Introduction to Part III

How Should Human Rights Law Respond to the Challenges of Digital Technologies?

Tiina Pajuste

Technological development has transformed the way societies function, creating unprecedented opportunities while giving rise to complex human rights issues. Digital technologies, from artificial intelligence and algorithmic decision-making to data collection and surveillance systems, have altered systems of governance and individual autonomy. While these technologies have the potential to enhance human rights – by improving access to information, supporting equality, and fostering innovation – they also risk undermining them through privacy violations, discrimination, and erosion of accountability. As the United Nations Secretary-General has emphasised, we need to 'ensure that new technologies are anchored in the values of […] the Universal Declaration of Human Rights'.[1] Accordingly, this part of the volume examines how human rights law should adapt to the ever-evolving situation. Each chapter addresses the core question: *How should human rights law respond to the challenges of digital technologies?* By delving into specific issues such as online disinformation, privacy violations, public health surveillance, and the intersection of digitisation with foreign investment, the chapters collectively explore the tensions between innovation and human rights protection, offering insights into how legal frameworks can adapt to contemporary technological realities.

These topics reflect key challenges where digital technologies intersect with human rights. Microtargeted disinformation threatens democratic participation and free expression, requiring legal responses to preserve public trust. The case study of COVID-19 apps highlights the balance between public health and privacy, offering lessons for future crises. The rise of drones necessitates safeguards to prevent privacy violations and misuse. Finally, the interplay between foreign investment and digitisation shows how human rights can shape global economic and regulatory strategies. Together, these chapters illustrate the need for a legal framework that protects human rights while fostering responsible innovation.

[1] UN Secretary-General, 'Strategy on new technologies' (2018), www.un.org/en/newtechnologies/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 20:34:45, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.018

CHAPTER 13. THE PARADOX OF DIGITALISATION IN THE CASE OF THE COVID-19 APPS: WHAT LESSONS CAN WE LEARN FROM THIS STRANGE EXPERIENCE?

Chapter 13 examines the role of digital technologies, particularly contact-tracing apps, during the COVID-19 pandemic and draws lessons from this experience that should be taken into consideration when crisis situations occur. Paula Veiga expresses how these technologies were developed and implemented as public health tools and digs into the reasons for their widespread failure in Western countries, despite their technical feasibility. She provides insight into how digitalisation impacts public trust, governance, and human rights. Digital technologies have reshaped societal norms, created new types of data-centric goods, and introduced novel legal challenges, such as redefining rights and the role of public authorities. The chapter shows how the pandemic highlighted tensions between public health measures, privacy, and the rule of law. The exceptional circumstances required balancing individual freedoms with collective security. In relation to the core question of this part of the volume, the chapter refers to the following ways in which human rights law should adapt to address digital technologies: (a) in balancing human rights with other considerations (such as public health) during crises, the temporary measures taken need to be proportionate; (b) legal frameworks should include mechanisms to build and maintain public trust (e.g., transparency in data use, clear communication); (c) the focus should be on inclusivity, ensuring that digital technologies do not deepen existing inequalities; and (d) new human rights (e.g., the right to digital education, the right to neutrality on the internet) should be recognised and formally included in international human rights frameworks.

CHAPTER 14. AERIAL SURVEILLANCE IN THE DIGITAL AGE: DRONE-RELATED PRIVACY CONCERNS AND THE PROTECTION OF OTHER HUMAN RIGHTS

In Chapter 14, Skirgailė Žalimienė and Saulius Stonkus explore the challenges and opportunities presented by drone technology, focusing on the human rights implications of its widespread adoption. The chapter examines how drones, as platforms integrating advanced technologies (e.g., cameras, the Global Positioning System, artificial intelligence), enable extensive surveillance capabilities that pose significant risks to privacy and other human rights. It also addresses the regulatory landscape, particularly within the European Union (EU), and notes how current regulations often lag behind technological advancements, with unclear or inadequate provisions for drone registration, data minimisation, and cybersecurity. The chapter offers recommendations for striking a balance between enabling innovation and safeguarding fundamental rights. In response to this part's core question – *How should human rights law respond to the challenges of digital technologies?* – the

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 20:34:45, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.018

chapter notes the following: (a) human rights law should anticipate technological developments and establish forward-looking regulatory frameworks; (b) legal frameworks should require the integration of privacy-enhancing measures (e.g., automatic anonymisation) within technologies; (c) the principle of proportionality should be used as a guiding method, when the need arises to balance different human rights; and (d) a co-ordinated global approach is critical for ensuring consistency in legal standards.

CHAPTER 15. ONLINE DISINFORMATION, MICROTARGETING, AND FREEDOM OF EXPRESSION: MOVING BEYOND HUMAN RIGHTS LAW?

Chapter 15 studies the rise of microtargeted online disinformation (MOD) and its implications for human rights, democracy, and regulatory frameworks. Birgit Schippers looks at how microtargeting – a practice that uses data analytics to deliver tailored messages to specific audiences – amplifies the spread of disinformation, distorts public discourse, and impacts democratic processes. The chapter highlights the challenges posed by MOD to freedom of expression and privacy while evaluating the adequacy of current legal frameworks, particularly within the EU. It demonstrates how human rights law, particularly Article 10 of the European Convention on Human Rights, limits state interference with speech, making it difficult to regulate disinformation. Schippers answers this part's core question by suggesting that (a) human rights law alone may not sufficiently address MOD (and other human rights issues in the digital environment), so complementary approaches (e.g., media literacy initiatives) are needed; (b) regulatory measures must balance the need to counter disinformation with protecting free speech to avoid disproportionate restrictions; and (c) international cooperation is necessary to address cross-border human rights challenges such as disinformation, harmonise regulatory standards, and counteract the influence of global tech platforms.

CHAPTER 16. DIGITAL BOOM: CURRENT ISSUES FROM INTERNATIONAL INVESTMENT TO HUMAN RIGHTS

Chapter 16 explores the relationship between international investments, digital technologies, and human rights. Cristina Elena Popa Tache, Cătălin-Silviu Săraru, and Sergio de Souza Salles demonstrate how digitalisation has transformed international investment practices and created new legal challenges, particularly regarding data protection, privacy, and equitable access to technology. The authors propose a human rights-centred approach to regulating digital investments, focusing on balancing innovation, investment protection, and fundamental rights.

In relation to the core question of this part of the volume, they note the following: (a) digitalisation amplifies the need for legal frameworks that protect human rights

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 20:34:45, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.018

while fostering technological innovation and international investment; (b) legal systems should anticipate technological advancements by adopting forward-looking frameworks that address potential human rights implications before they arise; (c) effective governance should reconcile state sovereignty, international investment interests, and the protection of human rights, ensuring legal systems can respond to evolving digital challenges; and (d) a multi-stakeholder approach should be adopted (involving states, businesses, and international organisations) to harmonise global standards.

SHARED THEMES AND INTERCONNECTIONS

The four chapters illustrate some of the ways in which human rights law can respond to the challenges posed by digital technologies, offering insights into areas ranging from health and surveillance to microtargeting and international investment. In the following, their common themes and approaches are summarised to highlight how they converge in addressing the question of this part: *How should human rights law respond to the challenges of digital technologies?*

A. BALANCING HUMAN RIGHTS WITH TECHNOLOGICAL INNOVATION

Each chapter emphasises the need to strike a balance between safeguarding human rights and enabling technological development. The authors share the view that human rights law must evolve to navigate the tension between regulating technology to prevent harm and fostering innovation that supports societal progress:

- Chapter 13 on COVID-19 apps explores how public health technologies must balance privacy with the right to health, highlighting the need for proportionality in emergencies.
- Chapter 14 on drone surveillance argues that regulations must balance privacy with public safety and innovation in drone use.
- Chapter 15 on microtargeted online disinformation emphasises that countering disinformation requires balancing freedom of expression with protections for privacy and democracy.
- Chapter 16 on digital investments emphasises the necessity to reconcile the drive for international digital investments with the need to protect rights such as equitable access and privacy

B. PROPORTIONALITY AS A GUIDING PRINCIPLE

All chapters recognise the importance of proportionality as a key legal principle and tool to be utilised in applying human rights law in the digital environment. Proportionality is seen as having the potential to ensure that regulatory responses to

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 20:34:45, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.018

digital technologies are targeted, avoiding unnecessary or overly restrictive measures that may infringe on fundamental rights:

- Chapter 13 discusses proportionality in using emergency measures to ensure they are temporary and necessary without becoming tools for long-term surveillance.
- Chapter 14 advocates for proportionality in drone regulations to prevent overreach while addressing privacy concerns.
- Chapter 15 highlights proportionality in regulating disinformation to avoid a chilling effect on free expression.
- Chapter 16 states that proportional regulations are essential for balancing investment growth and human rights.

C. TRUST, TRANSPARENCY, AND ACCOUNTABILITY

The chapters highlight trust and transparency as critical components of effective digital governance. They note that trust in digital governance can be fostered through transparency, vigorous accountability mechanisms, and public engagement.

- Chapter 13 stresses the importance of public trust in ensuring the success of health technologies, facilitated by transparency in data usage.
- Chapter 14 emphasises accountability mechanisms to prevent the misuse of surveillance technologies.
- Chapter 15 highlights the need for transparent content moderation and data usage practices to counter the effects of microtargeting.
- Chapter 16 argues for transparent and inclusive governance in digital investments to prevent exploitation and exclusion.

Like the chapters in Part II, all four chapters in this part of the volume also call for international cooperation and harmonised legal standards. The global nature of digital technologies necessitates co-ordinated international responses to protect human rights effectively while promoting innovation and economic growth.

The chapters collectively emphasise that human rights law and its implementation must evolve to address the challenges posed by digital technologies. This involves balancing regulation with innovation, expanding the scope of human rights frameworks (or their interpretation), fostering transparency and trust, and adopting a globally harmonised, multi-stakeholder approach. Together, these insights (and others contained in the chapters) outline a strategy for ensuring that human rights are protected in the face of rapid digital transformation.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 20:34:45, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.018

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 20:34:45, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.018