....	6
4. Technology and Human Rights .....	8
5. Global Governance and Policy Frameworks .....	10
6. Further considerations .....	12

Published in March 2025  
Published for the attendees of the IMZMUN 2025 only.  
Website: [www.mun.montana-zug.ch](http://www.mun.montana-zug.ch)

Contributors: Vanssh, Dillon, Faustine, Zaure, Inti & PJ Widen of the IMZMUN 2025 Secretariat

Care has been taken to acknowledge sources.  
If your source has not been acknowledged, please inform us at [info@imzmun.ch](mailto:info@imzmun.ch) and it will be updated with the next published version.

Please care about the environment and hence think twice before you print this publication!

© IMZMUN 2025

## 1. Introduction

The digital revolution has transformed nearly every aspect of modern life, from communication and education to healthcare and governance. While technology offers unprecedented opportunities for progress, it also raises critical questions about equity and privacy. Access to digital tools and the internet is now a fundamental driver of economic and social inclusion, yet billions of people remain disconnected. At the same time, the widespread collection and use of personal data present ethical and legal challenges, with governments and corporations struggling to balance security, economic interests and individual rights.

In the context of the Sustainable Development Goals (SDGs), digital access and privacy are deeply linked to broader global challenges. SDG10 (Reducing Inequalities) highlights the need to close the digital divide, ensuring that technological advancements benefit all, rather than deepening existing disparities. Similarly, SDG16 (Peace, Justice and Strong Institutions) emphasizes the importance of governance structures that protect digital rights, ensuring that emerging technologies do not become tools of surveillance, misinformation, or social control.

Given the complexity of these issues, addressing them requires a multi-layered approach. Examining digital rights as a single entity overlooks the different ways technology impacts people worldwide. Breaking the topic into distinct areas – such as digital access and equity, privacy in the digital era, AI and misinformation and global governance frameworks – allows for a more comprehensive analysis of both challenges and solutions. Each of these areas interacts with the others, requiring cooperation between governments, businesses, civil society and international organizations to ensure a digital future that is both inclusive and ethical.

The following sections will explore these key dimensions, examining the barriers to equitable digital access, the ethical dilemmas of online privacy, the role of AI in shaping information flows and the need for strong governance frameworks to regulate digital spaces.

## 2. Digital Access and Equity

### i. Defining the Issue

The digital divide refers to disparities in internet access, technology and digital literacy between different groups, such as urban and rural populations or developed and developing nations. This issue is complex due to economic, infrastructural and political factors that hinder universal access to digital tools. In the modern information age, lack of digital access creates inequalities in education, employment and societal development. Some communities face additional barriers, such as a lack of electricity, making digital inclusion even more challenging.

### ii. Key Terms

- **Digital literacy:** The ability to understand, access and communicate safely through digital technologies.
- **ICT (Information and Communication Technology):** Includes devices (e.g. phones, laptops), networks (e.g. internet, mobile networks) and services (e.g. online education, online banking).

### iii. Stances of Important Parties Involved

Efforts to bridge the digital divide are widely supported, as digital literacy enhances economic productivity. Various nations and organizations have implemented policies to address this issue:

- **China:** China's Consumer Trade-In Scheme is a government initiative aimed at stimulating domestic consumption and technological adoption. The program subsidizes the purchase of new digital devices, including smartphones, tablets and computers, making them more accessible to a broader segment of the population.
- **United States:** Ran the Affordable Connectivity Program (2021–2024), subsidizing internet costs for low-income households, benefiting over 23 million households with \$14.2 billion in aid.
- **Africa:** Elon Musk's Starlink satellite internet service operates in 19 African nations, providing affordable and reliable internet access, with plans to expand to 15 more countries.

### iv. Previous Attempts to Deal with the Issue

- **United Nations Volunteers Program (2000):** Launched an online volunteering service to use ICT for digital inclusion.
- **Libraries in South Africa & Kenya:** Serve as digital access hubs for community members.
- **U.S. Digital Inclusion Initiatives:** Provide affordable access to networks and educational technologies for children and low-income communities.
- **Global Digital Compact (2024, UN Initiative):** Aims to ensure universal internet access, prevent internet fragmentation, regulate AI and emphasize data protection.

### v. Suggested Possible Solutions

- **Tailored regional approaches:** While Western Europe may benefit from affordability initiatives, Africa requires infrastructure expansion.

- **Collaboration:** Governments, international businesses and NGOs must work together to connect over 2 billion unconnected people.
- **Education reform:** Digital literacy should be integrated into educational curricula to ensure accessibility and usability.

## vi. Sources Used and Recommended Readings

- [North Carolina Broadband](#)
- [UNESCO TVETipedia](#)
- [Wikipedia: Digital Divide](#)
- [Digital Responsibility](#)
- [Wikipedia: Global Digital Compact](#)
- [Reuters: China's Consumer Trade-In Scheme](#)
- [Wikipedia: Affordable Connectivity Program](#)
- [Le Monde: Starlink's Expansion in Africa](#)
- [Rest of World: Starlink's Internet Costs in Africa](#)
- [Reuters: Ending the Digital Divide](#)

## 3. Privacy in the Digital Era

### i. Defining the Issue

The digital age presents significant challenges to personal privacy, with governments and corporations collecting vast amounts of user data. The ethical debate centres on balancing security, economic interests and individual rights. Governments justify surveillance for national security, but excessive monitoring can infringe on personal freedoms. Meanwhile, large corporations profit from personal data, creating conflicts between economic gain and ethical responsibility. Additionally, inconsistent privacy laws across countries complicate international regulation efforts.

### ii. Key Terms

- **Data Privacy:** The right of individuals to control their personal information.
- **Surveillance:** The monitoring of individuals by governments or corporations.
- **General Data Protection Regulation (GDPR):** A strict European privacy law regulating data collection.
- **Big Data:** Large-scale data sets used for analysis and decision-making.
- **Digital Exploitation:** The misuse of personal data for profit, manipulation, or harm.

### iii. Stances of Important Parties Involved

- **United States:** Supports surveillance for national security; weak federal privacy laws, but some state laws (e.g. CCPA in California).
- **European Union:** Strong privacy protections under GDPR, regulating corporate data practices.
- **China:** Implements extensive government surveillance with strict data control and censorship policies.
- **United Nations:** Advocates for digital rights and ethical AI use.
- **Electronic Frontier Foundation (EFF):** Supports stronger privacy laws and transparency.
- **Technology Companies:** Defend data collection as necessary for innovation but face criticism over privacy violations.

### iv. Previous Attempts to Address the Issue

- **General Data Protection Regulation (GDPR, 2018):** Enforces strict data protection laws across the EU.
- **USA PATRIOT Act (2001):** Expanded U.S. government surveillance powers, sparking controversy.
- **EU-U.S. Privacy Shield (2016 - 2020):** Regulated transatlantic data transfers but was invalidated due to privacy concerns.
- **United Nations Resolutions on Privacy (2013 - present):** Advocate for privacy rights in the digital age.

## v. Suggested Possible Solutions

- **Regulating Big Tech:** Introducing stricter laws to prevent excessive data collection and misuse.
- **Enhancing Digital Literacy:** Educating vulnerable populations on online privacy risks.
- **Balancing Security and Privacy:** Implementing oversight mechanisms for government surveillance.
- **Stronger International Cooperation:** Creating a global treaty on digital privacy and data protection.
- **Encouraging Privacy-Respecting Technologies:** Promoting encryption and decentralized data storage.

## vi. Sources Used and Recommended Readings

- [Legal framework of EU data protection - European Commission](#)
- [Third Committee Resolutions on Digital Privacy - United Nations](#)
- [USA PATRIOT Act Overview](#)

## 4. Technology and Human Rights

### i. Defining the Issue

The rapid advancement of digital technologies, including artificial intelligence (AI) and big data, has transformed modern society, offering new opportunities for economic growth, communication and governance. However, these innovations also raise significant human rights concerns, such as privacy violations, algorithmic bias, misinformation and digital discrimination. The challenge lies in ensuring that technology serves as a tool for human progress rather than a means of control, exclusion, or manipulation.

### ii. Key Terms

- **Algorithmic Bias:** Algorithmic bias refers to the tendency of artificial intelligence (AI) systems to produce unfair, discriminatory, or unequal outcomes, particularly impacting marginalized groups such as racial minorities, women and low-income individuals.
- **Digital Self-Determination:** The right of individuals to control their digital identities, data and online interactions.
- **Surveillance Capitalism:** A business model where personal data is collected and monetized, influencing human behaviour and decision-making.

### iii. Stances of Important Parties Involved

- **Governments:** Policies vary from strict data protection laws to extensive surveillance measures for national security.
- **Technology Companies:** Some advocate for self-regulation and innovation, while others acknowledge the need for ethical oversight.
- **Civil Society Organizations:** Advocate for stronger privacy protections, ethical AI development and digital rights.

### iv. Previous Attempts to Address the Issue

- **Toronto Declaration (2018):** Emphasizes equality and non-discrimination in AI development.
- **OECD Principles on AI (2019):** Calls for responsible AI use aligned with human rights and democratic values.
- **Council of Europe's Framework Convention on AI (2024):** A legally binding treaty to prevent AI misuse and uphold human rights.

### v. Suggested Possible Solutions

- **International Regulatory Frameworks:** Binding agreements to set ethical standards for AI and digital governance.
- **Transparency and Accountability:** Mandating that companies disclose data collection practices and algorithmic decisions.
- **Enhancing Digital Literacy:** Educating individuals on their digital rights and online safety.



- **Multi-Stakeholder Collaboration:** Involving governments, corporations and civil society in policymaking to ensure inclusive and ethical digital development.

## vi. Sources Used and Recommended Readings

- [US Signs AI Treaty](#)
- [UK's AI Safeguards Treaty](#)
- [Council of Europe's AI Framework](#)

## 5. Global Governance and Policy Frameworks

### i. Defining the Issue

As digital technologies become central to economic, political and social life, the need for international agreements and standards to regulate digital spaces has grown. However, balancing global cooperation with national sovereignty remains a key challenge. Governments, corporations and civil society must collaborate to create ethical guidelines that ensure accountability, transparency and the protection of fundamental rights.

### ii. Key Terms

- **Digital Sovereignty:** A state's authority over its digital infrastructure, data policies and online governance.
- **Cybersecurity:** Measures taken to protect digital systems, networks and data from cyber threats and attacks.
- **Data Privacy:** The right of individuals to control how their personal data is collected, stored and used.
- **AI Ethics:** Principles and guidelines ensuring fairness, accountability and transparency in artificial intelligence systems.
- **Misinformation/Disinformation:** The spread of false or misleading information, often used to manipulate public opinion.

### iii. Stances of Important Parties Involved

- **United Nations:** Advocates for international cooperation in digital governance through initiatives like the Global Digital Compact.
- **European Union:** Enforces strong privacy laws, such as the General Data Protection Regulation (GDPR) and promotes ethical AI guidelines.
- **United States:** Focuses on innovation and cybersecurity but has fragmented privacy regulations.
- **China:** Implements strict state-controlled digital governance and surveillance policies.
- **Technology Companies:** Often favour self-regulation and resist government oversight.
- **NGOs & Civil Society Organizations:** Advocate for digital rights, transparency and stronger privacy protections.

### iv. Previous Attempts to Address the Issue

- **General Data Protection Regulation (GDPR, 2018):** A landmark EU privacy law regulating personal data use.
- **Paris Call for Trust and Security in Cyberspace (2018):** An international initiative to promote cybersecurity cooperation.
- **Budapest Convention on Cybercrime (2001):** The first legally binding treaty addressing cybercrime.

- **UN Roadmap for Digital Cooperation (2020):** A UN-led initiative to foster global digital governance discussions.
- **Current Efforts:** Ongoing discussions on global AI regulations, cybersecurity agreements and digital privacy standards.

## v. Suggested Possible Solutions

- **Establishing a Universal Digital Rights Framework:** Creating a global standard for digital privacy, AI ethics and cybersecurity.
- **Strengthening Public-Private Collaboration:** Ensuring cooperation between governments, technology firms and civil society.
- **Regulating AI & Surveillance:** Implementing safeguards to prevent misuse of AI and mass surveillance technologies.
- **Holding Big Tech Accountable:** Enforcing transparency in data collection, content moderation and algorithmic decision-making.
- **Enhancing Global Cybersecurity Agreements:** Strengthening international cooperation to combat cyber threats and digital warfare.

## vi. Sources Used and Recommended Readings

- [United Nations Roadmap for Digital Cooperation](#)
- [European Union's GDPR Overview](#)
- [Paris Call for Trust and Security in Cyberspace](#)
- [Budapest Convention on Cybercrime](#)
- [Electronic Frontier Foundation: Digital Rights Advocacy](#)
- [Access Now: Policy Papers on Privacy and AI Ethics](#)

## 6. Further considerations

### i. Defining the Issue

The future of human rights in the digital age depends not only on addressing specific challenges like digital access, privacy and governance but also on recognizing the broader forces that shape the digital landscape. Education, technological innovation and global partnerships are key to ensuring that digital advancements serve humanity rather than deepen inequalities.

However, progress in these areas is complicated by:

- **Unequal access to digital education:** While technology can enhance learning, many marginalized communities lack basic infrastructure, digital literacy programs, or access to relevant educational content.
- **The double-edged nature of innovation:** While AI, blockchain and other emerging technologies have the potential to drive positive change, they also pose risks such as job displacement, bias and misuse by authoritarian regimes.
- **Challenges in global cooperation:** While partnerships between governments, private companies and civil society are essential for tackling digital inequalities, conflicting interests often prevent effective collaboration.

This topic is controversial because:

- Governments and corporations may prioritize profit and national interests over universal digital rights.
- Debates persist over whether education and innovation should be state-driven, market-led, or community-centred.
- The role of big tech monopolies in shaping education and digital governance raises concerns about undue influence over public policy.

The causes of the current problem include:

- Lack of investment in digital literacy programs, particularly in developing countries.
- A skills gap between technological advancements and the workforce's ability to adapt.
- Insufficient global regulatory frameworks to ensure fair distribution of digital resources.

### ii. Key Terms

- **Digital Literacy:** The ability to navigate, critically assess and create content using digital tools.
- **Tech for Good:** Using technology to drive social and environmental progress, such as AI for humanitarian aid.
- **Public-Private Partnerships (PPPs):** Collaborations between governments, businesses and civil society to address societal challenges.
- **Digital Capacity Building:** Strengthening communities' ability to use digital tools effectively and responsibly.

- **Ethical AI Development:** Ensuring that artificial intelligence is designed to be fair, transparent and aligned with human rights.

### iii. Stances of Important Parties Involved

- **United Nations:** Advocates for digital literacy as a human right and promotes technology as a tool for sustainable development (e.g., UNDP's digital strategy).
- **European Union:** Implements digital education initiatives (e.g., Digital Education Action Plan) and enforces strong AI and data ethics regulations.
- **United States:** Invests heavily in tech innovation but has inconsistent approaches to digital education and regulation.
- **China:** Prioritizes state-led technological development while promoting digital infrastructure projects abroad (e.g., Digital Silk Road).
- **Technology Companies:** Invest in AI research, digital learning platforms and infrastructure expansion, but also face criticism for monopolistic practices.
- **NGOs and Civil Society Groups** – Advocate for open-source technology, digital rights education and community-driven innovation.

### iv. Previous Attempts to Address the Issue

- **UNESCO's Global Education Coalition (2020):** Established to support digital learning solutions during the COVID-19 pandemic.
- **OECD Skills Strategy:** A framework to improve digital skills worldwide, particularly in underprivileged regions.
- **G20 AI Principles (2019):** Guidelines for responsible AI innovation, including ethical considerations in education.
- **The African Union's Digital Transformation Strategy (2020 - 2030):** Aims to improve digital literacy and innovation ecosystems in Africa.
- **Various Tech-Driven Initiatives:** Projects like Google's Internet Saathi (India) and Microsoft's AI for Humanitarian Action have sought to bridge digital gaps, with varying success.

### v. Suggested Possible Solutions

To ensure a fair and inclusive digital future, policy approaches must focus on education, innovation and global partnerships:

- **Enhancing Digital Education**
  - Integrate digital literacy and ethics into national curricula.
  - Expand free and open-source educational platforms to ensure access for marginalized groups.
  - Support lifelong learning programs to help workers adapt to rapid technological changes.

- **Promoting Responsible Innovation**
  - Establish global AI ethics standards to prevent bias and ensure fairness.
  - Encourage ethical funding models that prioritize social impact over profit.
  - Invest in human-centered technology that empowers communities rather than exploits them.
  
- **Strengthening Global Cooperation**
  - Foster public-private partnerships that balance innovation with public interest.
  - Expand international funding mechanisms to support tech infrastructure in developing nations.
  - Create a global digital rights framework that sets minimum protections for all users.

By aligning education, innovation and partnerships, societies can harness digital technologies for positive change while mitigating the risks of exclusion, exploitation and unethical use.

## vi. Sources Used and Recommended Readings

- [UNESCO Global Education Coalition](#)
- [OECD Digital Skills Strategy](#)
- [G20 AI Principles](#)
- [African Union Digital Transformation Strategy](#)
- [Google's Internet Saathi Initiative](#)
- [Microsoft AI for Humanitarian Action](#)