International IDEA

RIGHTS IN THE DIGITAL AGE

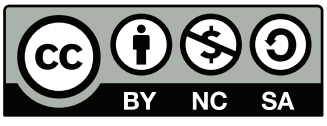
RIGHTS IN THE DIGITAL AGE

Juliane Müller

International IDEA
INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE

International IDEA
Strömsborg
SE–103 34 Stockholm
SWEDEN
+46 8 698 37 00
info@idea.int
www.idea.int

The Acknowledgement section of this report was added on 5 August 2025. The current PDF-file replaces all earlier versions.



International IDEA
Strömsborg
SE–103 34 Stockholm
SWEDEN
Tel: +46 8 698 37 00
Email: info@idea.int
Website: <https://www.idea.int>

Cover illustration: AI generated with Firefly
Design and layout: International IDEA
Copyeditor: Curtis Budden

DOI: <https://doi.org/10.31752/idea.2025.33>

ISBN: 978-91-7671-958-9 (PDF)

Abbreviations

ACHPR	African Charter on Human and Peoples' Rights
ACHR	American Convention on Human Rights
AI	Artificial intelligence
CCTV	Closed-circuit television
CJEU	Court of Justice of the European Union
DSA	Digital Services Act
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
GDC	Global Digital Compact
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and communication technology
IDS	Indigenous data sovereignty
IoT	Internet of Things
IP	Internet protocol
ISP	Internet service provider
ITU	International Telecommunication Union
LGBTQIA+	Lesbian, gay, bisexual, transgender, queer, intersex and asexual
NGO	Non-governmental organization
NHS	National Health Service (UK)
NSA	National Security Agency (USA)
Ofcom	Office of Communications (UK)
SDG	Sustainable Development Goal
UNDHR	Universal Declaration of Human Rights
UNESCO	United Nations Educational, Scientific and Cultural Organization
VLOP	Very large online platform
VLOSE	Very large online search engine

Acknowledgements

Acknowledgement is given to Sharon Pia Hickey for her internal memorandum on constitutionalized economic, social, and cultural rights, as well as emerging or fourth-generation rights, which provided valuable guidance for the framing and structure of this report.

Gratitude is also extended to International IDEA colleagues Sumit Bisarya, Sebastian Becker, and Alberto Fernández Gibaja for their insightful reviews and feedback. The external peer reviewer, Ramiro Alvarez Ugarte, warrants special recognition for his invaluable contributions to this report.

Contents

EXECUTIVE SUMMARY

This report advocates for the thorough protection of fundamental human rights in the digital age, arguing that addressing rights protection at a constitutional level offers a stronger, more enduring framework for confronting emerging digital threats than ordinary legislation alone. As digital technologies increasingly influence the exercise of civil and political rights, as well as other fundamental freedoms, robust constitutional safeguards are essential for addressing new challenges—from unwarranted surveillance and censorship to algorithmic governance and data monopolies.

Addressing rights protection at a constitutional level offers a stronger, more enduring framework for confronting emerging digital threats than ordinary legislation alone.

Enshrining digital rights in a constitution offers a uniquely durable and robust framework for safeguarding fundamental rights against novel challenges in the digital era. Because constitutional provisions are harder to amend and take precedence over ordinary laws, they help anchor protections for fundamental rights and freedoms across evolving technological contexts. By embedding digital rights in a constitution—often a nation's most symbolic articulation of shared values—countries can ensure consistent and uniform protection across various jurisdictions, especially in federal systems, while also providing stronger checks against both governmental abuses, such as unwarranted surveillance or censorship, and potential overreach by private actors, including large technology companies or data monopolies. Beyond its legal strength, constitutional recognition sets a clear standard for ethical and accountable corporate conduct and sends a powerful signal at home and internationally that digital rights are taken seriously and safeguarded at the highest legal level.

This report examines the impact of digitalization on fundamental rights and freedoms, discussing how modern digital technologies influence fundamental rights—particularly civil and political rights—

and also considers the various actors that shape these rights in the digital age, outlining ways to ensure accountability beyond traditional governance structures. It is divided into several sections that collectively provide an overview of the current landscape of digital rights issues, outlining existing constitutional protections and highlighting considerations for strengthening these protections to meet the challenges posed by the digital age.

The Introduction provides a general introduction and overview, while Chapter 1 delves into how digitalization affects core civil and political rights. This chapter includes an analysis of how freedoms such as speech, expression, association and non-discrimination are being reshaped by modern digital technologies.

Chapter 2 explores the adaptation and expansion of constitutional protections to address the novel challenges presented by digital technologies, covering a range of emerging digital rights, such as digital privacy, data protection, the right to informational self-determination, and rights related to Internet access and connectivity. The chapter also discusses rights aimed at ensuring democratic participation in the digital era and highlights the importance of new rights such as the right to digital disconnection and cybersecurity. To understand how different countries have addressed these issues in their national constitutions, the International Institute for Democracy and Electoral Assistance (International IDEA) has mapped constitutional provisions on these rights, capturing global comparative examples. Additionally, selected case law examples illustrate how courts around the world interpret constitutional rights within digital contexts, often navigating the balance between competing rights and addressing matters of public interest and security.

Chapter 3 assesses the role of new actors, particularly tech companies, and public–private partnerships in the digital domain. It discusses the horizontal application of rights as one way forward in ensuring that non-state actors that assume or are vested with quasi-state powers respect fundamental rights.

The report ends with some short conclusions in Chapter 4.

KEY RECOMMENDATIONS FOR POLICYMAKERS AND CONSTITUTION BUILDERS

- **Understand the impact of digital technologies and their effect on public life.** As digital technologies continue to evolve and become deeply integrated into every aspect of public life, it is crucial for those involved in designing and interpreting constitutions to fully comprehend their impact and to be adequately prepared to address the challenges posed by this new digital era and to provide robust protections for human rights. By thoroughly understanding these impacts, constitutional designers and interpreters can build, expand and protect constitutional legal frameworks that are adaptable to technological advancements while upholding fundamental human rights. Such a proactive approach will ensure that constitutions remain relevant and effective in the face of rapid change, while addressing these issues at the constitutional level also sends a strong message about a nation's commitment to protecting its citizens in the digital age. It provides a solid foundation for legislation and policies that promote not only technological innovation but also the ethical and equitable use of technology.

- **Adopt a human rights-based approach to digital technologies.** As digital technologies become increasingly integrated into both private and public life, the importance of a human rights-based approach, guided by international norms and national constitutional law, cannot be overstated. These technologies, ranging from artificial intelligence (AI) to cloud computing, are transforming how societies function, how governments interact with citizens, who exercises influence and holds power over people's rights and freedoms, and how individuals conduct their daily lives. While digital innovations offer significant opportunities for economic growth, social development and improved governance, they also present profound challenges to fundamental human rights, as outlined in this report.

  At the same time, it must be acknowledged that new regulatory models, such as the European Union's Digital Services Act (DSA), often adopt a risk-based approach that may not always place human rights at the centre. Instead, these frameworks rely heavily on corporate-driven risk assessments, which can inadvertently push rights considerations to the margins or transform them into balancing and proportionality analyses conducted behind closed doors. This tension remains slightly under-theorized, but it

It is crucial for those involved in designing constitutions to be adequately prepared to address the challenges posed by the new digital era and to provide robust protections for human rights.

underscores the urgent need to ensure that human rights remain integral to any policy or regulatory approach. Without explicit safeguards and monitoring mechanisms, there is a real risk that core human rights principles may be overridden by commercial or state security interests.

In the digital age, constitutions play an increasingly crucial role in safeguarding fundamental rights amid rapid technological transformations.

- **Create flexible constitutional frameworks for technological change in the digital age.** In the digital age, constitutions play an increasingly crucial role in safeguarding fundamental rights amid rapid technological transformations. As societies navigate the complexities introduced by digital advancements, the need for constitutional frameworks that are both robust and adaptable becomes paramount. Constitutions must evolve to encompass new realities, ensuring that laws keep pace with technology. This means embedding principles that anticipate future technological scenarios and creating legal standards that are clear, enforceable and universally applicable. Furthermore, these frameworks must be capable of withstanding the pressures of immediate technological threats while also being flexible enough to evolve with future technological developments. This dual capacity ensures that legal protections not only respond effectively to current challenges but are also prepared for emerging issues. Applying, adapting and reinterpreting constitutional norms to the digital context ensures that these frameworks continue to uphold and protect our fundamental rights, aligning with both present needs and future uncertainties.

- **Address the dual impact of technology.** Digital technologies enhance our freedoms, facilitating unprecedented connectivity and self-expression, while simultaneously posing significant threats to privacy and individual rights. As these technologies advance rapidly, the necessity for stringent oversight becomes ever more apparent. It is crucial to implement robust constitutional measures that safeguard civil liberties without stifling the potential benefits of digital innovation.

- **Combat rights violations and inequalities caused by digital technologies**. As digital technologies advance, there is an increasing risk that they are exacerbating existing biases, rights violations and inequalities. Numerous examples illustrate how countries and other powerful actors exploit these technologies to further their agendas and undermine fundamental rights. A particularly pressing concern is technology-facilitated harms, especially gender-based violence, which directly manifests as

online harassment, hate speech, stalking, hacking or the sharing of non-consensual imagery. These direct harms are compounded by indirect issues rooted in the design and operation of digital technologies, including algorithmic and data bias, as well as data security vulnerabilities (APC n.d.; EIGE 2020; OECD 2024; UN Women 2024). Such algorithmic and data-driven systems often perpetuate and even deepen gender bias (Smith and Rustagi 2021). To mention one example of technology impacting gender equality, a study conducted by the Berkeley Haas Center for Equity, Gender and Leadership analysed 133 AI-powered systems across various industries and found that approximately 44 per cent of them exhibited gender bias, while 25 per cent demonstrated both gender and racial bias (Smith and Rustagi 2021). Business models, algorithmic systems and data-driven processes frequently reflect and reinforce existing gender inequalities, limiting women's access to opportunities, marginalizing them further or exploiting harmful gender-based norms and stereotypes (Smith and Rustagi 2021). Additionally, unequal access to and knowledge of digital technologies prevents many from fully exercising their rights and opportunities in the digital age. Therefore, strengthening constitutional frameworks to protect individual rights from digital abuses and intensifying efforts to bridge the digital divide are crucial steps towards ensuring equitable and safe access to technology for all.

- **Adopt a balanced approach to safeguarding rights and addressing inequalities caused by digital technologies.** As digital technologies often create tensions between rights, such as the conflict between privacy and freedom of expression or between accessibility and intellectual property rights, addressing the rights violations and inequalities brought about by digital technologies requires a careful balancing of diverse rights and interests. Different constitutional cultures approach this challenge in distinct ways. For instance, some frameworks prioritize certain rights in specific contexts, such as considering freedom of expression a foundational right due to its critical role in democratic self-governance. In contrast, other systems uphold the principle of equality among rights, treating all rights as having equal standing and avoiding a hierarchy of priorities.

  Constitution builders, policymakers and stakeholders must therefore strive to achieve context-specific solutions that respect not only democratic practices and the rule of law but also the interconnected nature of rights, which often involves applying

balancing and proportionality analyses to resolve conflicts in ways that are just, equitable and reflective of local legal and cultural frameworks.

Moreover, a balanced approach also entails actively engaging marginalized and underrepresented groups, who are disproportionately affected by digital divides and rights violations in decision-making processes.

- **Adapt constitutional norms to the digital context.** Jurisprudence demonstrates that constitutional norms are increasingly being reshaped to fit the digital era. That said, substantial challenges remain when it comes to balancing evolving norms with other conflicting fundamental rights, particularly when they intersect with national security and public safety concerns. This balancing act is critical as courts work through the complexities of safeguarding rights in a time when digital technologies can both support and challenge traditional legal protections.

As tech companies increasingly assume roles traditionally held by countries, discussions around the need for the horizontal application of fundamental rights are gaining momentum.

- **Advocate for horizontal application of rights.** As tech companies increasingly assume roles traditionally held by countries, discussions around the need for the horizontal application of fundamental rights are gaining momentum. Beyond their influence over personal data and public discourse and their growing involvement in public life through public–private partnerships, private companies often control critical infrastructure, including at the network or physical level of the Internet stack. Given their significant role in managing these essential services, it is crucial that companies vested with such powers adhere to fundamental rights standards by ensuring that both their operations and their control over critical infrastructure do not undermine individual rights or democratic processes.

- **Harness digitalization to enhance democratic processes.** Digital technologies present a significant opportunity to strengthen democratic processes by enhancing accessibility, participation and inclusivity, among other things, and as these technologies continue to evolve and integrate into public life, including democratic processes, they have made it much easier for people to engage in democracy. Harnessing the power of digitalization aligns with international commitments under the Sustainable Development Goals (SDGs), particularly SDG 16, which aims to promote peaceful and inclusive societies with participatory and representative decision making at all levels, build effective and accountable

institutions, ensure public access to information and protect fundamental freedoms. By leveraging digital tools, governments can enhance transparency, improve citizen engagement and make democratic institutions more responsive.

- **Elevate the role of international organizations and actors in shaping global digital governance.** Ongoing efforts such as the Global Digital Compact provide crucial opportunities for countries and international organizations to shape international human rights law in the digital era. Involving a wide range of stakeholders—such as civil society, the private sector and academia—in global initiatives ensures that emerging global standards reflect diverse perspectives and expertise. The interplay between international law and constitutional law merits further exploration, as international commitments and frameworks can inspire national constitutions and offer guardrails for domestic regulatory efforts. By aligning constitutional protections with evolving global norms, countries can strengthen the protection of fundamental rights, reinforce accountability mechanisms and better respond to the rapid pace of technological change.

Involving a wide range of stakeholders in global initiatives ensures that emerging global standards reflect diverse perspectives and expertise.

INTRODUCTION

I.1. DEFINITION AND SCOPE

Digital technologies have become deeply integrated into our daily lives. From social media platforms and big data analytics to AI and the Internet of Things (IoT), these technologies have permeated almost every aspect of our private and public life. They not only influence personal and professional communications but also have a profound impact on many crucial sectors, such as commerce, governance, education and healthcare. Discussions around digital rights have become more prominent as incidents of data breaches, surveillance, censorship and digital exclusion highlight the vulnerabilities and challenges in protecting these rights.

The integration of digital technologies into everyday life raises critical questions about how traditional rights and freedoms are preserved and protected in the digital age, and governments, legal scholars and civil society organizations are increasingly focusing on how to adapt existing legal frameworks to ensure that constitutional rights are upheld in the face of rapid digital technological advancements.

The same rights that people have offline must also be protected online.

I.1.1. Defining digital rights

The United Nations has been at the forefront of promoting digital rights, emphasizing their importance as extensions of fundamental human rights. Grounded in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), the UN's efforts focus on ensuring that human rights are upheld in a digital environment. In 2012, 2014 and 2016, the UN Human Rights Council passed resolutions emphasizing that the same rights that people have offline must also be protected online, implying

that, rather than defining new rights for the online space, the UN advocates for the application and extension of existing human rights to the online realm (United Nations General Assembly 2016).

Following this approach, this report defines *digital rights* (or *rights in the digital era*) as those rights that are directly or indirectly affected by the growing integration of digital technologies into private and public life. In other words, digital rights are not wholly new entitlements; rather, they represent an adaptation or expansion of existing constitutional guarantees to address emerging challenges posed by modern data-driven and online realities. For instance, the right to privacy is tested by pervasive data-collection practices, while freedom of expression faces new constraints through Internet shutdowns or the moderation of social media content. These evolving dynamics also give rise to newer concepts such as the right to be forgotten, digital connectivity and cybersecurity.

By this definition, many foundational rights—such as privacy, freedom of expression or due process—already exist in constitutions worldwide. However, the digital environment demands a renewed articulation or reinterpretation of these rights to ensure that they remain effective in an age of mass data collection, algorithmic governance and platform monopolies. Consequently, constitutionalizing digital rights does not necessarily imply inventing them from scratch. Instead, it means updating, reframing or clarifying how well-established rights apply in an increasingly digital world.

The digital environment demands a renewed articulation of foundational rights to ensure that they remain effective in an age of mass data collection, algorithmic governance and platform monopolies.

I.1.2. **Global frameworks for digital rights**

There have been numerous initiatives to create guidelines and frameworks for digital rights, often in the form of Internet or digital bills of rights or charters that provide sets of norms and principles for the digital era. These initiatives can broadly be categorized into those led by non-governmental organizations (NGOs) and those spearheaded by institutional bodies.

Prominent among NGO-led efforts to establish digital rights frameworks is the Charter of Human Rights and Principles for the Internet, developed by the Internet Rights & Principles Coalition. This Charter outlines 10 fundamental Internet rights and principles, further elaborated in 21 detailed articles (Internet Rights & Principles Coalition n.d.). Similarly, the Association for Progressive Communications' Internet Rights Charter (APC 2024) categorizes 31 rights into seven distinct themes, providing a comprehensive guide for digital rights advocacy.

In terms of regional initiatives, the African Declaration on Internet Rights and Freedoms Coalition stands out as a significant example from Africa, which comprises various civil society organizations across the continent that collectively advocate for human rights standards and principles of openness in Internet policy formulation and implementation, calling for a digital rights framework tailored to the specific contexts and needs of African societies (African Declaration on Internet Rights and Freedoms Coalition 2014).

In contrast, institutional initiatives include frameworks developed by governmental or intergovernmental organizations. For example, the European Declaration on Digital Rights and Principles for the Digital Decade, adopted by the EU, sets out key principles to guide the digital transformation in Europe, emphasizing rights such as privacy, freedom of expression and access to digital services. Similarly, the Ibero-American Charter of Principles and Rights in Digital Environments (Carta Iberoamericana de Principios y Derechos en los Entornos Digitales), endorsed by the Ibero-American General Secretariat, outlines principles and rights in digital environments for the Ibero-American region (SEGIB n.d.).

Numerous similar charters exist. In a comparative analysis of Internet governance principles, the UN Educational, Scientific and Cultural Organization (UNESCO) identified over 50 specific declarations and frameworks related to the Internet (UNESCO 2015). The Berkman Klein Center for Internet & Society recognized 30 initiatives and compiled a list of 42 rights, organized into seven themes: (a) basic or fundamental rights and freedoms; (b) general limits on state power; (c) Internet governance and civic participation; (d) privacy rights and surveillance; (e) access and education; (f) openness and stability of networks; and (g) economic rights and responsibilities (Gill, Redeker and Gasser 2015).[1]

This report explores the impact of digitalization on fundamental rights in terms of the role of both state actors and non-state actors,

1 While the terms 'online' and 'digital' can be distinguished, 'digital rights' and 'Internet freedom' are often used interchangeably, typically referring to the same concepts—including the examples mentioned above.

such as tech companies and online platforms.[2] As the free exercise of fundamental rights is fundamental to democracy, this exploration delves into how digital technologies serve as both enablers and contesters of these rights. Chapter 1 of the report discusses the impact of digitalization on existing civil and political rights, including freedom of speech, freedom of association, the right to non-discrimination and the right to access government information (online). Chapter 2 then explores the adaptation and expansion of constitutional protections to meet the demands of the digital age, discussing rights such as digital privacy, data protection, and the emerging discourse around new rights such as digital disconnection and cybersecurity. Various case law has been selected to exemplify how courts around the world have interpreted and applied the constitutional law protecting these rights and freedoms. Chapter 3 assesses the roles of new actors and public–private partnerships in this context, discussing the application of constitutional fundamental rights horizontally as a way forward.

By addressing these issues, the report outlines both the opportunities and risks associated with exercising rights in the digital age, advocating for comprehensive legal protections, ideally enshrined in a nation's highest law—the constitution—and the application of law to protect fundamental rights in the digital context. Such an approach will ensure that the evolution of digital societies progresses with a firm commitment to respecting fundamental human rights and upholding democratic principles at its core.

I.2. **SETTING THE SCENE**

In the rapidly evolving digital age, rights that have been enjoyed offline are increasingly challenged in the online sphere. Digital rights encompass a broad range of human rights, including freedom of expression and assembly, the right to privacy, the right to access

In the rapidly evolving digital age, rights that have been enjoyed offline are increasingly challenged in the online sphere.

2 Online platforms—defined, for example, in article 2(i) of the EU Digital Services Act as intermediaries that host and manage user-generated content—are pivotal in the modern digital ecosystem. They serve as primary venues for public discourse, enabling individuals to express opinions, share information and engage in societal debates on a global scale. Given their role in moderating content through policies and algorithms, these platforms have a significant influence on what information is accessible to the public. This impact on the dissemination of speech makes them crucial actors in the information environment and particularly in the context of freedom of expression. Studying online platforms in detail is essential to understanding how their practices align with or challenge fundamental rights, ensuring that the digital public sphere remains open, diverse and respectful of democratic principles.

information and the right to self-determination, among others, as outlined in Chapter 1.

State censorship and Internet shutdowns severely restrict freedom of expression and the right to information.

As governments increasingly adopt digital technologies for governance, security and public administration, their actions also have profound implications for fundamental rights. The advent of state-operated digital surveillance systems, for instance, has increased concerns about privacy breaches and the potential for government overreach. Similarly, state censorship and Internet shutdowns severely restrict freedom of expression and the right to information, undermining the democratic principles they are supposed to uphold.

According to the latest 'Freedom on the Net' report by Freedom House, Internet freedom declined for the 14th consecutive year in 2024 (Funk, Vesteinsson and Baker 2024). A record number of national governments blocked websites featuring non-violent political, social or religious content. Of particular concern are network shutdowns, where authorities force Internet or social media service providers to suspend operations, often during politically sensitive times such as elections.

National security concerns frequently outweigh the rights to privacy and free expression. The World Economic Forum (Kaspersen 2015) notes the ongoing challenge of balancing security measures with the fundamental principles of democratic systems, including free speech, freedom of assembly and the right to privacy. As nations confront domestic and international threats, the tension between maintaining security and protecting individual rights becomes more pronounced.

The concentration of digital services, including public ones, in the hands of often a few major tech companies exacerbates the problem. These companies have extensive access to data flowing through the Internet, in areas such as banking, healthcare and personal communications. Furthermore, as online platforms wield significant market power, acting as gatekeepers that limit competition and make it difficult for users to switch platforms, their control over content distribution, driven by profit motives rather than a desire to disseminate information, not only reduces the diversity of information but also enables them to influence public opinion by controlling what content users see (Article 19 2021). The rise of disinformation, partly due to business models maximizing user engagement through algorithm-based content curation, complicates this issue, as the responsibility for managing misinformation remains unclear. While

these online platforms face criticism for their role in spreading false information, efforts to curb this phenomenon must be balanced against the risk of infringing on free speech.

On the positive side, certain digital processes can lower barriers to democratic participation. For instance, online voter registration and digital platforms providing information about candidates and issues can simplify processes that might otherwise be time-intensive or geographically restrictive. In some cases, remote voting technologies extend electoral participation to individuals living abroad or in remote areas or to those with disabilities (see Heinmaa and Kalandadze 2020; Pratama and Salabi 2020; International IDEA 2024a; Juneja 2024). Moreover, the Internet has expanded the possibilities for political debate—at least in principle—by enabling diverse groups of people to engage in discussions about policy and governance.

On the positive side, certain digital processes can lower barriers to democratic participation.

However, the broader democratic impact of digitalization is far from settled. While the number of participants in public discourse may have grown, the quality and nature of that discourse often suffers. Social media platforms, for example, can amplify hate speech, misinformation and polarizing content, eroding the potential benefits of heightened participation. In other words, while specific digital tools can indeed facilitate voter engagement and public debate, worrisome social dynamics—such as echo chambers and extreme partisanship—can undermine the overall goal of constructive democratic dialogue. As a result, any consideration of digital rights must also address the impact that these new communication spaces have on the substance of public discourse, not just the number of people involved.

To fully realize any of these benefits, it is crucial to guarantee unhindered Internet access, strong digital infrastructure and widespread digital literacy. Ensuring that digital technologies are inclusively designed, developed and applied helps prevent the exacerbation of existing inequalities, particularly for marginalized groups and women. Special attention must address gender-specific harms, such as targeted online harassment, surveillance and data misuse, which disproportionately impact women and gender minorities. Additionally, strong cybersecurity measures are crucial for protecting data integrity and upholding democratic processes.

This report, therefore, seeks to map out how digital rights—as rights in the digital era—are essential for maintaining the freedoms underpinning democratic societies and why this issue should also be discussed on a constitutional level. Digital rights ensure that

individuals can freely express their opinions, access information, and maintain privacy and autonomy in their digital interactions. It is also important to note that the digital revolution has not reached everyone equally. While some areas of the world enjoy constant connectivity and the latest technological advancements, many regions remain significantly underserved, with limited or no access to the Internet and modern digital technologies. Furthermore, another significant barrier for many people is their inability to use digital technologies or access the opportunities digital technologies can provide because they lack digital literacy.

The gaps suggest the need to expand existing rights—or even create entirely new ones, such as a right to digital participation and education, a right to remain offline or a right to cybersecurity.

These gaps suggest the need to expand existing rights—or even create entirely new ones, such as a right to digital participation and education, a right to remain offline or a right to cybersecurity. This report does not offer a single definitive solution. Instead, it explores three key questions: Are current rights and constitutional principles flexible enough to address today's digital challenges? Do we need to introduce new, technology-specific rights? Or should we rethink how existing rights—and the legal categories they occupy—apply in the digital era? For example, freedom of expression has traditionally been justified by the idea that a so-called free marketplace of ideas allows the best ideas to win out. On the Internet, however, the sheer volume of new information produced every day makes it impossible for individuals to sift through everything on their own. Instead, we rely on intermediaries like social media platforms and search engines to filter and organize information.

Because these intermediaries have immense control over what information we see, relying solely on constitutional protections for freedom of expression may no longer be enough to safeguard diverse perspectives. Generally, digital technologies impact democracies and constitutional regimes in new ways, often through the unchecked influence of tech power and the absence of applicable constitutional legal measures to address these issues. As the scholar Giovanni De Gregorio (2022a: 29–30) aptly noted, 'the protection of rights and freedoms in the algorithmic society cannot just be based on the expansionistic rhetoric of constitutional safeguards … Traditional bills of rights limit public powers and do not provide instruments to remedy the transparency and accountability gap among private actors.' This is where other legal tools—such as antitrust laws—may also come into play. By preventing any single platform from dominating the flow of online content, antitrust measures may help maintain competition and ensure that multiple platforms and services can emerge, giving users more choice and preserving a truly open exchange of ideas.

This report aims to clarify this problem and also explores the application of constitutional rights horizontally, including how certain notions of constitutional law could inspire and guide future regulatory efforts as a potential way forward.

I.3. **FREQUENTLY ASKED QUESTIONS**

Why does the report address digital rights at a constitutional level when protecting civil rights and liberties amid technological advancements is mainly safeguarded through ordinary legislation?

The report addresses digital rights at a constitutional level because it advocates for the constitutionalization of these rights. While ordinary legislation is crucial for protecting civil rights and liberties amid technological advancements, there are several reasons for embedding digital rights within constitutions.

Firstly, constitutionalizing digital rights provides stronger legal protection. Constitutional provisions hold the highest legal authority and are more resistant to change than ordinary laws, ensuring that fundamental digital freedoms are preserved against shifting political landscapes.

Constitutionalizing digital rights provides stronger legal protection.

Secondly, constitutionalization establishes long-term principles that guide legislation and policy. Constitutions serve as enduring legal frameworks that outlast transient technologies and trends. By incorporating digital rights at this level, we ensure that future laws remain aligned with fundamental rights despite rapid technological advancements, providing a stable foundation for adapting to new digital challenges.

Thirdly, constitutional recognition of digital rights offers safeguards against government actions and overreach, including those by non-state actors when applying constitutional rights horizontally (see Chapter 3). By clearly defining these rights at the highest legal level, constitutions limit potential infringements such as unwarranted surveillance, censorship or other abuses of power in the digital realm, creating a robust check on governmental authority and protecting individual freedoms.

Moreover, embedding digital rights in a country's constitution provides a basis for judicial review and constitutional claims as a firm

legal ground for challenging violations of these rights in court. The judiciary can interpret and enforce these rights, ensuring that they are upheld and offering a mechanism for citizens to seek redress.

Addressing digital rights constitutionally also helps reduce rights fragmentation, as promoting uniform protection of digital rights across all jurisdictions within a country prevents inconsistencies that might arise from varying ordinary laws. This uniformity is essential particularly for federal countries, to ensure consistent application and enforcement nationwide.

Constitutional provisions can encourage responsibility among technology companies.

Additionally, constitutional provisions can encourage responsibility among technology companies. Establishing clear expectations and standards for respecting user rights holds tech companies accountable for handling personal data and online interactions, which may promote greater corporate responsibility and ethical practices in the digital landscape.

Lastly, the symbolic value of constitutionalizing digital rights is significant. It demonstrates a nation's commitment to protecting its citizens in the digital age, sending a strong message both domestically and internationally. Such a commitment reinforces the importance placed on human rights within the context of technological progress and underlines a proactive approach to emerging challenges.

Some readers may find the notion of constitutionalizing digital rights contradictory, arguing that, based on the definition of digital rights as those directly or indirectly impacted by digital technologies, most of these protections already appear in constitutions worldwide. Are we not already there in most cases? Indeed, rights such as privacy, freedom of expression and due process are frequently codified in existing constitutional frameworks. This report contends, however, that constitutionalizing digital rights does not necessarily imply the creation of entirely new rights. Instead, it means adapting or expanding existing constitutional rights to address novel challenges—like mass data collection, algorithmic governance and platform monopolies—that might not have been envisioned when existing constitutions were originally drafted.

In other words, while many foundational protections do cover the essentials of digital life, the unique nature, scale and speed of today's technological environment often demand clearer articulation or an updated interpretation. By enshrining these nuances in

constitutional doctrine, we ensure that, as technology continues to evolve, the fundamental rights we rely on remain robust, relevant and enforceable in the face of new forms of digital infringement.

Why does the report refer to non-legally binding charters, declarations and bills of rights?

While some of the documents this report refers to may not be legally binding, they often reflect emerging norms, principles and societal expectations regarding the protection of rights in the digital age. One key reason why there is currently no international treaty on digital rights is the lack of global consensus on how such rights should be recognized. Competing visions of what the Internet should look like among different nations make agreement on a binding framework virtually impossible. A second, more fundamental reason is the outsized role of private actors in shaping the Internet's infrastructure. As a result, international norms in this sphere have largely fallen under 'business and human rights' frameworks, which rely on voluntary, soft-law approaches rather than formal treaties.

Nevertheless, non-binding declarations can still inspire legislative changes and influence judicial interpretations, thereby shaping the broader legal and policy debates on the subject. Additionally, such documents at the national level may entail political commitments, while regional and international documents offer global perspectives from different jurisdictions, which can help inform and strengthen international and domestic legal frameworks aiming to protect rights amid technological advancements.

Non-binding declarations can still inspire legislative changes and influence judicial interpretations, thereby shaping the broader legal and policy debates on the subject.

By examining these diverse sources, the report aims to provide a comprehensive overview of the global discourse on digital rights, highlighting innovative approaches, including the different kinds of (legal) language used, and inspire thinking about how these (proposed) rights can be effectively protected and promoted.

Are these rights infringements new to the digital era? Is there anything different from similar infringements in previous times?

Although many of the examples of how digital technologies affect people's rights mentioned in the report may seem familiar and not entirely new, rights infringements in the digital era are indeed novel because they occur in unprecedented ways and at an unprecedented speed and scale. The novelty of rights infringements in the digital era is particularly evident in the pervasive and often invisible nature of

digital surveillance, data collection and information dissemination. Unlike the analogue era, where privacy breaches were more tangible and localized, digital technologies enable mass data collection, real-time surveillance and automated decision making on an unprecedented scale. These capabilities create new risks such as algorithm-amplified mis- and disinformation, as well as algorithmic biases, identity theft and unauthorized data sharing, which can significantly impact individuals' privacy, freedom of expression and equality.

Additionally, the old gatekeepers (traditional media editors and broadcasters) are largely gone, replaced by online platforms that allow unfiltered, rapidly spreading content. While this change may broaden access to the public conversation, it is not easy to square with classical free-speech theories, which assume that individuals can rationally sort out what is true or false, good or bad. In a digitally driven world, algorithmic amplification and sheer volume can overwhelm users' ability to evaluate information critically, fuelling misinformation and hate speech at speeds and scales previously unimaginable. Consequently, though digital platforms offer new opportunities for participation, they have also fundamentally changed the quality and nature of public discourse—posing significant challenges for maintaining democratic processes and preserving the original values underlying freedom of expression.

Although the core principles of rights protection remain the same, the methods and impact of infringements in the digital age are fundamentally different.

Although the core principles of rights protection remain the same, the methods and impact of infringements in the digital age are fundamentally different, which necessitates updated legal frameworks and protections to address these new realities effectively. The report highlights these novel ways in which digital technologies are impacting people's lives and rights.

How do the rights outlined in this report relate to each other and to other fundamental rights?

The rights outlined in this report often serve as foundational rights, or 'meta-rights', that support and enable the effective exercise of other rights in the digital landscape. For instance, digital literacy and inclusion are essential prerequisites for the enjoyment of many other digital rights. Without adequate digital literacy and inclusive access to digital tools, individuals may struggle to benefit from opportunities to express opinions online, join digital assemblies or participate in public political life, which increasingly takes place in digital spaces. Similarly, digital literacy and inclusion are critical for accessing rights

not covered directly in this report, such as the right to education, which now relies heavily on digital connectivity and resources.

Cybersecurity also functions as a meta-right by providing the secure infrastructure necessary to uphold and protect other rights, such as privacy, freedom of expression and access to information. A secure digital environment is crucial for fostering trust in digital systems, which, in turn, enables meaningful participation in digital democracy and access to public services. Without confidence that their data and communications are safe, individuals may hesitate to engage with digital services, undermining their ability to fully participate in public life or access critical information.

A secure digital environment is crucial for fostering trust in digital systems, which, in turn, enables meaningful participation in digital democracy and access to public services.

In other words, the right to cybersecurity helps ensure that people can exercise their digital rights safely and without fear of harm or exploitation. For example, secure access is fundamental for online education, e-government services and digital freedom of association, as these all depend on a safe digital environment. Just as a meta-right supports other rights, cybersecurity is essential for maintaining the integrity of many digital rights. If cybersecurity measures are lacking, personal data may be compromised, impacting the right to privacy and data protection. Inadequate security also risks suppressing freedom of expression, as individuals might feel unsafe sharing their views online due to concerns over potential surveillance or retaliation.

When talking about digital technologies, what types of technologies does the report refer to?

The report examines how common digital technologies have a significant impact on fundamental rights, focusing on a few key examples, including social media platforms like Facebook, Instagram and X (formerly Twitter), which use advanced algorithms and AI to curate content and influence freedom of speech, privacy and user perceptions. Furthermore, the report also considers big data analytics and targeted advertising networks that track user behaviour, affecting rights such as non-discrimination and the right to informational self-determination, and acknowledges the importance of Internet access as a tool that enables the exercise of civil and political rights online.

How was the case law selected?

The case law in the report was selected to serve as illustrative examples of how various courts around the world have addressed different legal questions related to the impact of digital technologies

on protected constitutional rights. These cases demonstrate how courts have navigated complex issues, often faced with the need to balance different constitutional rights or to weigh the public interest against individual rights. It is important to note that the courts did not side with the claimant or determine that a rights infringement had occurred in every case. It should also be noted that the selected cases are not exhaustive; there are many other insightful and relevant cases that are not included in this report, and the jurisprudence is quickly evolving.[3]

Why is something considered a data breach or privacy violation if an individual has given consent by clicking to accept the terms and conditions?

Even when individuals have consented to the collection and processing of their data, particularly online, data breaches and privacy violations can still occur due to several factors. Firstly, individuals' capacity to understand the terms and conditions is often limited. Individuals may agree to data collection without fully comprehending the extent of what they are consenting to. If the terms and conditions are complex or not clearly presented, consent may not be truly informed. When data is used beyond the purposes that individuals believe they have agreed to, this constitutes a violation of privacy.

Secondly, data may be used for purposes beyond what was accepted, even if initial consent was given. Consent does not grant organizations carte blanche to misuse or mismanage personal data. Moreover, if data is sold or shared with third parties without explicit consent, or used in a manner that harms the individual, it violates their privacy rights.

It is important to recognize that individuals are often 'forced' to consent to data collection in order to access a service.

Finally, it is also important to recognize that individuals are often 'forced' to consent to data collection in order to access a service. In an increasingly digital world, where access to online services is becoming essential, this requirement can also raise ethical questions about the validity of consent. Breaches and violations occur when there is a deviation from the agreed terms, lack of adequate protection, misuse of the data or coercion in obtaining consent, all of which can happen despite initial consent.

3 For more digital rights case law from around the world, see CYRILLA: <https://cyrilla.org>.

What is the difference between the right to Internet access and the right to digital connectivity?

The right to Internet access refers to the principle that individuals should have the ability to access the Internet without restriction or censorship by governments or other entities. Meanwhile, based on how these terms are commonly used by scholars and practitioners, the right to connectivity pertains to the technical and physical capability to connect to the Internet, encompassing infrastructure such as broadband and mobile networks, service availability and the affordability of Internet access. Therefore, connectivity can be viewed as a prerequisite for exercising the right to Internet access (United Nations Human Rights Council 2022b).

Where to find the constitutions

The constitutional texts referred to in this publication, unless otherwise stated, are drawn from the website of the Constitute Project, <https://www.constituteproject.org>.

The next two chapters examines the impact of digital technologies on fundamental rights. The first chapter explores the ways in which digitalization has reshaped core civil and political rights, highlighting both the challenges and the potential for enhancing these rights through technological advancements. The second chapter focuses on how constitutional protections are adapting to the digital age, including a discussion of emerging rights such as digital privacy and data protection. It also reviews innovative constitutional reforms from around the world, such as the right to Internet access and digital connectivity, as well as proposals for a right to digital education, a right to digital disconnection and a right to computer security or cybersecurity.

Chapter 1

NAVIGATING RIGHTS AND FREEDOMS IN THE DIGITAL ERA

The growing digitalization of society necessitates a re-examination of how civil and political rights can be protected in an era defined by rapid technological change.

1.1. ONLINE AND OFFLINE: CIVIL AND POLITICAL RIGHTS AFFECTED BY DIGITALIZATION

As outlined in the Introduction, the growing digitalization of society necessitates a re-examination of how civil and political rights can be protected in an era defined by rapid technological change. Older forms of media—such as newspapers, radio and television—relied on broad market research and slower feedback loops to engage users. Although these forms also employed strategies to capture audience attention, their capacity to respond to individual preferences was comparatively limited.

By contrast, contemporary digital platforms and algorithms—particularly those undergirding social media—operate through adaptive, interactive feedback mechanisms that respond in real time to each user. According to Shoshana Zuboff's *The Age of Surveillance Capitalism* (2019), these platforms do not merely 'show' content; rather, they employ 'instrumentarian' strategies to predict and modify user behaviour, refining the user experience to maximize engagement and advertising revenue. While both old and new media seek to capture and hold public attention, the key shift lies in the immediacy and granularity of data-driven personalization, which often proceeds without users' explicit knowledge. This dynamic transcends the traditional 'passive versus active' distinction and raises new challenges for safeguarding civil liberties.

As discussed earlier (see I.3: Frequently asked questions), digitalization spans a broad spectrum of technologies, ranging from basic Internet access to complex algorithms that rank, classify

and present content on social media. However, these algorithms commonly operate with minimal external oversight or accountability, largely because both the underlying processes and the data they generate remain inaccessible to researchers and regulatory bodies. This opacity intensifies concerns about how to protect fundamental rights in a data-driven environment, where decisions made by opaque systems can significantly impact individual freedoms.

In light of these developments, it is imperative to reconsider and adapt existing legal and regulatory frameworks to address the unique challenges posed by contemporary digital technologies. The following section delves deeper into these issues, emphasizing the urgency of safeguarding civil liberties in an age of ever-evolving digital innovation.

It is imperative to reconsider and adapt existing legal and regulatory frameworks to address the unique challenges posed by contemporary digital technologies.

1.1.1. Freedom of speech and expression

Freedom of speech and expression is fundamental to democracy. This right not only empowers individuals to engage actively in public life, allowing for the expression of a wide range of ideas and opinions, but also facilitates democratic oversight, enabling citizens to hold public officials accountable. Indeed, without the liberty to freely seek, receive and impart opinions and ideas, a society cannot be genuinely considered democratic (Pollicino and De Gregorio 2021: 7).

For this reason, freedom of speech and expression is recognized as a fundamental human right, safeguarded by various international and regional human rights instruments. Examples include article 19 of both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, article 10 of the European Convention on Human Rights (ECHR), article 9 of the African Charter on Human and Peoples' Rights (ACHPR) and article 13 of the American Convention on Human Rights (ACHR), among others.

In today's digital age, the right to freedom of speech and expression extends well beyond traditional, analogue settings into the vast realm of online platforms—now crucial spaces for communication and information exchange. At the same time, digital repression, including censorship, surveillance and the silencing of online dissent, poses serious threats to these freedoms (Chan, Yi and Kuznetsov 2024; Gohdes 2024). For women, LGBTQIA+ individuals and ethnic minorities, these challenges often intersect with existing social inequalities, amplifying barriers to expression. Studies indicate that women face disproportionate online harassment, which can force them into self-censorship or even to withdraw from digital spaces (Posetti and Shabbir 2022). This reality undercuts the freedom of

Table 1.1. **Rights in the digital era**

Online and offline: Civil and political rights

The right to freedom of speech and expression
The right to freedom of association and assembly
The right to non-discrimination
The right to a fair trial

Digitally specific

Rights	Examples
The right to digital privacy	Article 44 of the Constitution of the Dominican Republic (2015): 'All people have the right to privacy. The respect and non-interference into private and family life, the home, and private correspondence are guaranteed. … The inviolability of private correspondence, documents, or messages in physical, digital, electronic, or all other formats is recognized …'
	Article 2(6) of the Constitution of Peru (1993): 'Every person has the right: … To the assurance that information services, whether computerized or not, whether public or private, will not provide information affecting personal and family privacy.'
The right to data protection and the prohibition against unauthorized data collection	See, for example, article 9(A) of the Constitution of Greece (1975): 'All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law.'

Table 1.1. **Rights in the digital era (cont.)**

Rights	Examples
The right to informational self-determination and the right to be forgotten	See, for example, article 35(1) of the Constitution of Portugal (1976): 'Every citizen shall possess the right to access to all computerised data that concern him, to require that they be corrected and updated, and to be informed of the purpose for which they are intended, all as laid down by law. …'
	See, for example, article 21A of the Constitution of the Canton of Geneva (substate constitution): 'Everyone has the right to safeguard their digital integrity. 'Digital integrity includes, in particular, the right to be protected against misuse of data relating to his or her digital life, the right to security in the digital space, the right to an offline life and the right to be forgotten. …'
The right to Internet access and digital connectivity	See, for example, article 6(3) of the Constitution of Mexico (1917, rev. 2015): 'The State shall guarantee access to information and communication technology, access to the services of radio broadcast, telecommunications and broadband Internet. To that end, the State shall establish effective competition conditions for the provision of such services.'
The right to freedom of information and access to government information	See for example article 2(4) of the Constitution of Peru 1993: 'To freedom of information, opinion, expression, and dissemination of thought, whether oral, written, or in images, through any medium of social communication, and without previous authorization, censorship, or impediment, under penalty of law. The State promotes the use of information and communication technologies throughout the country.'

Table 1.1. **Rights in the digital era (cont.)**

Rights	Examples
Right to digital participation, inclusion and education	See, for example, article 21A(4) of the Constitution of the Canton of Geneva (substate constitution): 'The Canton promotes digital inclusion and raises awareness of digital issues.'
	See also Chile's 2022 draft constitution (rejected), article 152: 'Citizens have the right to participate in an incident or binding manner in matters of public interest. It is the duty of the State to give adequate publicity to the mechanisms of democracy, tending to favor a broad deliberation of the people, in accordance with this Constitution and the laws.' 'The public authorities shall facilitate the participation of the people in the political, economic, cultural and social life of the country. It will be the duty of each organ of the State to have the mechanisms to promote and ensure the participation and deliberation of citizens in the management of public affairs, including digital media [alt. translation: through digital means].' 'The law shall regulate the use of digital tools in the implementation of the participation mechanisms established in this Constitution and which are different from suffrage, seeking that their use promotes the highest possible participation in such processes, as well as the widest possible information, transparency, security and accessibility of the process for all persons without distinction.' Article 90: 'Everyone has the right to digital education, to the development of knowledge, thought and technological language, as well as to enjoy its benefits. The State shall ensure that everyone can exercise their rights in digital spaces by creating public policies and financing free plans and programmes for this purpose.'
The right to disconnection and to remain offline	See, for example, Chile's 2022 draft constitution (rejected), article 46(1): 'Everyone has the right to work and to free choice of employment. The state guarantees decent work and its protection. This includes the right to fair working conditions, to health and safety at work, to rest, to leisure time, to digital disconnection, to guaranteed compensation and to full respect for fundamental rights in the context of work.'
The right to cybersecurity	See, for example, Chile's 2022 draft constitution (rejected), article 88: 'Every person has the right to the protection and promotion of computer security. The State and individuals must adopt the appropriate and necessary measures to guarantee the integrity, confidentiality, availability and resilience of the information contained in the computer systems they manage, except in the cases expressly indicated by law.'

Source: Developed by the author.

these groups to engage in public discourse and advocate for their rights. Protecting freedom of expression now requires a fresh approach that reflects the rapidly evolving digital landscape and addresses these unique challenges to inclusivity.

In today's digital age, the right to freedom of speech and expression extends well beyond traditional, analogue settings into the vast realm of online platforms.

On the one hand, digital platforms allow for the rapid dissemination of information, enabling individuals to share and access content on a global scale, almost instantly, greatly enhancing people's ability to exercise their freedom of expression. On the other hand, major tech companies now hold significant control over what is published on their platforms and can enforce community standards or guidelines that may restrict speech more heavily, and often also more arbitrarily, than traditional media laws would allow. Reports indicate that Meta, for instance, has unjustifiably and systematically restricted pro-Palestinian content and reduced the visibility of or suspended pro-Palestinian accounts under the pretext of community rules or algorithmic errors (7amleh 2018; Access Now 2023a; Human Rights Watch 2021; Mac 2021; *The Washington Post* 2021). This is just one of many examples that show that, as social media networks increasingly replace traditional media in the information field, tech companies are similarly assuming roles in shaping public opinion and exerting influence over broader constitutional and democratic processes (Amelin, Channov and Milusheva 2022).

Furthermore, countries often employ informal methods to steer platform governance, pressuring corporations through the threat of regulation or enforcement if their demands are not met (Gorwa 2024). This behind-the-scenes dynamic can prompt companies—eager to avoid legal battles, reputational damage or financial penalties—to overcompensate in their content moderation decisions, restricting certain types of speech more broadly (Sombatpoonsiri and Mahapatra 2024). In effect, public officials may gain substantial influence over online discourse without adhering to the usual legal frameworks that uphold transparency, due process and free-speech protections—further complicating the governance of digital platforms.

The regulation of freedom of speech has long been a contentious arena, where the ideal of unrestricted information flow often conflicts with democratic principles such as protections against hate speech or harmful misinformation. In the digital era, information spreads not only faster and in greater volumes but also through opaque and algorithmic mechanisms that lack transparency, making it increasingly difficult to determine how information is disseminated

and amplified. At the same time, governmental efforts to regulate digital platforms risk over-censorship or the suppression of legitimate discourse.

Freedom of expression must be safeguarded against new forms of censorship and control, such as Internet shutdowns, content filtering and algorithmic distortions.

These developments magnify threats to freedom of expression that were already familiar from the analogue era and highlight the need to adapt traditional rights to the unique challenges posed by digital technologies. In particular, freedom of expression must be safeguarded against new forms of censorship and control, such as Internet shutdowns, content filtering and algorithmic distortions—whether imposed by state or non-state actors.

However, existing 20th-century theories of freedom of expression—such as US First Amendment jurisprudence—may be insufficient for questioning certain corporate content-filtering processes or addressing subtler forms of algorithmic bias. While the First Amendment is a strong tool for challenging overt government-imposed censorship (e.g. Internet shutdowns), it does not easily extend to privately developed recommendation algorithms that can filter and shape the flow of information. Nor does it offer a clear avenue for tackling algorithmic biases rooted in corporate decision making.

In the landmark case of *Reno v American Civil Liberties Union*,[4] the US Supreme Court affirmed that speech on the Internet deserves the same First Amendment protections as traditional print media (Kahn 2025). However, this ruling predates today's sophisticated, data-driven environment and thus does not fully address the complexities of modern digital platforms. Consequently, a new or expanded theory of freedom of expression—one that accounts for the power of non-state actors and the pervasiveness of algorithmic tools—may be necessary. Although it is beyond the scope of this report to articulate such a theory in full, acknowledging this gap underscores the urgency of refining existing legal frameworks to meet the rapidly evolving realities of the digital age.

Many Internet bills of rights and digital rights charters have included provisions that reinforce freedom of expression in the virtual realm, affirming the right to disseminate diverse ideas (NETmundial n.d.; La Moncloa 2021: article XIII). Brazil's Online Bill of Rights, for example, declares in article 2 that 'Internet use in Brazil is founded on the basis of respect for freedom of expression' and in article 3 affirms the

4 521 US 844 (1997).

'guarantee of freedom of speech, communication and expression of thought, in accordance to the Federal Constitution' (Edições Câmara Brasília 2016). Nigeria's proposed Digital Rights and Freedom Bill declared that the right to freedom of expression and opinion online also included 'the freedom to seek, receive and impart information and ideas, regardless of digital frontiers' (Federal Republic of Nigeria 2019: article 6[1]). The bill was passed by both houses of the National Assembly, but then-President Muhammadu Buhari declined to sign the bill into law in March 2019, arguing that it covered too many technical subjects without addressing them extensively, and that there was potential for legislative conflicts with other pending bills covering similar issues (Fowowe 2019).

Many Internet bills of rights and digital rights charters have included provisions that reinforce freedom of expression in the virtual realm, affirming the right to disseminate diverse ideas.

As in the offline realm, freedom of expression online should be safeguarded against any unlawful government restrictions, interference or censorship (Federal Republic of Nigeria 2019: article 6[1]). The African Declaration on Internet Rights and Freedoms[5] goes so far as to demand that countries protect freedom of speech by preventing 'violent attacks against anyone on their territory' to allow for the full exercise of the right to freedom of expression online. Additionally, it calls on countries to 'create a favourable environment for participation in public debate ..., enabling [individuals] to express their opinions and ideas without fear' (African Declaration on Internet Rights and Freedoms Coalition 2014).

While freedom of expression is not absolute, Internet bills of rights promote a delicate balance between allowing individuals to express themselves freely and safeguarding intellectual property, national security, public order and individual interests, such as data protection and protection from hate speech or abuse.

Global perspectives on the extent of freedom of expression in online content differ widely across value systems and legal cultures, highlighted by the stark contrasts between China and the United States. China's strict online content regime utilizes a liability framework that requires platforms to proactively monitor and remove content, while employing broad definitions of *harm* (Pillalamarri and Stanley 2021). In contrast, the USA adopts a more permissive model, grounded in the Constitution's First Amendment and specifically codified in section 230 of the Communications Decency Act of

5 The African Declaration on Internet Rights and Freedoms, officially launched in 2014, is a non-legally binding, normative framework that sets out principles and guidelines for governments, companies and civil society in Africa to follow to protect and promote Internet rights. While it does not have the force of law, it has been influential in shaping policy discussions and advocacy efforts across the continent.

Global perspectives on the extent of freedom of expression in online content differ widely across value systems and legal cultures.

1996. Section 230, often referred to as 'the twenty-six words that created the Internet' (Kosseff 2019), grants broad immunity to online platforms (then known as interactive computer services), ensuring that they will not be held liable for user-generated content. It immunizes platforms from traditional speech torts, such as defamation, and other civil claims that effectively treat a platform as the publisher of a user's speech (Keller 2018). This legal framework allows both platforms and users greater freedom in sharing content online.

Beyond these polarized approaches, numerous countries in Europe and Asia pursue regulatory models that lie somewhere between the Chinese and US approaches (Pillalamarri and Stanley 2021). The United Kingdom opts for conditional immunity for online platforms, granting them immunity from liability for user-generated content only if they meet certain statutory conditions, and the Office of Communications (Ofcom), the nation's communications regulator, has been granted authority over online speech. Ofcom's mandate allows it to regulate online platforms by setting and enforcing standards aimed at preventing the dissemination of illegal and harmful content, including the power to create and oversee codes of practice that platforms must follow to protect users from content related to terrorism, child sexual exploitation, hate speech and other unlawful activities. Ofcom can require platforms to implement effective content moderation systems, user reporting mechanisms and transparency measures regarding how they handle online harms (United Kingdom Government 2024). Similarly, India follows a conditional-immunity approach (Pillalamarri and Stanley 2021). The EU, which has previously relied on voluntary measures, recently enacted the DSA, a landmark regulation that introduces extensive enforcement mechanisms, clarifies the liability of online intermediaries and seeks to create a harmonized framework for digital services across the EU by defining clear responsibilities for online platforms to promptly remove unlawful content. Under the DSA, online intermediaries are granted conditional immunity from liability for user-generated content, provided they comply with certain obligations (articles 4–7). For instance, article 5 specifies that hosting services are exempt from liability for illegal content if they do not have actual knowledge of the illegal activity or if, upon obtaining such knowledge, they act expeditiously to remove or disable access to the content.

Importantly, the DSA establishes specific obligations for very large online platforms (VLOPs) and very large online search engines

(VLOSEs)—services that reach more than 45 million users per month within the EU (article 33)—subjecting them to stricter regulations due to their significant societal impact.

Under article 34 of the DSA, VLOPs and VLOSEs are required to conduct annual risk assessments to identify and analyse systemic risks associated with their services, such as the dissemination of illegal content, negative effects on fundamental rights and manipulation of services. They must implement appropriate risk mitigation measures, which may include adapting content moderation processes, limiting the display of certain advertisements or adjusting algorithms (article 35). Additionally, the DSA mandates that these platforms enhance transparency by providing annual reports containing clear information on content moderation policies, algorithms used for recommending content and advertising practices (article 15), including actions taken against illegal content (article 24).

Permitting broad regulatory freedoms to online platforms expands the space for free expression, reducing state interference. However, this autonomy allows platforms to impose their own regulatory standards, which might not always adhere to and arguably are not always suited to democratic principles or the rule of law. Conversely, stringent state regulation of these platforms risks government censorship of certain opinions or media—echoing historical cases where governments have controlled print media to suppress democratically legitimate speech.

The court rulings described in Boxes 1.1–1.4 not only highlight the critical importance of safeguarding fundamental rights, which in the digital age have expanded to include access to digital resources as enablers of rights and freedoms, but also emphasize that any restrictions on these rights must be grounded in laws that are clear, precise and transparent.

1.1.2. **Freedom of association and assembly**

The right to freedom of association and assembly empowers individuals to form communities with others with similar interests and to express collective interests and grievances. These rights are crucial for forming groups such as political parties and unions, which not only check government power but also help build a strong civil society that can influence public decision making.

Box 1.1. **Free speech or undermining democratic institutions?**

The central issue in the case of *Federal Supreme Court of Brazil v Elon Musk and X*[1] is whether X (formerly Twitter), a foreign company operating in Brazil, can lawfully continue its operations after failing to comply with multiple judicial orders issued by the Brazilian Federal Supreme Court. These orders required X to block user accounts disseminating unlawful content, pay fines and appoint a legal representative in Brazil (International IDEA 2024b).

Under Brazilian law, specifically the Brazilian Civil Rights Framework for the Internet (Marco civil da Internet), all Internet service providers operating in Brazil are obligated to comply with Brazilian laws and judicial decisions (articles 10 and 11). They must remove unlawful content when ordered to do so by a court, becoming civilly liable if they fail to do so within the stipulated time frame (article 19). Additionally, these providers are required to have a legal representative in Brazil to ensure accountability and adherence to national regulations (article 11, paragraph 2).

The Brazilian Civil Code (articles 997, VI; 1,016; 1,022; 1,137; and 1,138) mandates that companies, whether domestic or foreign, appoint legal representatives and administrators responsible for compliance with legal obligations and judicial decisions. Failure to comply can result in penalties, including fines and suspension of operations. Furthermore, the Brazilian Constitution emphasizes national sovereignty (article 1, I), asserting the supremacy of Brazilian law within its territory and mandating that all individuals and entities must respect judicial decisions to maintain the rule of law and democratic order.

X failed to comply with the Supreme Court's orders issued on 7 August 2024. The platform was instructed to block user profiles involved in disseminating the personal data of and threats against police officers and their families following an attempted coup on 8 January 2023. X was also ordered to cease monetization related to these profiles, provide information about the profiles sharing unlawful content and pay a daily fine of BRL 50,000 (approximately USD 10,000) for non-compliance.

Despite multiple summonses and court orders, X did not adhere to these directives. Instead, Elon Musk, CEO of X, publicly declared on 17 August 2024 the cessation of X's operations in Brazil, citing disagreements with Justice Alexandre de Moraes and expressing an intent to avoid compliance with Brazilian laws and judicial orders. The company's non-compliance was evident in its refusal to block unlawful accounts as ordered, failure to appoint a legal representative in Brazil and public statements undermining the authority of the Brazilian judiciary.

In response to these actions, the Supreme Court suspended X's operations in Brazil on 30 August 2024. The Court froze X's bank accounts and assets and extended the asset freeze to Starlink due to the fact that X had

1 Federal Supreme Court of Brazil (7 April 2024).

Box 1.1. **Free speech or undermining democratic institutions? (cont.)**

insufficient assets to cover the fines. The Court imposed cumulative fines exceeding BRL 28 million (approximately USD 5.6 million) and ordered third-party companies, including Apple, Google, VPN services and Internet service providers, to implement technological measures to prevent the use of X in Brazil.

The Court emphasized that Brazilian law applies to all companies operating within its territory regardless of their foreign status. It reiterated that freedom of expression is not absolute and does not extend to hate speech, misinformation, or actions that undermine democracy and public safety. It also highlighted that non-compliance with judicial orders poses a threat to democratic institutions and the rule of law, especially during sensitive periods such as elections.

Following the suspension and additional enforcement actions, X eventually complied with the Court's orders. The company blocked the user accounts as initially required, appointed a legal representative in Brazil and agreed to pay the imposed fines.

The right to freedom of speech and assembly is protected by several key international instruments, such as article 20 of the UDHR, article 21 of the ICCPR, article 11 of the ECHR, article 15 of the ACHR and article 11 of the ACHPR.

The advent of digital technologies has revolutionized the way individuals communicate and interact, giving rise to new virtual spheres for social interaction, such as online communities and virtual meetings. Digital platforms have enabled the organization and execution of virtual protests. For instance, movements such as #EndSARS and #MilkTeaAlliance gained international traction through social media, where people organized rallies, shared stories and called for change, all within online spaces. During the 2011 Arab Uprisings, individuals across several countries in the Arab world used the Internet and social media platforms to organize, mobilize and sustain their protest movements (United Nations Human Rights Council 2019). By using platforms such as Facebook, X (formerly Twitter) and YouTube, protestors could bypass state-controlled media to coordinate gatherings, share live updates and expose human rights abuses to a global audience in real time. Digital mobilization was not just supplementary but central to the organization of protests, providing a new venue for assembly and association that transcended physical spaces, thus demonstrating the power of digital spaces in organizing and advocating for change (Howard et al. 2011).

Box 1.2. **Liability of online platforms for hate speech**

In the case of *Delfi AS v Estonia*,[1] the European Court of Human Rights (ECtHR) dealt with the question of whether an Internet news portal is liable for offensive comments posted by its users. Delfi AS, a prominent Estonian online news outlet, found itself at the centre of a legal battle concerning the extent of liability for defamatory comments posted by its readers. The site allowed anonymous comments, which were moderated only through an automated filter for lewd language and upon reports by other readers. After publishing an article that led to offensive comments against a business's shareholder, Delfi was requested to remove the comments and pay damages for defamation. Initially, the Harju County Court found that Delfi was not liable under Estonia's Information Society Services Act. However, the decision was overturned upon appeal, and Delfi was ultimately held liable as the publisher of the comments.

The core legal question revolved around whether holding Delfi liable for defamatory comments made by users infringed on its rights to free expression under the ECHR. Specifically, the case considered whether an Internet news portal could be responsible for user-generated content without prior notice of the defamatory nature of the content, and what the boundaries should be for such liability in light of the right to freedom of expression.

Article 10 of the ECHR provides for the right to freedom of expression, which includes the freedom to hold opinions and to receive and impart information and ideas without interference by public authorities. However, this right is subject to certain conditions, restrictions or penalties as are prescribed by law and necessary in a democratic society; in the interests of national security, territorial integrity or public safety; for the prevention of disorder or crime; for the protection of health or morals; for the protection of the reputation or rights of others; for preventing the disclosure of information received in confidence; or for maintaining the authority and impartiality of the judiciary.

In this case, the ECtHR specifically assessed whether Estonia's decision to hold Delfi liable for not promptly removing hate speech and defamatory comments constituted a justified and proportionate interference with the portal's rights under article 10 of the ECHR. Delfi contended that, as an Internet platform, it should not be held accountable for the comments posted by its users, especially since it had implemented measures to remove inappropriate comments upon notification.

In evaluating whether the imposition of liability on Delfi was justified, the ECtHR considered several critical factors. Firstly, the nature of the speech involved was scrutinized; the comments were not merely offensive but constituted hate speech and incitement to violence, categories of speech that are not protected under article 10 of the ECHR. Furthermore, the Court emphasized the duties and responsibilities of Internet platforms, noting that Delfi, as a prominent

1 App no 64569/09 (ECtHR, 16 June 2015).

Box 1.2. **Liability of online platforms for hate speech (cont.)**

commercial news publisher, bore a higher duty to ensure that its platform was not used to infringe upon the rights of others. This responsibility was underscored by its commercial nature and wide reach. Regarding the measures taken by Delfi, the Court acknowledged that the platform had implemented a disclaimer and a system for users to flag offensive comments. However, these measures were deemed insufficient given the volume and severity of the comments in question. Lastly, in assessing the proportionality of the sanction—a fine—the Court deemed it modest and appropriate, considering it proportional to the necessity of upholding the dignity and rights of others and combating hate speech and defamation.

Finally, the ECtHR upheld the Estonian appeals courts' decisions, concluding that Estonia had not violated article 10. The Court ruled that holding Delfi liable for the comments was a justified and proportionate restriction on its freedom of expression and necessary in a democratic society for protecting the reputation and rights of others.

While the Internet has become integral to exercising freedom of assembly, its potential is inseparable from the need to protect privacy, ensure secure encryption and safeguard online spaces from overbroad surveillance. Preventing the creation of back doors in communication systems is crucial to maintaining a safe environment for political organizing, as any tool used to monitor hateful or violent content might also be repurposed to curb legitimate protests. Similarly, mechanisms of content moderation, although essential for managing hate speech and misinformation, can inadvertently undermine the right to assembly and protest if employed without clear legal frameworks and due process. There is thus a delicate balance between combating harmful content and preserving citizens' ability to mobilize and advocate for change online.

Various international recommendations, such as those from UNESCO (2011) and the bodies of the European Union (2023, the European Declaration on Digital Rights), affirm that the rights to freely associate, establish organizations, form trade unions and engage in peaceful assembly are equally applicable in digital spaces. UNESCO's Code of Ethics (2011), for instance, states that 'everyone should have a freedom of association on the Internet' and that 'Member States should take preventive steps against monitoring and surveillance of assembly and association in a digital environment'. Moreover, article 8 of Nigeria's draft Digital Rights and Freedom Bill explicitly ensures the right to peaceful assembly and association online, including continuous Internet access during protests (Federal Republic of Nigeria 2019).

Box 1.3. **Preventing arbitrariness and the importance of the rule of law**

In the case of Zimbabwe Lawyers for Human Rights and Media Institute of Southern Africa (MISA) v Minister of State in the President's Office Responsible for National Security and Others,[1] the key legal issue was whether the Minister of State, Owen Ncube, had the authority to issue an order under the Interception of Communications Act to shut down the Internet in Zimbabwe during the national strike in January 2019, and whether such an action was constitutional.

The Interception of Communications Act allows for the interception of communications for national security purposes. However, the Constitution of Zimbabwe guarantees the right to freedom of expression, including the freedom to seek, receive and communicate ideas without interference (section 61). The act also requires that any interception of communications be authorized through a judicial process, not merely at the discretion of a member of the executive branch.

The Zimbabwean chapter of the Media Institute of Southern Africa and Zimbabwe Lawyers for Human Rights challenged the Internet shutdown, arguing that it was not only a violation of the constitutional right to freedom of expression but was also executed without proper authority. They contended that the Minister of State overstepped his bounds by issuing an interception warrant, a power that they argued should reside solely within the judiciary to prevent abuses of power and protect privacy and freedom of expression.

The government defended the shutdown as a necessary measure for maintaining public order during a volatile protest. However, the legal focus was on the appropriateness of the Minister's authority to issue such an order under the act and the broader implications of such actions for constitutional rights. The Court found that the Minister of State did not have the legal authority to issue the shutdown order under the Interception of Communications Act, as the act was to be administered directly by the president, not delegated to a minister. The Court set aside the Minister's order and mandated that full Internet services be resumed immediately by all telecommunications providers in Zimbabwe (Columbia University Global Freedom of Expression n.d.g).

The High Court's ruling highlights the importance of following established legal protocols, even in the unfamiliar territory of new digital developments, when restricting constitutional rights. Following established legal procedures ideally serves as a safeguard against arbitrary interference with communications and the fundamental rights of individuals, ensuring that any limitations on civil liberties are justified, transparent and consistent with the rule of law.

The decision was a significant victory for digital rights in Zimbabwe, reinforcing the principle that governmental power must be exercised within the strictures of the law, especially when it involves curtailing fundamental freedoms such as the right to freedom of expression.

1 High Court of Zimbabwe Case HC 26511921 (2019).

Box 1.4. **Prohibition of Internet use for election campaigns**

The Constitutional Court of Korea addressed the crucial issue of whether, in the interests of democracy, fundamental rights such as the right to freedom of speech can be restricted to safeguard election integrity.[1] The National Election Commission claimed that article 93(1) of the Public Official Election Act, which prohibits any Internet communication about political candidates within 180 days of an election, violates the constitutional right to freedom of political expression.

While recognizing the legislature's legitimate interest in preventing corruption and ensuring fair elections, the Court noted that such interests must be balanced with the public's right to freedom of expression, including political expression. The Court's analysis focused on whether the restriction was justified by examining the legitimacy of the act's purpose, the appropriateness of the means it used to achieve its purpose, its necessity and the balance between legal interests. It then affirmed that the goal of ensuring fair election campaigns and guarding against corruption was legitimate.

Nevertheless, it criticized the absolute prohibition on Internet communications as inappropriately broad and indiscriminate and found that such a ban failed to appropriately target the act's objectives.

Furthermore, the Court determined that the complete ban was not the least restrictive means available, adding that less intrusive measures could achieve the same ends without such a profound infringement on free speech. Additionally, when balancing the interests of maintaining electoral integrity against the rights to free political expression and participation in election campaigns, the Court found the law excessively restrictive (Columbia University Global Freedom of Expression n.d.e). It concluded that the public's right to political freedom outweighed the benefits of the ban and that less restrictive measures could be adopted, leading to the declaration of article 93(1) of the act as unconstitutional (Columbia University Global Freedom of Expression n.d.e).

1 Ruling of the Constitutional Court of the Republic of Korea Hun-Ma1001 [23-2(B) KCCR 739, 2007 Hun-Ma1001, 2010Hun-Ba88, 2010Hun-Ma173 191(consolidated), 29 December 2011. See also: <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2015/03/English-Summary-of-Decision.pdf> and <https://globalfreedomofexpression.columbia.edu/cases/prohibition-of-Internet-use-for-election-campaign>, accessed 10 May 2025.

Overall, these frameworks and legislative initiatives emphasize that individuals are entitled to use Internet platforms and other information and communication technologies for organizing and participating in public debates. However, they also caution that strict regulation aimed at hate speech or disinformation might inadvertently stifle legitimate activism if not carefully calibrated. Hence, adapting constitutional norms to a digital society must include nuanced protections for assembly and association, balancing the imperative to prevent harm with the equally vital need to protect privacy, free expression and the right to organize, both offline and online (see more in Celeste 2022).

Box 1.5. **The role of the Internet as a democratization tool**

In a case before the Constitutional Court of Colombia, the Court was asked to determine whether the Colombian Government had violated the rights to freedom of expression, association and assembly by failing to provide complete and truthful information regarding Internet service interruptions and the use of signal jammers during public protests in Cali in 2021.

The applicable legal framework and principles in this ruling were grounded in both domestic and international law. Both article 20 of the Colombian Constitution and article 13 of the American Convention on Human Rights protect the right to freedom of expression, including the free dissemination and reception of information, without undue interference from the state. Additionally, Colombia's Law on Information and Communications Technology obliged the government to intervene in communications technologies to ensure the protection of user rights and the quality and efficiency of services (Columbia University Global Freedom of Expression n.d.a).

The Court found that, while there was insufficient evidence to directly attribute the Internet and signal disruptions during the protests to the government, the state failed in its duty to investigate and transparently communicate the reasons behind these interruptions. Due to the government's failure, the petitioners were unable to access information freely, which impacted their rights to freedom of expression, association and assembly. The Court highlighted the necessity for freedom of expression and net neutrality in a democratic society and emphasized the role of the Internet as a democratization tool that facilitates the communication of opinions and information (Columbia University Global Freedom of Expression n.d.a).

Eventually, the Court concluded that, by not providing timely and truthful information about the Internet service interruptions and the usage of signal jammers during the protests, the Colombian Government violated the petitioners' constitutional rights to freedom of expression, association and assembly. It ordered relevant government ministries to disclose this information publicly to uphold transparency and accountability (Columbia University Global Freedom of Expression n.d.a).

1.1.3. **The right to non-discrimination**

The right to non-discrimination is foundational to the integrity and functionality of democratic systems.

The right to non-discrimination is foundational to the integrity and functionality of democratic systems. It ensures that all individuals have equal access to political, social and economic opportunities, thereby supporting a fair and inclusive society.

The digital era presents unique challenges in safeguarding the right to non-discrimination, including but not limited to algorithmic bias, digital profiling, online harassment and unequal access to digital resources. In several documented cases, the use of AI or algorithms by both government and private entities in decision-making processes—such as hiring, social benefit allocation, fiscal operations, loan approvals and law enforcement—has reinforced and amplified biases, particularly concerning race, ethnicity and gender. Such systems, often trained on biased data sets, can introduce direct discrimination by using protected attributes like gender, race, religion or age to make decisions that result in unequal or less favourable treatment (European Union Agency for Fundamental Rights 2020: 69–74).

Importantly, the problem is not always that the data itself is inaccurate; rather, it can be objectively true information that records past discriminatory practices, policies and institutional realities. In these situations, the model works precisely as designed, yet produces discriminatory outcomes because it reflects pre-existing social biases. For instance, historical data on crime or recidivism rates may be influenced by long-standing patterns of over-policing or unequal sentencing. Although this historical data may be accurate, when it is used to train predictive models, the resulting decisions perpetuate discrimination (Fourcade and Healy 2024).

This challenge also arises in online services such as dating apps. Algorithmic ranking and matching can inadvertently encode prevailing social prejudices. In a majority-white user base, a tendency to dismiss people of colour or give them a low rating may translate into lower algorithmic scores and reinforce segregation in recommendations—even though the system is functioning correctly from a purely technical perspective. Consequently, the discrimination occurs upstream in the social reality the data reflects, making it difficult to address without revisiting how these models are developed and deployed (Fourcade and Healy 2024: 268–69).

AI systems can yield direct discrimination by explicitly utilizing protected attributes (e.g. gender, race, religion, age) in ways that

AI systems tend to function in less transparent ways, making the discrimination they perpetuate more systemic and challenging to address.

cause unequal treatment. These systems can also bring about indirect discrimination by using proxies—which appear neutral on the surface—that correlate strongly with protected characteristics. For example, selecting specific neighbourhoods for increased police surveillance might disproportionately affect minority communities (European Union Agency for Fundamental Rights 2020: 34). Unlike human decision makers, who can be more easily monitored and corrected, algorithms and AI systems, which suffer from biases, can operate on a larger scale and produce conclusions that are often nearly impossible to understand. Even in the best scenarios, these systems tend to function in less transparent ways, making the discrimination they perpetuate more systemic and challenging to address.

A notable example from 2022 highlights the potential dangers. In the Netherlands, the tax authority implemented a machine-learning algorithm to develop a risk profile aimed at detecting possible child benefit fraud. The profile disproportionately flagged low-income and ethnic minority families, resulting in the imposition of wrongful penalties by the tax authority. The impact was severe, with people wrongly accused of fraud and driven into poverty due to repayment demands. This situation had tragic outcomes, including suicides and the placement of over 1,000 children into foster care (Heikkilä 2022).

Some scholars argue that algorithms might discriminate not only by replicating existing human biases—many of which relate to protected attributes such as race or gender—but also by acting on novel combinations of behavioural and demographic traits. Such algorithm-based discrimination could create new disadvantaged groups, necessitating a broader scope of discrimination prevention. Examples of such groups might include, for example, online gamers or dog owners (Wachter, Mittelstadt and Floridi 2017; Wachter 2020; Wachter, Mittelstadt and Russell 2021: 6).

Furthermore, digital technologies enable more invasive surveillance and data collection practices. Reported instances include cases of discriminatory profiling, where certain groups are disproportionately targeted based on their ethnicity, religion or socio-economic status (Turner Lee and Chin-Rothmann 2022). Within the Black Lives Matter movement, concerns have been raised over the allegedly disproportionate use of surveillance, such as aerial surveillance, location tracking and facial recognition, which was particularly focused on communities of colour (Turner Lee and Chin-Rothmann 2022).

The problem of profiling, particularly ethnic profiling, is especially pressing in the areas of counterterrorism, law enforcement, immigration, customs and border control (European Union Agency for Fundamental Rights 2010; Turner Lee and Chin-Rothmann 2022). Through new forms of public–private partnerships, so-called smart-border technology establishes migration and asylum management systems that include electronic monitoring, satellites, drones and facial recognition. Other technologies, such as lie detectors and iris scanning, are also reportedly used in these systems. Together, these tools not only perpetuate racial biases and discrimination, but they are also disproportionately deployed against certain groups of people (Amnesty International 2024).

In the analogue era, the widespread data collection we encounter today—carried out by both state and private entities—was not as feasible. Today's rise of digital technologies amplifies extensive surveillance and the discriminatory practices that can accompany it. On top of this, systematic errors in facial recognition technology cause the technology to disproportionately affect historically marginalized communities. For instance, in December 2020 three Black men in the USA were wrongfully arrested due to errors in facial recognition matches (Hill 2021). Studies, including a 2018 analysis by researchers from the Massachusetts Institute of Technology and Microsoft, have highlighted these biases, showing higher misclassification rates for darker-skinned women compared with lighter-skinned men (Buolamwini and Gebru 2018). Further, a 2019 study by the National Institute of Standards and Technology found that US-developed facial recognition algorithms were more likely to misidentify Black, Asian and Native American individuals than white individuals (US National Institute of Standards and Technology 2019).

Today's rise of digital technologies amplifies extensive surveillance and the discriminatory practices that can accompany it.

The frequent references to protection against discrimination in various digital rights charters, such as the African Declaration on Internet Rights and Freedoms, the Italian Declaration of Internet Rights, and Nigeria's proposed Digital Rights and Freedom Bill 2019, reaffirm the importance of protecting individuals against discriminatory practices in safeguarding fundamental rights online. Moreover, the Spanish Charter of Digital Rights goes as far as to dedicate an entire paragraph to the right to equality and non-discrimination in the digital environment, highlighting the centrality of these protections in today's digital landscape (La Moncloa 2021: article VIII).

The concept of non-discrimination is further recognized in various Internet bills of rights, particularly through the principle of net neutrality. Net neutrality ensures that all Internet traffic is treated equally, without favouring certain content, services or users over others. This impartial approach is crucial for maintaining an open and fair Internet, where users can freely access information without interference from service providers (Brazil 2014; Italian Republic 2015: article 4). As illustrated in a popular Burger King ad, net neutrality can be understood as akin to a fair pricing system, where customers should not have to pay more for faster service, just as Internet users should not experience slower access based on the content they seek (Advertising TV 2018). Promoting net neutrality supports inclusion, gender equality and the protection of marginalized groups (European Union 2023: Chapter II; African Declaration on Internet Rights and Freedoms Coalition 2014: articles 9 and 13), advocates for a multilingual Internet (United Nations 2014: article 19) and emphasizes the Internet's role as a crucial tool for exercising fundamental rights (Italian Republic 2015: article 4 II; Celeste 2022: 186 ff.).

1.1.4. **Right to access government information online**

The right to information refers to the public's right to access information held by public bodies, ensuring transparency and accountability.

The right to information refers to the public's right to access information held by public bodies, ensuring transparency and accountability in the public authorities' exercise of power. This right is a crucial principle of democratic governance, as it enables citizens to participate effectively in public life, hold governments accountable and engage in informed decision making. Traditionally, the right to information focused on the public's ability to access documents and information held by the government; however, with the expansion of digital technologies, this right now encompasses access to digital data, including government databases and other information stored digitally.

Many bills of rights and declarations already recognize the need for digital public services and transparency online.

Many bills of rights and declarations already recognize the need for digital public services and transparency online (see, for example, the European Declaration on Digital Rights and Principles for the Digital Decade). With regard to freedom of information more generally, Peru passed an amendment to article 2 of its Constitution in September 2023 that strengthens citizens' right to freedom of information (ConstitutionNet 2023).

The digital transformation of access to information also creates potential tensions with other rights. For instance, the principles of the Open Government movement and frameworks like the Model

Freedom of Information Law of the Organization of American States advocate for publishing state-held data in raw and machine-readable formats (i.e. open data). While this approach increases transparency and civic engagement, it may clash with privacy protections or newer rights like the right to be forgotten. Releasing public data sets in open-data formats can inadvertently expose personally identifiable or sensitive information, creating risks for individuals—even when the initial aim is to enhance transparency. This risk is especially significant, as data that is posted online can be replicated and disseminated in ways that are difficult, if not impossible, to reverse, heightening concerns around the misuse and permanence of data. Such data might also be harnessed to train AI models (see 1.1.5: Right to a fair trial, effective remedy and equality before the law), potentially compounding existing privacy risks.

One concrete example of how open-data principles can conflict with other rights involves Indigenous data sovereignty (IDS). IDS underscores the right of Indigenous peoples to govern how data relating to their communities, lands and resources is collected, owned and applied. Although open data can foster civic innovation and public accountability, it can clash with the governance rights and cultural autonomy of Indigenous groups if information is published without their express permission. All too often, Indigenous knowledge or community data is digitized, placed into open-data repositories and subsequently reused for purposes unintended or disapproved of by those communities (Rainie et al. 2019).

From the standpoint of IDS, the right of Indigenous peoples to determine which data may be publicly released, how it can be used and whether it should be removed or withheld is not only a question of respecting cultural traditions and knowledge systems but also a matter of complying with privacy and self-determination rights that are fundamental to Indigenous communities. In this sense, the tension between open data and IDS parallels broader debates on privacy and the right to be forgotten—illustrating how data freedoms can become problematic when they extend into areas of communal identity and historical marginalization (Rainie et al. 2019).

The tension between open data and Indigenous data sovereignty parallels broader debates on privacy and the right to be forgotten.

The call for legal frameworks that enable and regulate the digital dissemination of information therefore reflects a broader recognition of the need to strike a balance between openness and privacy—ensuring that freedom of information continues to serve as a vital cornerstone of contemporary democratic governance without unduly compromising individuals' personal data or broader rights (Celeste 2022: 26).

Table 1.2. **Right to freedom of information and access to government information online**

Peru 1993	Chapter I. Fundamental Rights of the Person Article 2(4)[1]	Every person has the right: … 4. To freedom of information, opinion, expression, and dissemination of thought, whether oral, written, or in images, through any medium of social communication, and without previous authorization, censorship, or impediment, under penalty of law.

1 On 23 September 2023, Law No. 31878 was published: the Constitutional Reform Law that promotes the use of information and communication technologies (ICTs) and recognizes the right to free internet access throughout Peru. This law introduces two amendments to the Political Constitution of Peru: Article 2, paragraph 4 (freedom of information) now adds that the State shall promote the use of information and communication technologies nationwide. Article 14-A is created, establishing that the State shall guarantee, through public or private investment, free internet access across the entire national territory, with special emphasis on rural areas and peasant and Indigenous communities. *Source*: Rodrigo, Elias & Medrano Abogados, 'Ley de reforma constitucional que promueve el uso de las tecnologías de la información y reconoce el derecho de acceso a internet libre en todo el país' [Constitutional reform law that promotes the use of information technologies and recognizes the right of access to free Internet throughout the country], [n.d.], <https://perma.cc/YSD4-FY8M>, accessed 24 March 2025

1.1.5. **Right to fair trial, effective remedy and equality before the law**

The right to a fair trial, effective remedy and equality before the law is crucial in a democracy, as it upholds the rule of law and ensures that individuals can rely on a consistent and transparent legal system to protect their rights and resolve disputes fairly. Article 8 of the UDHR states that everyone has the right to an effective remedy by competent national tribunals for acts violating the fundamental rights granted by the relevant constitution or by law (United Nations 1948). Article 14 of the ICCPR ensures that everyone is equal before the courts and tribunals and is entitled, without any discrimination, to a fair and public hearing by a competent, independent and impartial tribunal established by law (United Nations 1966).

While the integration of digital tools into judicial and administrative processes is intended to enhance efficiency, it often introduces complexities that can obstruct traditional avenues for legal recourse. For instance, the use of automated decision-making systems in determining eligibility for social benefits, loan approvals, or even law enforcement and predictive policing can result in decisions that adversely affect individuals without clear or accessible explanations. Appealing decisions made by digital systems is often more

difficult than addressing mistakes made by humans, as reliance on algorithms and big data can obscure the reasoning behind decisions due to their complexity and the vast amounts of data they process. Such black box technology disables transparency and makes it impossible for affected individuals to discern why a particular decision was made, hindering their ability to prove discrimination or error. This lack of transparency extends to data collection methods, training procedures for algorithms, the data utilized in model creation and the specifics of individual consent (Burrell 2016). Moreover, the global nature of technology platforms means that data handling and processing often cross international borders, further complicating jurisdictional claims and the enforcement of legal rights.

In this regard, the use of algorithms in judicial or quasi-judicial settings is also particularly challenging for the right to a fair trial. This issue has been highlighted in various real-life cases, particularly involving recidivism prediction systems such as COMPAS, which is used in several states across the USA to assess the likelihood that a person will reoffend. An investigation revealed that COMPAS displayed racial biases, as it incorrectly predicted that Black individuals were more likely to reoffend than white individuals. This type of biased prediction can influence judicial decisions, potentially leading to harsher sentencing for minorities based on flawed risk assessments, thereby undermining legal predictability and the fairness of sentencing (Larson et al. 2016).

The use of algorithms in judicial or quasi-judicial settings is particularly challenging for the right to a fair trial.

Particularly concerning in this regard is UNESCO's finding that only 9 per cent of surveyed judicial operators reported that their organization had issued internal guidelines or regulations for using AI chatbots. An equally small percentage indicated that their organization had provided any AI-related training or information (Gutiérrez 2024).

Legal frameworks have also not kept pace with technological developments, making it unclear how laws apply to decisions made by algorithms. This lack of clarity can complicate efforts to challenge these decisions because it may not be clear who is responsible or how to legally attribute liability for errors (Pagallo 2013). Furthermore, algorithms and humans process information based on a fundamentally different logic. Machine-learning algorithms use complex mathematical models to detect patterns and make decisions through statistical analysis. In contrast, human decision making, particularly in legal contexts, relies more on intuition and experience, methods that lawyers are familiar with when litigating

rights violations (Burrell 2016). Moreover, while legal professionals are accustomed to this intuitive human process, understanding and contesting decisions made by digital systems often requires substantial technical expertise. This level of technical knowledge is beyond what most legal professionals possess (Crawford and Calo 2016) or might implicate intellectual property issues, deterring private entities from revealing the logic and processes of their technologies (Burrell 2016).

The Spanish Digital Rights Charter has picked up on these challenges and declared that 'transparency, auditability, explainability and traceability shall be ensured' in the use and application of AI technologies (La Moncloa 2021: XXV 2).

As countries increasingly rely on digital tools to administer public and judicial processes, it is crucial to safeguard the right to a fair trial, effective remedy and equality before the law and to ensure predictability and certainty.

As countries increasingly rely on digital tools to administer public and judicial processes, it is crucial to safeguard the right to a fair trial, effective remedy and equality before the law and to ensure predictability and certainty. The EU Artificial Intelligence Act, for example, addresses these concerns by imposing stringent requirements on high-risk AI systems, including those used in judicial and administrative processes (EU Artificial Intelligence Act: Annex III, section 8, article 6). It is imperative that legal frameworks be bolstered so that the use of such technologies will enhance rather than compromise the equitable administration of justice—a cornerstone of democratic society. People subjected to the coercive power of the state must not be subjected to automated decision-making processes whose rationale cannot be fully explained, whose transparency is lacking or whose outcomes cannot be objectively justified. The right to be treated fairly by the state is a fundamental right, and no efficiency interest on the part of the state can justify weakening or infringing upon it.

Chapter 2

ADVANCING DIGITAL HUMAN RIGHTS: ADAPTING AND EXPANDING CONSTITUTIONAL PROTECTIONS

While certain rights—such as those mentioned previously—need only reaffirmation or an expanded scope for the digital age, others, particularly traditional civil and political rights such as privacy, require translation or adaptation to the digital era. These adaptations, or even expansions, are necessary to adequately protect individuals from challenges unique to the digital context.

Traditional civil and political rights, such as privacy, require translation or adaptation to the digital era.

2.1. DIGITAL PRIVACY

The right to privacy—traditionally understood as encompassing the privacy of communications and the home—is a foundational aspect of personal freedom and security. Historically, this right has shielded individuals from unwarranted intrusions into their personal life and communications—for example, letters and phone calls. The right to privacy is a fundamental human right recognized in numerous international legal instruments, such as article 12 of the UDHR, article 17 of the ICCPR and article 8 of the ECHR. These instruments protect the right to respect for one's private and family life, home and correspondence, as well as the freedom from arbitrary interference and from attacks upon one's honour and reputation. The right to privacy, a crucial safeguard for other fundamental rights—especially freedom of expression and association (United Nations Human Rights Council 2022c; Lanza 2017)—plays a pivotal role in the power dynamic between the state and the individual; it stands as a cornerstone of a democratic society (United Nations Human Rights Council 2021b: para. 6).

The digital age has transformed communication, shifting people from handwritten letters to emails and from traditional phone calls to instant messaging services like WhatsApp. While these tools offer unprecedented convenience and connectivity, they also open new channels for surveillance and data harvesting. For example, Edward Snowden's 2013 revelations exposed the vast reach of global surveillance programmes, which intercepted millions of video chats, instant messages, Internet logs, emails and even photos shared on file-sharing platforms (Amnesty International 2015).

These revelations also illustrate how the collection of data extends far beyond traditional communications. Everyday interactions with digital devices and services—from using smartphones and wearable technology to browsing the Internet and engaging with social media—generate a continuous stream of personal data. This data is often collected, analysed and stored by companies and governments, sometimes without clear or explicit consent from individuals. Furthermore, newer types of personal data, such as genetic (e.g. DNA) and biometric data (e.g. fingerprints, iris scans), serve as unique personal identifiers. These identifiers not only raise privacy concerns for the individual but also have implications for their extended family, potentially spanning generations.

The rise of big data analytics and particularly AI has enabled the analysis of vast amounts of personal information at an unprecedented scale.

The rise of big data analytics and particularly AI has enabled the analysis of vast amounts of personal information at an unprecedented scale. These technologies can identify patterns and make inferences about personal behaviour, preferences and even future actions, which can be used for purposes ranging from targeted advertising to predictive policing. On top of that, the use of digital devices in homes, cities and workplaces (such as smart speakers and meters, connected appliances, integrated surveillance cameras) has further blurred the boundaries of privacy, making it hard to fully escape the digital space.

Smartphones have essentially become location-tracking devices, mapping users' every move. While apps like Facebook, Google and X (formerly Twitter) are widely recognized for collecting location data, the true extent of tracking goes far beyond these platforms. Mobile networks and Internet service providers (ISPs) continuously gather metadata, including location data, every time devices connect to the Internet or make a call. Apps often subtly push users into granting permissions for location tracking or quietly extract data directly from devices (Boshell 2019). However, the stakes rise further when governments are involved. In 2013, US National Security Agency

(NSA) surveillance programmes were revealed, showing how metadata was used to track individuals' physical locations through mobile networks—transforming routine phone use into a powerful tool for global monitoring (Gellman, Soltani and Peterson 2013). This tracking, by both private corporations and state actors, uncovers not just where individuals are but also intimate details about their routines, associations and movements. Additionally, state-sponsored hacking has become alarmingly common, with much of it targeting citizen databases—further complicating the ongoing battle for data privacy (CSIS n.d.). Such practices do not stop at the borders of established democracies. In the case of Catalonia, for example, more than 60 phones belonging to pro-independence politicians, lawyers and activists were targeted, likely by Spanish Government authorities (Farrow 2022).

Amnesty International and other organizations have reported that authorities in many regions of the world have used surveillance technologies to suppress dissent and monitor individuals under the guise of security (Access Now 2023b; Amnesty International 2023). For example, there has been extensive reporting on the use of Pegasus spyware, developed by the Israeli cyber-arms company NSO Group, to spy on journalists, activists and political leaders worldwide. Notable investigations, including the Pegasus Project in 2021, revealed that the spyware was used in countries such as India, Mexico and Saudi Arabia to infiltrate the devices of hundreds of individuals, including human rights activists, journalists and other political figures (Amnesty International 2021).

There has been extensive reporting on the use of Pegasus spyware to spy on journalists, activists and political leaders worldwide.

The Indian Government's use of Aadhaar, a biometric database, links biometric data with personal information. While Aadhaar has facilitated bureaucratic processes, it has also been criticized because of privacy concerns, particularly regarding the extensive collection of biometric data and personal information, as well as issues relating to how data is stored and accessed. Instances where personal information was leaked from the database have raised concerns about the potential for surveillance and the misuse of private data (Jain 2019).

Moreover, what many experts call 'surveillance and data capitalism' is further amplified by the global nature of the Internet. The fact that personal data can easily be transferred across national borders, often to countries with lower privacy standards or inadequate protection mechanisms, poses grave challenges to the right to privacy.

In this digital world, personal information is more vulnerable than ever, and privacy is often the first casualty.

While traditional privacy rights focus on non-interference in one's private life and the secrecy of communications, the illustrative cases above show that the digital age tests the limits of existing legal frameworks and demands an expanded definition that includes data and metadata privacy. The UN High Commissioner for Human Rights and the Inter-American Commission on Human Rights have also noted the importance of the right to privacy for the enjoyment and exercise of other human rights, both offline and online, in our increasingly data-centric world (United Nations Human Rights Council 2021b: para. 6). Protecting this right involves addressing issues related to surveillance and data collection, data security and international data flows, as well as digital tracking and profiling (Zubenko 2023).

A crucial tool in protecting privacy in the digital era is end-to-end encryption, which ensures that only the sender and recipient can access the contents of a message.

A crucial tool in protecting privacy in the digital era is end-to-end encryption, which ensures that only the sender and recipient can access the contents of a message. Encryption plays a vital role in safeguarding personal information against both unauthorized access by private actors and state surveillance. However, the deployment of encryption varies across digital platforms. While services like Signal and WhatsApp offer encryption by default, others, like Facebook Messenger and certain email services, may provide only partial encryption or none at all, leaving communications exposed to interception.

The use of encryption poses a key challenge for law enforcement, which often seeks access to encrypted data for legitimate purposes, such as preventing terrorism or addressing child sexual abuse material. Governments frequently push for back doors in encryption, arguing that such access is necessary for national security. Critics argue, however, that such back doors inherently weaken encryption systems, making them more vulnerable to misuse and hacking by malicious actors (Friedersdorf 2015; EFSAS 2021).

This tension mirrors broader debates over privacy and security, as illustrated in a case before the Indian Supreme Court, where petitioners challenged the constitutional validity of a governmental order based on the Information Technology Act, which allows intelligence services to intercept, monitor and decrypt digital communications and data generated, stored, shared or transmitted through digital platforms in the country. They argued that the order

lacked necessary safeguards and disproportionately affected the rights to freedom of expression and privacy guaranteed in the Indian Constitution (the latter interpreted through the right to life and liberty).[6]

In another case[7] brought before the European Court of Human Rights (ECtHR), the petitioner claimed that his Romanian employer unlawfully monitored his private messages on his work computer. He argued that his emails were protected under article 8 of the ECHR, which pertains to privacy and correspondence. The Court upheld the employer's right to monitor staff communications but emphasized the importance of respecting employees' privacy and correspondence rights. It stated that such monitoring is permissible only if it is transparent, proportionate and conducted for legitimate purposes.

The increased integration of AI systems into various sectors also deserves attention in discussions surrounding the right to privacy. AI has had a significant impact on the right to privacy, often intensifying and expanding potential intrusions. Aspects of privacy that are of particular importance in the context of the use of AI include informational privacy, covering information that exists or can be derived about a person and their life and decisions based on that information, and the freedom to make decisions about one's identity (United Nations Human Rights Council 2021b: paras 12–15).[8]

AI has had a significant impact on the right to privacy, often intensifying and expanding potential intrusions.

AI systems rely heavily on large data sets, many of which contain personal data. This reliance incentivizes extensive data collection, storage and processing, often beyond what is necessary. Companies, particularly those operating online, such as social media platforms, collect vast amounts of data from users, which is then monetized. The IoT has also contributed to the proliferation of data collection, extending it into private and public spaces alike. The aggregation of this data by political consulting and data analytics firms, which merge, analyse and distribute it, typically occurs with minimal transparency and under weak legal frameworks. The sheer scale of these data sets, coupled with the often opaque nature of data transactions, leads to significant privacy risks, exposing individuals to potential breaches and misuse of their sensitive information (United Nations Human Rights Council 2021b: paras 12–20).

6 *Internet Freedom Foundation and Another v Union of India and Others* SCI (2019).
7 *Bărbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017).
8 Also see *Goodwin v United Kingdom* App no 28957/95 (ECtHR, 11 July 2002), para. 90.

Moreover, the use of AI systems introduces complex challenges related to the right to privacy that go beyond mere data collection. AI's ability to make inferences and predictions based on large data sets allows for the detailed profiling of individuals, potentially exposing private aspects of their lives to both corporations and governments. These systems can deduce sensitive information, such as health conditions or political affiliations, and make probabilistic predictions about future behaviours. Such inference can have profound implications, influencing decisions that affect individuals' rights, including autonomy over one's identity. AI systems are prone to errors, and their outputs can be affected by biased or inaccurate data, leading to decisions that may unfairly discriminate against certain individuals or groups. The opacity of AI decision-making processes, often referred to as the 'black box problem', exacerbates these issues by making it difficult to scrutinize and hold accountable the systems that infringe upon privacy rights (United Nations Human Rights Council 2021b: paras 2–20).

In practice, the use of AI systems has great implications for a wide range of sectors, such as law enforcement, national security, border management, public services, employment and managing information online, as thoroughly outlined in the 2021 annual report of the UN Office of the High Commissioner and the UN Secretary-General on the right to privacy in the digital age (United Nations Human Rights Council 2021a).

Several charters of Internet rights articulate and safeguard the digital right to privacy.

Several charters of Internet rights articulate and safeguard the digital right to privacy. For example, the Italian Internet Bill of Rights and Brazil's Civil Rights Framework for the Internet advocate for consent and principles of data minimization that limit surveillance to targeted interventions and recognize the rights to anonymity and encryption online (also see Federal Republic of Nigeria 2019: article 4; La Moncloa 2021: articles IV and V). Also, the Human Rights Committee, which monitors the implementation of the ICCPR, has discussed interpreting the international human right to privacy in the context of modern challenges, including state surveillance and data protection (Office of the United Nations High Commissioner for Human Rights 1988, 2022a, 2022b, 2022c).

Furthermore, countries such as the Dominican Republic and Peru have specifically recognized the right to digital privacy in their constitutions. These principles aim to protect individuals from indiscriminate monitoring and ensure the integrity of digital

communications, emphasizing the necessity of these rights in preserving the essence of privacy in the digital era.

In light of these extensive transformations—often referred to as the datafication of society—the impact on the right to privacy stems not just from surveillance and data capitalism or state monitoring but from a broader social and technological push to gather and analyse data in the name of efficiency, innovation or self-improvement. As elaborated in the next section of this chapter, on data protection, the sheer availability of data—and the incentives driving its collection by countries, corporations and even individuals themselves—demands new legal and conceptual frameworks that go beyond traditional notions of privacy.

These frameworks may need to strengthen the right to privacy vis-à-vis both public and private actors. They may also require expanding or supplementing privacy protections to guard those who wish to opt out of data-intensive systems, preventing scenarios in which they must surrender personal information or subject themselves to constant monitoring in exchange for social or economic benefits (e.g. lower insurance premiums contingent upon real-time driving data). Such developments might align with an expanded right to informational self-determination (discussed in detail in 2.4: Right to informational self-determination and the right to be forgotten), reinforcing each individual's autonomy over how their data is collected, shared or utilized. Taken together, these measures reflect the urgent need to adapt existing legal protections to a world where data-driven governance and personal-data economies blur traditional boundaries of privacy, potentially impacting every facet of individuals' lives.

2.2. **RIGHT TO DATA PROTECTION AND PROHIBITION AGAINST UNAUTHORIZED DATA COLLECTION OR USE**

Indirectly supported by international legal provisions on the right to privacy, such as the UDHR and ICCPR, the right to data protection refers to the legal entitlement of individuals to control their personal data and safeguard it from unauthorized access or misuse (see Taylor 2020: 475–78). Personal data entails any information that can identify a person either directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location

Table 2.1. **Right to (digital) privacy**

Chile [rejected draft] 2022	Chapter II. Fundamental Rights and Guarantees Article 70	Everyone has the right to personal, family and community privacy. No person or authority may affect, restrict or impede its exercise, except in the cases and forms determined by law. Private premises are inviolable. The entry, search or seizure may only be carried out with a prior court order, except in cases of flagrant crime as established by law. All private documentation and communications are inviolable, including their metadata. Interception, seizure, opening, registration or search may only be carried out with a prior court order.
Dominican Republic 2015	Title II. Fundamental Rights, Guarantees and Duties Article 44	All people have the right to privacy. The respect and non-interference into private and family life, the home, and private correspondence are guaranteed. … The inviolability of private correspondence, documents, or messages in physical, digital, electronic, or all other formats is recognized …
Peru 1993	Chapter I. Fundamental Rights of the Person Article 2(6)	Every person has the right: … To the assurance that information services, whether computerized or not, whether public or private, will not provide information affecting personal and family privacy.

data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (European Union 2016: article 4).

As societies shift towards increasingly interconnected digital ecosystems, the essence of data protection is challenged by the vast amounts of data collected in almost every aspect of modern life, often without explicit knowledge or consent by the average person. By automating tasks that were once manual, digital tools allow for the collection and real-time processing of vast data sets with advanced analytics that increase accuracy and efficiency. Furthermore, the rise

Box 2.1. **Protecting rights from legislative overreach: *Disini v The Secretary of Justice***

The Supreme Court of the Philippines evaluated the Cybercrime Prevention Act of 2012 to determine whether several of its provisions contravened constitutional rights, specifically the rights to freedom of expression and privacy. The provisions under scrutiny included section 4(c)(3), which pertained to unsolicited commercial communications; section 12, which authorized the real-time collection of computer data without a warrant; and section 19, which allowed the government to restrict or block access to computer data without judicial oversight (Columbia University Global Freedom of Expression n.d.b).

The Philippines Constitution safeguards the rights to freedom of expression and privacy against unreasonable searches and seizures. In applying these principles, the Court utilized the 'rational basis standard' to ensure that any law infringing upon constitutional rights must be narrowly tailored to serve a compelling governmental interest. Additionally, the 'expectation of privacy standard' was employed to ascertain whether the privacy claims were justifiable by evaluating if there was a legitimate and objectively reasonable expectation of privacy. In its decision, the Court identified spam as a form of commercial speech which, though not as protected as other types of speech, is nonetheless entitled to some level of protection under the right to freedom of expression (Columbia University Global Freedom of Expression n.d.b).

The Court also found that the absolute prohibition of unsolicited commercial communications imposed by section 4(c)(3) was overly broad and unduly restrictive of the right to receive information and therefore unconstitutional.

Regarding section 12, the Court raised concerns about privacy due to the allowance of warrantless surveillance of Internet traffic data. Despite acknowledging the government's interest in thwarting cybersecurity threats, the Court ruled that the provision lacked the necessary specificity and safeguards against abuse, failing to meet the rational basis standard. Although the Court noted that, while users might subjectively expect privacy in their Internet communications, this expectation is not always objectively reasonable. However, the potential for the law's overreach without adequate checks led to its declaration as unconstitutional (Columbia University Global Freedom of Expression n.d.b).

Finally, section 19 was criticized for enabling the Department of Justice to block access to computer data without judicial review, which was found to violate not only the right to freedom of expression but also protections against unreasonable searches and seizures. The Court emphasized that any interference with these rights must typically be accompanied by a judicial warrant to ensure legality and proportionality, concluding that the absence of such oversight rendered the section unconstitutional (Columbia University Global Freedom of Expression n.d.b). In this ruling, the Supreme Court reaffirmed the essential balance between upholding security measures and protecting constitutional freedoms in the digital age.

Box 2.2. **Reinforcing the right to be secure against unreasonable search or seizure in the digital age**

The central issue in *R. v Spencer*[1] was whether the police had violated the accused's rights under section 8 of the Canadian Charter of Rights and Freedoms, which protects against unreasonable search and seizure, by obtaining his subscriber information associated with an IP address from an ISP without a warrant.

Section 8 of the charter ensures that everyone has the right to be secure against unreasonable search or seizure. This right requires that any search or seizure must be conducted lawfully, with a warrant, unless exigent circumstances justify otherwise. The Supreme Court had previously established that information that can reveal personal details, habits and activities, thereby impacting an individual's reasonable expectation of privacy, is protected under section 8. In this case, the police identified an IP address that had been used to access and share image- and video-based child sexual abuse. They requested and obtained the subscriber information linked to this IP address from the ISP, Shaw Communications, without a warrant. This action was challenged as being an unreasonable search and seizure under the charter.

The Supreme Court had to determine whether there was a reasonable expectation of privacy concerning an IP address's subscriber information. The Court noted that the nature of the information accessible through IP addresses could reveal substantial personal details about an individual, including one's online activities, which are inherently private. As such, the Court held that individuals do have a reasonable expectation of privacy in relation to the subscriber information linked to their IP address.

The Court then assessed whether obtaining this information without a warrant was lawful. The police had relied on a section of the Criminal Code which allows for law enforcement to obtain subscriber data from a telecom provider, and the Personal Information Protection and Electronic Documents Act, which outlines how private sector organizations may manage personal information. The Court found that neither the code nor the act authorized the police to obtain the subscriber information without a warrant, particularly in a situation where the user had a reasonable expectation of privacy.

The Court concluded that obtaining subscriber information violated section 8 of the charter, as the search was conducted without a warrant and not justified by law or exigent circumstances.

The Court's decision clarified the limits of law enforcement's ability within the digital space. Like a private home, private subscriber information is protected under the right to privacy and cannot be accessed without a warrant.

1 *R v Spencer* (2014) 2 SCR 212, 2014 SCC 43 (CanLII).

Box 2.3. **High privacy standards for digital data on mobile phones**

In a similar case, *Riley v California*,[1] a person was stopped for a traffic violation, and his subsequent arrest led to the warrantless search of his cell phone, revealing evidence linking him to criminal activities. The key legal issue in this case was whether the police are required to obtain a warrant to search digital information on a cell phone seized from an individual during an arrest, or if such a search falls under the exceptions to the warrant requirement, typically applied to searches incident to an arrest.

The Fourth Amendment to the US Constitution protects citizens from unreasonable searches and seizures, stating that a warrant must generally be secured.

The defence argued that digital data on cell phones could neither pose a threat to police safety nor be used by the arrestee to escape, rendering the warrantless search unreasonable and overly broad. The prosecution contended that the search was necessary and urgent due to the potential destruction of digital evidence.

The Court considered the differences between the type and amount of information accessible on cell phones and that found in physical searches during arrests. Recognizing that cell phones often contain extensive personal data comparable to the contents of one's home, the Court ruled unanimously that such digital information warrants greater privacy protections. It concluded that, because cell phones hold vast quantities of personal data unrelated to any crime, searching them without a warrant during an arrest violates the Fourth Amendment.

This ruling is particularly significant, as it recognized the need to adapt traditional principles of search and seizure to the digital context to align constitutional protections with the realities of modern technology.

1 573 US 373 (2014).

of cloud computing provides scalable and cost-effective storage and processing solutions, facilitating broader data accessibility, while AI and machine learning offer profound advancements in pattern recognition and predictive analytics.

Collectively, the use of big data analytics, AI and ubiquitous online tracking technologies undermines individuals' ability to control their personal information. Every click, search, like and share is meticulously tracked through technologies like cookies and pixels (Silverman et al. 2022). The data users unintentionally leave behind while using these services—referred to as 'behavioural surplus' (see Zuboff 2019)—is harvested by companies like Google and Meta. By analysing this behavioural surplus, they gain deep insights into user

Box 2.4. **Balancing online content moderation with the right to information and freedom of expression**

The core issue in ADI 5527—a legal case before Brazil's Supreme Federal Court—was the constitutionality of certain provisions within Brazil's Civil Rights Framework for the Internet, commonly known as the 'Internet Bill of Rights'. These provisions addressed the liability of Internet platforms regarding content posted by their users, specifically outlining the conditions under which the platforms are required to remove content based on court orders or notifications of privacy or personal rights violations.

Brazil's Civil Rights Framework for the Internet is a federal law which sets legal guidelines to govern the Internet, aiming to ensure privacy, net neutrality and freedom of expression online. Article 19 states that ISPs are not liable for content published by their users unless they fail to comply with a court order to remove such content. The exemption of ISPs from liability is supported by the Brazilian Constitution, which safeguards freedom of expression and the right to privacy—fundamental in evaluating the legality of online content moderation.

In this case, Brazil's Supreme Federal Court was tasked with examining the balance between freedom of expression and the rights to privacy and personal honour, as outlined in the Internet Bill of Rights. The petitioners argued that the stipulation requiring court orders before ISPs are compelled to remove content provided excessive protection for the freedom of expression, potentially at the expense of other fundamental rights, such as privacy. This level of protection, they claimed, could lead to the unchecked dissemination of harmful content, including fake news and defamatory material.

The Court evaluated whether the judicial order requirement for content removal imposed an undue burden on individuals seeking to protect their privacy or personal rights, potentially rendering it constitutionally disproportionate and inconsistent. It also assessed whether these provisions struck a fair balance between the right to information and freedom of expression on the Internet and protection against abuses and personal rights infringements.

Ultimately, the Court upheld the constitutionality of the Internet Bill of Rights, specifically affirming the judicial order requirement for content removal as a valid measure that appropriately balances freedom of expression with the protection of personal rights. The Court concluded that this requirement did not place an excessive burden on the right to privacy or personal dignity but was, instead, a necessary safeguard to protect against censorship and the arbitrary removal of content.

This decision underlined the Court's commitment to maintaining a balanced approach to content regulation on the Internet, ensuring that freedom of expression is preserved while protecting individuals from privacy violations and other abuses (Atta and Moraes 2020).

behaviour, enabling them to tailor advertisements and content with unprecedented precision.

However, states also collect and process vast amounts of data for various purposes, ranging from improving administrative efficiency and public service delivery to national security and law enforcement. For example, data on employment history, family income, health status and more is collected and analysed to administer social welfare programmes such as unemployment benefits, disability assistance and food security programmes. Governments and national security agencies use surveillance systems, including closed-circuit television (CCTV) networks, licence plate readers and facial recognition technologies, and monitor communications, financial transactions and other activities to identify and prevent potential threats (United Kingdom Government 2017).

Worldwide, there have been notable cases where state actors have been accused of the unconstitutional collection of data. As revealed during Edward Snowden's disclosures in 2013, the US National Security Agency (NSA) had been collecting the phone records of millions of Americans and foreign nationals in bulk, without a warrant or any suspicion of wrongdoing. Under the PRISM programme, the NSA obtained direct access to the servers of major US technology companies, including Apple, Google, Meta, and others. This access enabled the NSA to collect a wide range of data, including emails, chats from online communication tools, videos, photos, stored data, file transfers, video conferencing and logins. Documents suggested that surveillance data was used not only for counterterrorism efforts but also for economic espionage and political surveillance of foreign leaders and businesses, going beyond the original national security intentions (Macaskill and Dance 2013; Taitz 2023). China, perhaps the country that conducts the most extensive collection of data on its citizens, employs a vast network of CCTV cameras enhanced with facial recognition technology. The data from these cameras feeds into the social credit system, which integrates various data sources to evaluate the social behaviours of individuals and businesses. Scores from this system can have significant impacts, such as restricting access to flights and train tickets (Mitchell and Diamond 2018; Qian et al. 2022).

In addition to the threats posed by the unauthorized collection or use of data, the insufficient protection of data has become another challenge to people's privacy in the digital age. The possibilities of the increased collection and processing of data through new digital

Worldwide, there have been notable cases where state actors have been accused of the unconstitutional collection of data.

technologies has led to an increased risk of privacy breaches and unauthorized data use. In the past decade, many databases owned by entities like the Indian Council of Medical Research and T-Mobile, along with platforms such as MySpace, X (formerly Twitter) and Yahoo, have been compromised, revealing sensitive information, including names, email addresses, telephone numbers, dates of birth and hashed passwords. In some cases, even security questions and answers have been exposed. This data has been found for sale on hacking forums and the dark web, significantly elevating the risk of phishing and other identity theft tactics (Komnenic 2024).

Many jurisdictions have passed laws on data protection, with the EU's General Data Protection Regulation being one of the most advanced. These laws emphasize principles such as lawfulness, purpose limitation, necessity and proportionality, setting minimum standards for the retention and processing of personal data, including across borders (European Union 2016).

Many constitutions contain general provisions related to data protection, with some countries, such Cabo Verde and Greece, specifically contemplating digital data protection. Constitutions often ban the unauthorized gathering or improper handling of personal data, including by electronic means, and delineate specific categories of sensitive information that are safeguarded against collection and utilization, with exceptions for research and statistical analysis, provided that the information is anonymized. This category of sensitive data typically encompasses affiliations with political and trade unions, ideological views, religious convictions and ethnic backgrounds.

Many constitutions contain general provisions related to data protection, with some countries specifically contemplating digital data protection.

Furthermore, in the digital era, where personal data essentially extends one's identity into the virtual realm, many constitutions, charters, declarations and legal frameworks have recognized the right to data protection as encompassing not only privacy but also the broader aspects of dignity and individual identity in the digital age (Celeste 2022: 194). For example, article 5 of the Italian Declaration of Internet Rights reads: 'Everyone has the right to the protection of the data that concern them in order to ensure respect for their dignity, identity and privacy' (Italian Republic 2015). Many Internet bills of rights and declarations grant individuals the ability to access, rectify, transfer and erase their data. Some go as far as to assert a right to data ownership, suggesting that personal data, despite its scattered presence across various platforms, remains an integral and inalienable part of an individual's identity. This ownership is

envisioned to persist beyond death, allowing for the transfer of an individual's data to their heirs (Celeste 2022: 195).

Both state and non-state actors leverage technology to collect vast amounts of data, necessitating legal protections. Widespread data collection exceeding acceptable boundaries is not only a breach of privacy but also a significant risk, as demonstrated by numerous incidents of data breaches and misuse across various platforms and entities.

2.3. **RIGHT TO COMPUTER SECURITY OR CYBERSECURITY**

Secure information technology is crucial not only for protecting sensitive data but also for building trust in government institutions. The Center for Strategic and International Studies has documented over 900 grave cyber incidents since 2006, including state-sponsored cyberattacks on the public sector in many countries, ransomware, phishing or activities by so-called hacktivists as a form of social and political activism (CSIS n.d.).

Protecting citizens' data builds the trust that spurs engagement with—and benefits from—digital public services. This trust is further reinforced by stringent data protection laws worldwide, which require the handling of personal data in line with high security standards, including safeguards against unauthorized access, accidental loss, or damage (State of California 2018: sections 1798.105 and 1798.140; Republic of India 2023). Additional protections include technical or organizational safeguards against unauthorized or illegal processing, accidental loss, destruction or damage (Wolford n.d.).

The inclusion of computer security and cybersecurity rights in Chile's proposed constitution represents a notable development that signifies an evolving understanding of digital rights as fundamental to the security of citizens and trust in public systems. Similar initiatives, such as the African and Italian declarations on net security and Spain's legislation on digital security, reinforce the critical role of strong cybersecurity measures. Ensuring that the benefits of the digital age are realized securely and inclusively not only protects individual rights but also ensures the reliable and secure growth of digital infrastructure.

Table 2.2. **Right to data protection and prohibition against unauthorized data collection or use**

Algeria 2020	Chapter I. Fundamental Rights and Public Freedoms Article 47	… The protection of individuals when handling personal data shall be a fundamental right. The violation of these rights shall be punishable by law.
Greece 1975	Part II, Individual and Social Rights Article 9(A)	All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law.
Slovakia 1992	Chapter II. Basic Rights and Freedoms Article 19(3)	… Anyone has the right to be protected against unwarranted collection, disclosure, and other misuse of personal information.
Portugal 1976	Part I. Fundamental Rights and Duties Article 35(3) (Use of Computers)	… Computers shall not be used to treat data concerning philosophical or political convictions, party or trade union affiliations, religious beliefs, private life or ethnic origins, save with the express consent of the datasubject, with authorization provided for by law and with guarantees of non-discrimination, or for the purpose of processing statistical data that cannot be individually identified.
Cabo Verde 1980	Part II. Rights and Duties of Citizens Article 42(3) (Utilization of Computer Records)	… No one shall have access to archives, files, computer records, or databases to find out personal data regarding a third party, nor transfer personal data from one computer file to another belonging to various services or institutions except in cases provided by law or judicial decision.

2.4. RIGHT TO INFORMATIONAL SELF-DETERMINATION AND THE RIGHT TO BE FORGOTTEN

The concept of self-determination has long existed in various forms, traditionally relating to a person's (or a people's) right to determine their own political status without external compulsion or interference (Cats-Baril 2018). This right is enshrined in international law, particularly in instruments like the UN Charter and the ICCPR,

Box 2.5. **Protecting privacy and data against overreach in crime prevention and prosecution**

In 2014 the Court of Justice of the European Union (CJEU) made a significant decision in the Digital Rights Ireland case[1] against an EU directive that mandated ISPs to retain telecommunications data to aid in crime prevention and prosecution. The CJEU determined whether EU Directive 2006/24/EC, mandating ISPs to store telecommunications data for preventing and prosecuting serious crime, was compatible with articles 7 and 8 of the Charter of Fundamental Rights of the European Union, which protect privacy and personal data.

Articles 7 and 8 of the charter safeguard an individual's right to privacy and to the protection of personal data. Any limitation of these rights must comply with article 52(1) of the charter, which requires that restrictions be provided by law, respect the essence of fundamental rights and be proportionate to the legitimate aims pursued.

The CJEU examined whether the directive met these requirements. The directive aimed to help combat serious crime across the EU by harmonizing member states' data retention practices. However, the Court found the directive excessively broad and lacking in necessary safeguards, such as clear rules on the duration of data storage, the use of data and access to data by authorities. This lack of specificity led to potential mass surveillance, impacting all EU citizens' fundamental rights indiscriminately and for periods ranging from 6 to 24 months.

The CJEU ruled the directive invalid, as it failed the proportionality test. While the directive's goal of fighting serious crime was legitimate, the means of achieving this goal via mass data retention were not adequately balanced against the fundamental rights to privacy and personal data protection.

The Court's ruling reinforced the importance of protecting individual privacy rights even in the face of security challenges.

1 CJEU C-293/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* [2014].

which highlight the right of nations and peoples to self-determination (United Nations 1945: article 1[2]).

In the analogue era, the individual's right to self-determination was predominantly associated with personal freedom, autonomy and privacy. Although this right included the ability to make decisions about one's life and personal data to a certain extent, it was not

Table 2.3. **Right to computer security or cybersecurity**

Chile [rejected draft] 2022	Chapter II Fundamental Rights and Guarantees Article 88	Every person has the right to the protection and promotion of computer security. The State and individuals must adopt the appropriate and necessary measures to guarantee the integrity, confidentiality, availability and resilience of the information contained in the computer systems they manage, except in the cases expressly indicated by law.

explicitly articulated as such in law until the advent of detailed privacy laws.[9]

The digital era's right to self-determination is somewhat new and more explicitly defined than its analogue counterpart.

The digital era, however, has necessitated a more concrete definition and expansion of the right to self-determination, primarily due to the profound ways in which data is now collected, used and stored. With the ubiquity of online communication, individuals face potential infringements of their privacy and reputation from outdated or incorrect information persisting online, especially when personal data is so easily accessible and distributable across the Internet. Consequently, the digital era's right to self-determination is somewhat new and more explicitly defined than its analogue counterpart (Vivarelli 2020). It encompasses not just the broader concept of autonomy but also specific rights to access, control, manage, correct and delete personal data, as well as to understand why and how it is collected (European Union 2016; AUDRi 2022).

Although it shares similarities with privacy rights and data protection, informational self-determination has unique attributes. It focuses on an individual's authority over the disclosure and use of their personal data, contrasting with traditional privacy rights, which primarily focus on protection from invasive searches. Informational self-determination encompasses a broad range of rights and freedoms, including freedom of speech, the right to privacy, the right to personal data protection and the right to access public sector information, thus offering a comprehensive framework for personal autonomy in the information age (Gutwirth et al. 2009; Kodde 2016).

9 See, for example, the landmark decision in Germany in 1983 on the right to self-determination: BVerfGE 65, 1—Volkszählung Urteil des Ersten Senats vom 15. Dezember 1983 aufgrund der mündlichen Verhandlung vom 18. und 19. Oktober 1983—1 BvR 209, 269, 362, 420, 440, 484/83in den Verfahren über die Verfassungsbeschwerden.

Several countries have already recognized the right to self-determination in their constitutions (Table 2.4).

Illustrative cases highlight how the concept of self-determination has evolved to address challenges specific to data and privacy. A foundational case is the 2014 European Court of Justice case of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*.[10] The Court's ruling acknowledged the potential for lasting damage caused by the Internet's perpetual memory and highlighted the right to control one's personal information online, particularly the ability to request the correction or removal of such information from search engines under certain conditions (Crowther 2014; Allegri 2022). The judgment in this case played a significant role in the establishment of a right to be forgotten in EU jurisprudence (Crowther 2014).

In June 2023 a right to be forgotten was constitutionally enshrined for the first time in the substate constitution of the Geneva Canton in Switzerland, under the innovative right to digital integrity (Guglya 2023). This development marks a significant step in acknowledging and addressing the challenges of maintaining personal dignity and privacy in the digital age.

2.5. **RIGHT TO INTERNET ACCESS AND DIGITAL CONNECTIVITY**

The Internet has become a cornerstone of many people's daily lives. It is used for a range of purposes, including communication, accessing information and knowledge, influencing economic growth, advancing education and healthcare, and enhancing democratic participation. The ability to access an unmatched breadth and depth of knowledge and data on virtually any subject breaks down barriers that once limited individuals based on geography, economic status, sex or social class.

Digital connectivity has emerged as a pivotal driver of economic development, enabling businesses to access broader markets, creating employment opportunities and playing a key role in the transition to service-oriented, knowledge-based economies. For individuals, the Internet serves as both a platform for upskilling

10 Case C-131/12 [2014] ECLI:EU:C:2014:317.

Table 2.4. **Right to informational self-determination or informational autonomy**

Chile [rejected draft] 2022	Article 87(1)	Everyone has the right to informational self-determination and the protection of personal data. This right includes the power to know, to decide and control the use of the concerned data, to access, to be informed and oppose the treatment of them, and to obtain their rectification, cancellation and portability, notwithstanding other rights established by statute. …
Albania 1998	Chapter II. Personal Rights and Freedom Article 35	1. No one may be obliged, except when the law requires it, to make public the data connected with his person. The collection, use and making public of data about a person is done with his consent, except for the cases provided by law. 2. Everyone has the right to become acquainted with data collected about him, except for the cases provided by law. 3. Everyone has the right to request the correction or expunging of untrue or incomplete data or data collected in violation of law.
Ecuador 2008	Chapter 3. Jurisdictional Guarantees Section 5. Habeas Data Proceedings Article 92	All persons, by their own rights or as legitimate representatives for this purpose, shall have the right to know of the existence of and gain access to documents, genetic data, personal data banks or files and reports about themselves or about their assets that appear in public or private entities, whether in hard copy or on electronic media. Likewise, they shall have the right learn about the use made of this information, its end purpose, the origin and destination of the personal information and the time of validity of the data file or bank. The persons responsible for the data banks or files will be able to disseminate the filed information with the authorization of the holder or the law. The person owning the data will be able to request the person in charge to allow access free of charge to the file, as well as update of the data and their correction, deletion or annulment. In the case of sensitive data, whose file must be authorized by law or by the person owning the information, the adoption of the security measures that are needed shall be required. If the petition is not duly answered, the person can resort to a judge. The affected person can file a complaint for damages caused.
Portugal 1976	Fundamental Rights and Freedoms Article 35(1)	Every citizen shall possess the right to access to all computerised data that concern him, to require that they be corrected and updated, and to be informed of the purpose for which they are intended, all as laid down by law. …

Table 2.4. **Right to informational self-determination or informational autonomy (cont.)**

Mozambique 2004	Title III. Fundamental Rights, Duties and Freedoms Article 71 (Use of Computerised Data)	1. The use of computerised means for recording and processing individually identifiable data in respect of political, philosophical or ideological beliefs, of religious faith, party or trade union affiliation or private lives, shall be prohibited. 2. The law shall regulate the protection of personal data kept on computerized records, the conditions of access to data banks, and the creation and use of such data banks and information stored on computerised media by public authorities and private entities. 3. Access to databases or to computerised archives, files and records for obtaining information on the personal data of third parties, as well as the transfer of personal data from one computerised file to another that belongs to a distinct service or institution, shall be prohibited except in cases provided for by law or by judicial decision. 4. All persons shall be entitled to have access to collected data that relates to them and to have such data rectified.

through online education and a vehicle for entrepreneurial ventures via e-commerce. The World Bank and other international organizations have demonstrated a strong correlation between broadband expansion and gross domestic product growth in developing countries, emphasizing the economic necessity of widespread Internet access (Hjort and Sacchetto 2022). This relationship between connectivity and economic progress is also reflected in the SDGs. For example, target 9.c calls for a significant increase in Internet access globally, while target 5.b focuses on harnessing information and communication technology (ICT) to empower women, leveraging technology to advance gender equality (United Nations General Assembly 2015).

Governments worldwide are increasingly moving services online, from filing taxes to applying for permits and social benefits. Internet access supports civic participation by enabling citizens to vote, express opinions and mobilize for social causes online. In contexts where traditional media may be restricted, the Internet provides a platform for political discourse and advocacy. The Internet's ability to fill this gap shows how fundamental Internet access and digital connectivity have become to modern societies and people's daily freedoms.

Governments worldwide are increasingly moving services online, from filing taxes to applying for permits and social benefits.

Table 2.5. **Right to be forgotten**

Canton of Geneva 2013 [substate Constitution]	Title II Fundamental Rights Article 21A	1. Everyone has the right to safeguard their digital integrity. 2. Digital integrity includes, in particular, the right to be protected against misuse of data relating to his or her digital life, the right to security in the digital space, the right to an offline life and the *right to be forgotten*. …

Source: Constitution de la République et canton de Genève [Constitution of the Republic and Canton of Geneva], 1 January 2025, <https://silgeneve.ch/legis/program/books/rsg/pdf/rsg_a2_00.pdf>, accessed 25 March 2025.

However, Internet shutdowns continue to be a growing concern. According to data collected by the digital rights NGO Access Now, governments and other actors disrupted the Internet at least 187 times across 35 countries in 2022 alone (Access Now 2023c). Internet shutdowns frequently occur in politically sensitive times, such as during elections or in the context of protests and political crises. Authorities often refrain from publishing information about these shutdowns, deny acknowledging disruptions or outright reject having ordered any interventions (United Nations Human Rights Council 2022b: paras 20 and 24–25). The UN special rapporteur on the promotion and protection of the right to freedom of opinion and expression has documented cases such as Tajikistan blocking messaging services and social media during protests (United Nations General Assembly 2016). Similarly, Gabon has experienced network disruptions during elections, while Russia has blocked major online platforms to control the flow of information (Budnitsky 2022). These measures are seen as efforts by governments to manage public discourse, influence opinion and oppress dissent during politically significant events (United Nations General Assembly 2016).

The Office of the United Nations High Commissioner for Human Rights notes that 'targeted shutdowns of a communications service provided through the Internet may be deemed proportionate and justifiable only in the most exceptional circumstances, as a last resort when necessary to achieve a legitimate aim, as defined by article 19 (3) of the [UN] Covenant [on Civil and Political Rights], such as national security or public order, and when no other means are effective to prevent or mitigate those harms' (United Nations Human Rights Council 2022b: para. 13). However, 'given their indiscriminate

reach and broad impacts, Internet shutdowns very rarely meet the fundamental requirements of necessity and proportionality. Their adverse impacts on numerous rights often extend beyond the areas or periods of their implementation, rendering them disproportionate, even when they are meant to respond to genuine threats' (United Nations Human Rights Council 2022b: para. 59).

In this context, the debate on the right to an open and interoperable Internet becomes increasingly relevant. As the world faces growing instances of Internet fragmentation—where governments or other actors deliberately limit access to or control online information—the push for maintaining an open and globally connected Internet has been more widely discussed, including by the Council of Europe and the EU (Council of Europe 2014; European Commission 2022). These discussions have included demands for an open and interoperable Internet to ensure that users, regardless of their location, can access the same information and services, protecting human rights by, for example, fostering freedom of expression, transparency and inclusivity (Global Partners Digital 2021; European Commission 2022). Furthermore, the idea of an open and interoperable Internet is seen as crucial in protecting individuals' rights in the digital age, as shutdowns and censorship measures erode not only the freedom of expression but also economic, social and cultural rights.

While Internet shutdowns pose a significant challenge, another key issue is the disparity in access to Internet services. According to the latest data from the UN's International Telecommunication Union (ITU), 2.6 billion people worldwide still lacked Internet access as of 2023 (ITU 2023). Although this figure represents a slight decrease from the 2.7 billion people reported in 2022, a significant portion of the global population remains offline. The ITU report also indicates significant disparities in connectivity between urban and rural areas, especially in poorer regions. Africa, for instance, continues to experience substantial challenges in digital connectivity, with only 36 per cent of the continent's population having broadband Internet access as of 2023. Similar challenges exist in parts of Asia and Latin America, where inadequate infrastructure, affordability and a lack of digital literacy further impede access to digital technologies (ITU 2023).

While Internet shutdowns pose a significant challenge, another key issue is the disparity in access to Internet services.

Limited access to technologies and digital connectivity disproportionately affects women. Globally, Internet access is available to 63 per cent of women, compared with 69 per cent of men. Additionally, women are 12 per cent less likely than men to own a mobile phone. Factors such as race, age, disability, socio-

economic status and geographic location have a significant influence on digital connectivity for women. In particular, marginalized groups of women—like older women, rural women and women with disabilities—experience acute barriers to access. Although mobile broadband reaches 76 per cent of the population in the least developed countries, only 25 per cent of women are connected, with men 52 per cent more likely than women to be online (UN Women 2023). This digital gender gap exacerbates existing social, political and economic inequalities.

Recognizing access to the Internet and digital connectivity as a right, a vital gateway necessitating freedom from interference by any third party, be it a governmental or non-state actor, may be crucial for personal and collective development. The UN Human Rights Council has emphasized that both states and companies, particularly telecommunications and Internet service providers, have responsibilities in preventing and responding to government-ordered shutdowns. Companies must take preventive measures, implement transparency mechanisms and challenge disruptions through lawful means (United Nations Human Rights Council 2022b: paras 47–51). Access to the Internet is, therefore, recognized in many Internet bills of rights as a means of engaging in social life and exercising one's fundamental rights.

Some countries have interpreted the right to Internet access and digital connectivity as being included within existing constitutional provisions.

Some countries have interpreted the right to Internet access and digital connectivity as being included within existing constitutional provisions. A survey by the ECtHR reveals that the right to Internet access is protected under constitutional guarantees related to the freedom of expression and the freedom to receive ideas and information across all 20 Council of Europe member states surveyed.[11] This right is seen as integral to the broader right to access information and communication as outlined in national constitutions, emphasizing both the individual's right to participate in the information society and the state's obligation to ensure that citizens have Internet access.[12]

The emphasis on Internet access as an enabler of other rights and freedoms underlines the necessity of not only theoretical access but also substantive prerequisites to ensure real and effective connectivity (Çalı 2020; Celeste 2022).

11 Austria, Azerbaijan, Belgium, the Czech Republic, Estonia, Finland, France, Germany, Ireland, Italy, Lithuania, the Netherlands, Poland, Portugal, Romania, Russia, Slovenia, Spain, Switzerland and the UK.

12 *Ahmet Yildirim v Turkey* App no 3111/10 (ECtHR, 18 December 2012).

Table 2.6. **Right to Internet access and universal digital connectivity**

Mexico 1917 (rev. 2015)	Title One: Chapter I. Human Rights And Guarantees Article 6(3)	… The State shall guarantee access to information and communication technology, access to the services of radio broadcast, telecommunications and broadband Internet. To that end, the State shall establish effective competition conditions for the provision of such services.
Greece 1975	Part II. Individual and Social Rights Article 5A(2)	All persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State …
Peru 1993	Chapter I. Fundamental Rights Of The Person Article 14(A)	The State guarantees, through public or private investment, access to free Internet throughout the national territory, with special emphasis on rural areas, peasant and native communities.
Colombia [rejected draft] 2022[1]	Title II: On Rights, Guarantees, And Duties Article 20	Everyone is guaranteed the freedom to express and disseminate their thoughts and opinions, to report and receive truthful and impartial information, to effectively access the Internet, and to found mass media …

1 Petro Urrego, H. S. G., et al., 'Por medio del cual se establece el internet como derecho fundamental', Cámara de representantes, 11 May 2022, <https://www.camara.gov.co/Internet-derecho-fundamental-2>, accessed 2 April 2025; Muñoz Lopera, L. F., 'Proyecto de Acto Legislativo No. ___ De 2022 "Por medio del cual se establece el internet como derecho fundamental', Cámara de representantes, 30 March 2022, <https://www.camara.gov.co/sites/default/files/2022-03/P.A.L.442-2022C%20INTERNET%20DERECHO%20FUNDAMENTAL%29.pdf>, accessed 2 April 2025.

Box 2.6. **Internet access as a derivative fundamental right**

In 2020 the Economic Community of West African States Court of Justice decided on the legality of an Internet shutdown during protests in Togo in September 2017, specifically assessing its compliance with the right to freedom of expression (Columbia University Global Freedom of Expression n.d.c).

The Court drew on article 25 of the Togolese Constitution and article 9 of the African Charter on Human and Peoples' Rights, which protect the rights to receive information and to express and disseminate opinions. Both norms mandate that any infringement on these fundamental rights must be explicitly authorized by law to ensure that any derogation, such as an Internet shutdown, is based on clear, lawful grounds that are specifically justified and are necessary and proportionate to the intended legitimate aims, such as national security.

In its judgment, the Court emphasized that, although Internet access is not listed explicitly as a fundamental right, it is deemed a derivative right crucial for exercising the right to freedom of expression. The Court also determined that there was no national legislation that would have supported the Internet shutdown as a lawful derogation from the right to access the Internet.

Therefore, the Court found that the government's action to disable Internet access without a legal basis, purportedly on national security grounds, was unlawful. Concluding that the Togolese Government's shutdown of the Internet unlawfully infringed upon the right to freedom of expression, the Court mandated that Togo implement measures to prevent such incidents in the future, enact laws aligning with their obligations to protect freedom of expression and compensate each applicant in the amount of CFA 2,000,000 (approximately USD 3,500) (Krapiva 2020).

2.6. **RIGHT TO DIGITAL PARTICIPATION, LITERACY AND INCLUSION**

The right to public participation, recognized in many international instruments, allows citizens to engage in decision-making processes (for example, article 25 of the ICCPR). Traditionally, this right involved attending town hall meetings, voting in person and engaging in face-to-face civic activities. However, digital technologies have expanded these avenues, introducing new ways for public engagement and participation, particularly in how opinions are voiced and how electronic electoral processes function.

With the digital transformation, the scope and methods of public participation have expanded significantly. Digital platforms have made it possible for more people to engage in political discourse.

Social media, blogs and forums enable users to share their opinions and news instantly with a global audience. Even governments and officials use these platforms not only to disseminate information but also to interact with the public through polls, surveys and question-and-answer sessions. For example, cities like Boston and New York used social media to engage with residents on various policies and community issues during the Covid-19 pandemic, facilitating broader and more inclusive participation (Statusbrew 2022). Unlike traditional town hall meetings, which occur periodically, online platforms facilitate continuous discussions and debates. Individuals are offered various ways to express their views, from posting written opinions and sharing video content to participating in virtual protests and signing digital petitions.

Recognizing the potential of these digital advancements, Chile's 2022 draft constitution, for instance—though ultimately rejected—acknowledged and emphasized the digital aspects of the right to public participation.

Nevertheless, for digital democracy to be effective, countries must not only promote but also support citizens' ability to participate digitally, anchoring this ability in the protection of fundamental human rights, including the right to participate in public life, as recognized in instruments such as the ICCPR (article 25). Replacing processes that were once analogue with their digital counterparts could essentially exclude from public participation many people who either lack access to these technologies or who lack digital literacy. Particularly in marginalized and rural areas, people are vulnerable to having limited access to public information and state services, which impacts other fundamental rights such as freedom of expression.

Replacing processes that were once analogue with their digital counterparts could essentially exclude many people from public participation.

The UN special rapporteur for education thus advocates for a right to education that 'include[s] digital agency as a goal, understood as the ability to control and adapt to a digital world with digital competence, digital confidence and digital accountability' (United Nations Human Rights Council 2022a: para. 37). Also, the International Commission on the Futures of Education, convened by the director-general of UNESCO, advocates for recognition of digital literacy and Internet access as fundamental rights in the 21st century. The Commission emphasizes the importance of expanding the concept of the right to education to encompass digital competencies and access, thereby reinforcing the right to education, the right to information and cultural rights (UNESCO n.d.). Furthermore, under article 27 of the UDHR and article 15 of the ICCPR, everyone has the right to share in scientific advancement and its benefits.

Central to this digital transformation is the concept of 'digital citizenship'. UNESCO defines digital citizenship as the ability to efficiently locate, access, use and create information; actively, critically and ethically engage with content and other users; and navigate online and ICT environments safely and responsibly, while being mindful of one's rights (UNESCO n.d.). Other definitions of digital citizenship emphasize the importance of understanding the principles governing the digital environment and analysing the role of technology in society, its impact on daily life and its use for social engagement. A digital citizen should be able to navigate the complexities of the digital world; grasp the social, economic, political and educational implications of technology; and practise responsible stewardship of digital tools. Education and training should also focus on raising awareness and understanding of AI technologies and the significance of data (United Nations Human Rights Council 2022a).

The Constitution of the Canton of Geneva, in this light, asserts that '[The Canton] promotes digital inclusion and raises awareness of digital issues', acknowledging the critical role of digital inclusivity in ensuring equitable access to public services and political participation and preventing a further exacerbation of existing inequalities (Swiss Confederation 2012: article 21[A][4]).

The European Declaration on Digital Rights, although not binding, also addresses these concerns by dedicating a chapter to solidarity and inclusion. This chapter emphasizes the importance of connectivity, digital education, training and skills, alongside fair and just working conditions, underscoring the interconnected nature of digital inclusivity and broader social and economic rights (European Union 2023).

It must be noted that the increased digitalization of education presents opportunities for and risks to the right to education.

It must be noted that the increased digitalization of education presents opportunities for and risks to the right to education. The UN special rapporteur on the right to education has addressed these issues extensively, noting that the Covid-19 pandemic accelerated the integration of digital technologies into educational strategies. This shift has introduced several key trends, including blended learning approaches that combine face-to-face instruction with computer-mediated activities, distance learning tailored for non-traditional students and those in emergency situations, and the use of AI to identify learning patterns and suggest curriculum activities.

The digitalization of education has the potential to enhance the essential features of availability, accessibility, acceptability and

adaptability in education, as outlined by the Committee on Economic, Social and Cultural Rights and the special rapporteur on the right to education (United Nations Human Rights Council 2020). However, the impact of digital education on these features can vary greatly, depending on the context and the policy measures put in place to accompany this process (United Nations Human Rights Council 2022a: 6).

The Covid-19 pandemic also highlighted how increased reliance on digital education, particularly distance learning, can exacerbate pre-existing inequalities. Students often have unequal access to the Internet, adequate hardware and qualified teachers with digital skills, while teachers themselves have varying levels of proficiency in using digital technology (United Nations Human Rights Council 2022a: 11). These disparities underscore the need for careful consideration and regulation of digital education to ensure that it serves all students equitably.

2.7. **RIGHT TO DIGITAL DISCONNECTION**

In the digital age, the right to connect must be balanced with the right to disconnect.

As we navigate the expanding digital universe and the growing recognition of digital rights, we must remember that the analogue world still holds its own essential space. In the digital age, the right to connect must be balanced with the right to disconnect. The rise of digital technologies, remote work and flexible schedules has reshaped the nature of employment, bringing both benefits and new burdens. Chief among these burdens is the expectation of perpetual connectivity, which blurs the boundaries between work and personal life, ultimately affecting mental and physical well-being (Weber and Llave 2021). This blurring of boundaries has sparked a critical conversation about modern labour rights, including the right to unplug and be offline.[13] Efforts to maintain boundaries between offline and online have been undertaken in countries such as France (Republic of France 2016: article 55), where laws protect employees from being contacted outside of agreed-upon hours; Italy (Italian Republic 2017: article 19.1), where the right to disconnect is embedded in labour law; and Germany, where similar protections exist (Vasagar 2013). Additionally, the European Parliament approved a report with recommendations to the European Commission on

13 The right to disconnect refers to a worker's right to be able to disengage from work and refrain from engaging in work-related electronic communications, such as emails or other messages, during non-working hours (Weber and Llave 2021).

Table 2.7. **Right to digital participation and digital inclusion**

Chile [rejected draft] 2022	Chapter II. Fundamental Rights and Guarantees Article 152	1. Citizens have the right to participate in an incident or binding manner in matters of public interest. It is the duty of the State to give adequate publicity to the mechanisms of democracy, tending to favor a broad deliberation of the people, in accordance with this Constitution and the laws. 2. The public authorities shall facilitate the participation of the people in the political, economic, cultural and social life of the country. It will be the duty of each organ of the State to have the mechanisms to promote and ensure the participation and deliberation of citizens in the management of public affairs, including digital media [alt. translation: through digital means]. 3. The law shall regulate the use of digital tools in the implementation of the participation mechanisms established in this Constitution and which are different from suffrage, seeking that their use promotes the highest possible participation in such processes, as well as the widest possible information, transparency, security and accessibility of the process for all persons without distinction.
Canton of Geneva 2013 [substate Constitution]	Title II. Fundamental Rights Article 21A(4)	The Canton promotes digital inclusion and raises awareness of digital issues.

Table 2.8. **Right to digital education**

Chile [rejected draft] 2022	Chapter II. Fundamental Rights and Guarantees Article 90	Everyone has the right to digital education, to the development of knowledge, thought and technological language, as well as to enjoy its benefits. The State shall ensure that everyone can exercise their rights in digital spaces by creating public policies and financing free plans and programmes for this purpose.

an EU-wide right to disconnect, especially in light of the increased remote work during the Covid-19 pandemic (European Parliament 2020).

The Constitutional Convention of Chile tried to introduce such a right in the country's 2022 draft constitution, which was ultimately rejected. The draft article 46(1) created a right to disconnect, stating the following: 'everyone has the right to work and to free choice of employment. The state guarantees decent work and its protection. This includes the right to fair working conditions, to health and safety at work, to rest, to leisure time, to digital disconnection, to guaranteed compensation and to full respect for fundamental rights in the context of work' (Draft Constitution Chile 2022).

While the right to disconnect addresses the work environment, the broader concept of a right to be offline—seeking a balance between the digital and physical worlds—extends beyond the workplace into all aspects of life. Efforts are being made to increase access and improve digital literacy, but some argue that individuals should also have the freedom to disengage from digital tools without penalty or disadvantage (Custers 2022). This freedom particularly applies to those who find it challenging to navigate digital services, such as older adults, for whom online solutions may be cumbersome. Similarly, anyone who prefers offline interactions for personal, cultural or practical reasons should have the option to conduct their affairs without being compelled to go online.

In conclusion, while the digital age has brought unparalleled access to information and connectivity, it also necessitates a re-evaluation of human rights in the context of digital well-being and the freedom and ability to choose to abstain from digital advancements. The right to be offline may be a first step to ensuring that individuals retain the freedom to disconnect and that society values health and well-being alongside technological progress.

While the digital age has brought unparalleled access to information and connectivity, it also necessitates a re-evaluation of human rights in the context of digital well-being and the freedom to choose to abstain from digital advancements.

The list of rights mentioned in this section is not exhaustive. Other new or adapted rights for the digital age found in discussions among scholars and experts include the right to an online identity, encryption, the right to algorithmic transparency and digital consent as well as emerging discussions on net neutrality. The digital rights scholar Jun-e Tan speaks of four spheres of digital rights: (a) conventional rights in digital spaces, which include rights such as the freedoms of expression, association and assembly online and the right to non-discrimination; (b) data-centred rights, such as right to data privacy

and the right to data security; (c) access to digital spaces, which includes rights such as the right to access state and other services online, the right to Internet access and the right to information; and finally (d) governance of the digital, which includes the right to participate in digital governance processes or be consulted on Internet policy issues, the latter of which is not discussed in this report (Tan 2019). This categorization also shows the difficulty of viewing digital rights in isolation, as rights in the digital era have to be approached holistically from various angles.

Chapter 3

ACTORS AND THE HORIZONTAL APPLICATION OF FUNDAMENTAL RIGHTS

Traditionally, constitutions have governed countries' internal organization, roles, powers and structures. They delineate the physical and conceptual boundaries within which the state is legitimized to act, defining the relationship between the state and its citizens. This delineation typically involves specifying citizens' freedoms from state interference, as well as outlining certain rights and duties that the state is obligated to protect and fulfil, respectively. In most societies, the state alone possesses specific powers to govern within a designated territory. By granting citizens fundamental rights and freedoms, the constitution not only outlines the state's powers but also sets limits which the state, including its various bodies and officials, has to respect, protect and uphold. This direct relationship between individuals and the state is known as the vertical application of human or fundamental rights.

By granting citizens fundamental rights and freedoms, the constitution not only outlines the state's powers but also sets limits which the state has to respect, protect and uphold.

The horizontal application of human or fundamental rights, on the other hand, relates to the obligations between private individuals and private entities, meaning that not only the state but also private companies and individuals must adhere to fundamental human rights standards in their interactions (see Frantziou 2020; Gonçalves da Silva and Leitão 2023; Haupt 2024). The horizontal application of human or fundamental rights refers to the idea that these rights should not only protect individuals from violations by the state (vertical application), but also from violations by other private actors, such as corporations, individuals or organizations. Essentially, it means that human rights are not limited to interactions between the government and the people, but also extend to interactions between private entities and individuals.

In practice, horizontal application can imply that individuals can rely on fundamental rights to protect themselves against actions that violate their rights by other private parties, like discrimination in the workplace, abuse by a corporation, or violations by other private entities. This approach has been adopted in several legal systems and can be a more comprehensive way of safeguarding human rights in society.

The reach and implementation of horizontal human rights application can differ widely, influenced by each country's legal traditions and the specific rights at stake. Some legal systems allow for these constitutional rights to be directly or indirectly invoked in private disputes, such as in cases of landlord discrimination or corporate misconduct (Futch 1996).[14] Other countries incorporate such rights through legislation in areas like employment or consumer protection.[15]

Today, the horizontal effect of fundamental rights takes on renewed importance because of the enormous power private actors hold in the Internet's ecosystem. As digital platforms and other technology companies increasingly shape our access to information, free expression and economic opportunities, the question of how human rights apply to these entities has become one of the most pressing challenges of our time.

The growing prominence of non-state actors adds another significant player alongside the state that holds substantial power and influence over the safeguarding of fundamental rights.

3.1. **NEW ACTORS**

In the digital age, the growing prominence of non-state actors, particularly private technology companies, adds another significant player alongside the state that holds substantial power and influence over the safeguarding of fundamental rights at a societal level. This change is in part linked to the evolving nature and meaning of public space since the rise of digitalization. The Covid-19 pandemic further

14 In Germany, the concept of *Drittwirkung*, or the indirect third-party effect of fundamental rights, allows rights enshrined in the German Basic Law to be applied in private-law disputes. This principle has been a significant part of German constitutional law since the landmark *Lüth* case in the Federal Constitutional Court, where it was held that fundamental rights must be considered in private-law contexts. Inspired by the German model, South Africa also recognizes the horizontal application of rights through its Constitution, especially in cases involving discrimination where private parties are involved.

15 The US legal system often addresses the horizontal effects of constitutional rights through various legislative measures, such as employment laws that prevent workplace discrimination and consumer protection laws that safeguard against unfair business practices.

accelerated this shift, as in many places around the world traditional venues such as public squares, parks, shopping centres, cinemas and restaurants were replaced by virtual spaces. Consequently, this transition significantly altered our understanding and interaction with public domains.

As a result, much of the power and responsibility for governing what constitutes the new civic 'public sphere' has moved into the private sector. This shift is not limited to social media platforms; it extends across the entire digital realm, where technology companies wield substantial influence over public discourse, values and the protection of fundamental rights. Indeed, these private corporations can reach a scale and depth of impact that rivals or surpasses certain state functions:

1. **Vertical-versus-horizontal divide**. While constitutions typically constrain the state (vertical application), the new reality demands more attention to horizontal relationships, where private corporations exercise near public power over how people express themselves, assemble online or receive information.

2. **Private corporations as state-like actors**. In domains typically linked with public authority—such as overseeing communication flows—private companies have so much control that they could be seen as state-like actors (Haupt 2024). The question arises: should constitutional safeguards also bind private platforms which effectively govern pivotal aspects of public life?

3. **Old versus new regulatory approaches**. Traditional media gatekeepers faced broadcast licensing requirements, defamation laws and content standards designed for print, radio and television. However, Internet-specific affordances—such as ease of use, massive reach, real-time global dissemination and near-permanent data storage—pose fresh challenges that old regulatory models cannot neatly address.

The problem becomes clear when considering protection of freedom of speech. Historically, traditional media have acted as a gatekeeper of information, governed by editorial standards, journalistic ethics and regulatory oversight. These mechanisms ensure that the information disseminated to the public is curated and verified and that, when misinformation arises, there are clear channels for accountability. Governments have regulated traditional media through broadcast licensing, defamation laws and content standards to

safeguard public interest and minimize harmful content. However, social media platforms operate differently.

Online platforms such as Facebook and YouTube have long imposed their own regulatory frameworks, including rules for moderating online content (see, for example, Facebook n.d. or YouTube n.d.). The number of users of these platforms signifies the scope and magnitude of the influence these companies hold over new virtual public spaces. As of 2024 Facebook had approximately 3 billion monthly active users, making it a critical platform for social interactions and information dissemination (Statista n.d.). About 31 per cent of US adults report regularly getting their news from Facebook. In other parts of the world, particularly in areas with low media literacy, these numbers are even higher. For instance, 61 per cent of people in the Philippines and 48 per cent in Colombia use Facebook for news, while 39 per cent in Thailand and 36 per cent in Kenya use TikTok for news. YouTube is not far behind (Newman et al. 2024). These statistics highlight the fact that the private companies hosting online platforms in these countries have a particularly strong influence on public opinion and people's rights and freedoms. However, the rules these companies impose on users often differ significantly from the constitutional safeguards that public actors must follow (De Gregorio 2022a: 14).

In January 2021, for instance, X (formerly Twitter) banned then-former US President Donald Trump from the platform, following the attack on the US state Capitol on 6 January 2021. Just one month later, Facebook blocked news on its platforms across Australia to protest a proposed law that would have required Facebook (now Meta) and Google to compensate media companies for the news stories featured on their platforms (Gollom 2023).

In countries where media freedom is restricted and controlled by the state, social media serves as a crucial tool for seeking, receiving and sharing information that might otherwise be inaccessible.

Since the information on online platforms plays a major role in people's news consumption, as seen above, thus shaping public opinion, platforms themselves are increasingly assuming roles traditionally held by both media outlets and government authorities, positioning them as key players in managing public information—but without the same level of oversight or accountability.

Nevertheless, it is important to note that, particularly in countries where media freedom is restricted and controlled by the state, social media serves as a crucial tool for seeking, receiving and sharing information that might otherwise be inaccessible.

Furthermore, the influence of private actors on public life is particularly evident when social media algorithms preferentially amplify certain political messages. Studies show that algorithms often amplify content that is emotionally charged or politically extreme, especially through mechanisms designed to boost user engagement (Brady et al. 2023). One such study, focusing on Twitter, found that right-leaning content and political messages are more likely to be amplified than left-leaning content in multiple countries, including the USA and the UK (Huszár et al. 2021). Another significant instance was the manipulation of misinformation about public health during the Covid-19 pandemic. Platforms like Facebook were used to spread false information about vaccines and treatments, impacting public health responses and vaccination rates globally (World Health Organization 2022). Such events highlight the pervasive reach of private enterprises into critical areas of public interest and welfare.

While the extensive influence of private companies on public discourse, and essentially on the exercise of certain rights, is a broad issue that is also pertinent to traditional mass media, the scope and nature of digital platforms introduce unique complexities. Unlike traditional media, online platforms combine unparalleled reach and speed in disseminating information with new technological capabilities that enable them to micro-target audiences by using vast amounts of personal data. Social media can disseminate information instantly across global networks, target individuals with extreme precision using data analytics and continuously adapt content delivery using sophisticated algorithms. These capabilities create an exceptionally dynamic and pervasive form of influence that can impact millions of viewers quickly and shape societal beliefs on a scale and with a level of specificity that traditional media could never achieve (International IDEA 2018, 2020).

Ultimately, this transfer of power from public to private actors—while offering benefits such as broader participation—raises the question of applying fundamental rights horizontally. In particular, if these corporations are akin to state-like entities in function but not in accountability, how can constitutional or international human rights standards adapt to ensure the protection of individual freedoms in these new digital realms?

The transfer of power from public to private actors—while offering benefits such as broader participation—raises the question of applying fundamental rights horizontally.

3.2. **PUBLIC–PRIVATE PARTNERSHIP**

In the digital age, the lines between the public and private sectors are becoming increasingly blurred, with private enterprises playing pivotal roles in shaping the delivery of essential services. From healthcare to education, public–private partnerships are transforming how societies operate, often introducing technological innovations that improve lives in unprecedented ways. As these partnerships deepen, however, they raise pressing questions about control, data privacy and the balance of power. What happens when the same corporations facilitating humanitarian aid or running city infrastructure also hold vast amounts of sensitive data? The following examples explore the powerful, and at times problematic, dynamics of these partnerships, showcasing both the promise of digital innovation and the ethical challenges it presents in maintaining democratic oversight and protecting fundamental rights.

Public–private partnerships are at the forefront of transformative change across the globe, blending innovation with societal needs in ways that redefine how governments deliver essential services. In India, telecom providers are bridging the gap between rural communities and healthcare, enabling remote consultations and access to medications through digital dispensaries—an initiative that is already making a tangible difference in the state of Madhya Pradesh (Buckup 2023). Similarly, in Mumbai, digital platforms are being leveraged to improve maternal and child health services, demonstrating the power of technology to reach underserved populations (Buckup 2023).

On a broader scale, the use of mobile technology in humanitarian efforts has become indispensable. The World Health Organization's partnership with WhatsApp to disseminate Covid-19 information globally illustrates how private sector tools can play a crucial role in public health emergencies (Taylor 2021). These kinds of collaboration extend beyond healthcare, as seen in Rwanda, where partnerships with companies like Mastercard are driving a shift towards a cashless economy, creating opportunities for financial inclusion and economic growth (Buckup 2023).

Beyond healthcare and economic development, partnerships with the private sector are also protecting cultural heritage. In an innovative response to climate threats, the island nation of Tuvalu plans to preserve its cultural identity through the Metaverse, which is providing a digital space where citizens can maintain connections

to their homeland, even if their physical territory is lost (Craymer 2022). Meanwhile, on the battlefield, Ukraine has shown how quickly adaptable commercial technologies—ranging from satellites to machine learning—can provide a strategic edge, illustrating how digital tools extend into national security and defence (Breaugh et al. 2023).

These examples vividly illustrate how public–private collaborations are not just reshaping public services but also redefining governance itself. From improving healthcare and driving economic modernization to preserving cultural heritage and strengthening military capabilities, these partnerships are playing an increasingly vital role in addressing both present challenges and future uncertainties. As a result, such collaborations have become integral to the governance frameworks of many countries. Simultaneously, however, they are also elevating the global technology sector's political influence and shaping how governments approach public service delivery (Taylor 2021).

Public–private collaborations are not just reshaping public services but also redefining governance itself.

Not all public–private collaborations are benign. In certain cases, the state can use private partnerships to evade the legal or constitutional checks that would apply if it were acting alone. Such partnerships can become avenues for illegal surveillance, data exploitation or censorship—coordinated quietly or under the guise of formal agreements. This problem has been documented in multiple contexts.

Digital surveillance is a prominent example, where the use of such technologies can infringe on privacy. In Jordan, for example, investigations by Access Now and Citizen Lab revealed that Pegasus spyware—developed by the Israeli company NSO Group—was used to target Jordanian civil society figures, including journalists, lawyers and human rights activists. Deployed ostensibly for national security purposes, the spyware enabled extensive monitoring of private communications and personal data (Access Now 2024; The Citizen Lab 2024).

Some governments encourage—or coerce—private social media or telecom companies to implement censorship policies. For instance, the Great Firewall in China relies heavily on corporate compliance and technical expertise supplied by private firms (Freedom House 2024).

Some governments encourage—or coerce—private social media or telecom companies to implement censorship policies.

While these efforts may be framed as 'protecting national security' or 'preserving social harmony', they can involve clandestine content

filtering and account takedowns that violate freedom of expression (Funk, Vesteinsson and Baker 2024; Human Rights Watch 2006a).

In one example, Yahoo faced criticism in the mid-2000s for providing user information to Chinese authorities, leading to the imprisonment of dissidents (Human Rights Watch 2006a, 2006b).

Even in liberal democracies, law enforcement or intelligence services may obtain personal data through partnerships with corporations instead of using formal search warrants or legislative processes. A prominent example is the Amazon Ring partnership with US police departments, which has raised concerns about warrantless access to residents' video footage (Guariglia 2019; Molla 2019).

Another notable case of unauthorized data collection occurred in 2019, when the UK Government partnered with Amazon to provide health advice via voice assistants, which granted Amazon access to National Health Service (NHS) data. This data was monetized without compensation being paid to the NHS (Chan 2019). Similarly, Google's Sidewalk Labs collaborated with city governments, using data collected from public transport to boost its market presence and benefit partners like Uber (Taylor 2021).

Beyond concerns about dependency and monopolies (Foley and Swilling 2018: 82), the widespread reliance on proprietary digital technologies for government services has raised serious questions about the protection of constitutionally guaranteed rights. These 'workarounds' allow countries to collect, analyse or censor content in ways they could not achieve through public channels alone, eroding constitutional safeguards around privacy, due process or freedom of speech.

It is important to recognize that the ongoing trend of private enterprises expanding into the public domain and influencing our social and political life is being vastly accelerated in the digital age.

A global investigation by Human Rights Watch into education technologies endorsed by 49 countries during the pandemic revealed even more troubling practices. Many of these platforms violated children's privacy, secretly collecting data on their activities, locations and personal networks, which was then shared with advertising technology companies (Human Rights Watch 2022). These examples illustrate how corporate involvement in public services often results in the exploitation of sensitive data, posing significant risks to individual rights.

As a result, it is also important to recognize that the ongoing trend of private enterprises progressively expanding into the public domain and significantly influencing our wider social and political life is being

vastly accelerated in the digital age. However, business ethics and private law are not traditionally designed to address questions of fundamental rights compliance and democracy, offering minimal protection in the face of this new distribution of power.

3.3. APPLYING RIGHTS HORIZONTALLY AS A WAY FORWARD

The legal mechanisms that safeguard rights and public powers in most legal systems—namely national constitutions—have not been applied to the private sector thus far. However, the private sector's accumulation of control over services and public functions necessitates a paradigm shift: from perceiving state actors as the sole threats to rights and freedoms, to recognizing that private companies, especially online platforms, can pose equally significant challenges to the protection of human rights.

These challenges were already recognized a decade ago by the architect of the United Nations Guiding Principles on Business and Human Rights, who found that 'the root cause of the business and human rights predicament today lies in the governance gaps created by globalization—between the scope and impact of economic forces and actors, and the capacity of societies to manage their adverse consequences' (Office of the United Nations High Commissioner for Human Rights 2020: 1). In response, international efforts are trying to address the growing influence of private companies over public life through initiatives such as the UN's B-Tech Project, which works directly with online platforms to ensure their operations align with human rights standards. Building on the UN Guiding Principles on Business and Human Rights and advocating for rights-based public policy and legal measures 'to govern how new technologies are developed, deployed and used' (Office of the United Nations High Commissioner for Human Rights 2020: 1), the B-Tech Project aims to promote human rights due diligence, urging companies to identify, prevent and mitigate any adverse human rights impacts in their activities (Office of the United Nations High Commissioner for Human Rights 2020).

International efforts are trying to address the growing influence of private companies over public life.

Beyond the Guiding Principles and the B-Tech Project, several other international initiatives aim to ensure that tech companies respect human rights. For example, the Global Network Initiative brings together major tech companies, civil society and academics to advance freedom of expression and privacy in the ICT sector,

although its commitments remain voluntary. Similarly, the Organisation for Economic Co-operation and Development Guidelines for Multinational Enterprises recommend responsible business conduct, including respect for human rights, but these guidelines are non-binding. A significant recent development is the adoption of the Global Digital Compact (GDC) at the UN Summit of the Future in September 2024. Serving as the first comprehensive global framework for digital cooperation, the GDC aims to anchor digital governance in human rights and international law. It addresses key issues such as universal Internet connectivity, data protection, digital trust and AI governance, while also promoting efforts to combat disinformation, hate speech and the digital gender divide. Although not legally binding, the GDC provides a road map for ensuring that digital technologies are developed and governed responsibly, emphasizing multilateral cooperation.

However, a fundamental criticism of the UN Guiding Principles and similar voluntary approaches is that they lack enforceability. While this strategy makes sense from a realist perspective—given the UN's limited power to impose binding treaties on transnational corporations—it comes at a cost. In effect, it dilutes the legal essence of human rights, reducing them to aspirational standards that corporations can decide to follow or ignore. The lack of binding power opens the door to symbolic compliance, wherein companies adopt human rights rhetoric but fail to implement meaningful reforms. Ultimately, voluntary frameworks risk developing processes and structures that do not produce real change.

Therefore, on the legally binding side, the EU has enacted regulations such as the General Data Protection Regulation, which has had a significant impact on tech companies globally by enforcing strict rules around data protection and privacy, with penalties for non-compliance. The EU's Digital Services Act further mandates large platforms to mitigate risks to fundamental rights like freedom of expression, placing enforceable obligations on tech companies.

These efforts illustrate the widely accepted scholarly view (see e.g. Alexy 2002) first discussed in the famous judgement of the German constitutional court that 'constitutional rights are not just defensive rights of the individual against the state, but embody an objective order of values, which applies to all areas of the law ... and which provides guidelines and impetus for the legislature, administration and judiciary' (Federal Constitutional Court (Bundesverfassungsgericht) judgement of 15 January 1958 – 1 BvR 400/51 paragraph 25). Nevertheless, in light of these challenges to

the protection of rights and freedoms as outlined in the previous section, there is also a growing demand to extend constitutional protections to cover the quasi-public functions performed by private entities, beyond merely addressing the influence of private entities through regulation. This growing concern has sparked discussions on rethinking and remodelling constitutional instruments that protect rights and prevent abuses. Among the solutions proposed by practitioners and scholars is the application of constitutional norms to private entities that perform public functions or wield significant influence over public discourse and rights (De Gregorio 2022a; Haupt 2024).

In light of these discussions, to ensure that constitutional rights are not circumvented merely because an actor is private, particularly when private entities undertake roles functionally equivalent to governmental activities, many scholars have argued that they should bear similar constitutional obligations, arguing for a constitutional interpretation of horizontality that goes beyond traditional doctrines like direct effect. This approach suggests that fundamental rights should be viewed as enabling conditions for participation in public life, thus requiring a more substantive form of equality beyond 'state-versus-individual paradigms' (Frantziou 2020).

Some legal systems have expanded the protection of fundamental rights to encompass private entities, through what is known as the horizontal application of fundamental rights. This legal principle, which was originally developed in the 1950s by the German Constitutional Court, has since been adopted in various constitutional jurisdictions, including by the Court of Justice of the European Union and the European Court of Human Rights (Stein 2022).[16] This approach enables individuals to invoke constitutional rights in litigation against other private parties, alleging violation of

16 The famous *Lüth* judgment (1958) of the German Federal Constitutional Court (Bundesverfassungsgericht) developed the horizontal application of fundamental rights in Germany (enforced as between private citizens rather than vertically as against the state). BVerfG, Urteil des Ersten Senats vom 15. Januar 1958 – 1 BvR 400/51 –, Rn. 1-75, <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1958/01/rs19580115_1bvr040051.html>, accessed 6 May 2025 (in German). For summary and analysis of the case in English see Stein, S. K., 'Lüth and Elfes – a German approach to a horizontal effect of fundamental rights', IACL-AIDC BLOG, 14 June 2022, Blog, <https://blog-iacl-aidc.org/new-blog-3/2022/6/14/lth-and-elfes-a-german-approach-to-a-horizontal-effect-of-fundamental-rights>, accessed 6 May 2025. The European Court of Justice also confirmed the horizontal application of human rights in the *Egenberger und Bauer* case. Case C-414/16 Egenberger EU:C:2018:257, paras 76–77 Joined cases C-569/16 and C-570/16 Bauer EU:C:2018:871, para 89, <https://www.maastrichtuniversity.nl/file/novadigitalisationpolicybrieffinaldocxpdf>, Case C-68/17 *IR v JQ*, ECLI:EU:C:2018:696., Joined Cases C-569/16 and C-570/16 *Stadt Wuppertal v Maria Elisabeth Bauer* and *Volker Willmeroth v Martina Broßonn*, ECLI:EU:C:2018:871, Case C-684/16 *Max-Planck-Gesellschaft zur Förderung der Wissenschaften eV v Tetsuji Shimizu*, ECLI:EU:C:2018:874.

Some legal systems have expanded the protection of fundamental rights to encompass private entities.

those rights. Although there is an ongoing debate about whether horizontality should be treated as a structural constitutional principle[17] or as an extension of the direct effect doctrine[18] (Frantziou 2020), the academic discourse has extensively explored the idea of mandating private entities to uphold fundamental rights, thereby also constraining their autonomous activities based on constitutional protections, especially in areas such as freedom of expression, privacy and data protection. Many practitioners and scholars view the horizontal application of human rights as a potential solution to the challenge of rights protection in the digital era (Pollicino 2021).

The *Google Spain*[19] ruling, for example, introduces a novel method for protecting fundamental rights in the digital age. It is a notable case to discuss for two reasons: firstly, it introduced discussions on the right to be forgotten; secondly, it is a landmark decision regarding the horizontal application of fundamental rights and digital rights jurisprudence. In its ruling, the Court relied on article 7 (respect for private and family life) and article 8 (protection of personal data) of the EU Charter of Fundamental Rights and applied the constitutional mechanisms of fundamental rights protection between private parties. In its ruling, the Court required private entities, like search engine operators, to balance the right to information with data protection rights, and underlined the critical role of human dignity in achieving this balance (Pollicino 2021).

In this case specifically, the claimant, Mario Costeja González, sued Google Spain for displaying search results that linked to his outdated financial hardships, which he wanted removed. The Court was asked to determine whether Google, as a search engine operator, had to comply with an individual's request to remove links to personal information in search results even when the information itself was lawfully published on web pages.

The relevant legal frameworks were EU Directive 95/46/EC, which regulates the processing of personal data within the EU, and article 8 of the EU Charter of Fundamental Rights, which specifically

17 Treating horizontality as a structural constitutional principle means that the constitution inherently applies to all legal relationships within the society in question, including those between private parties. In this view, constitutional norms have a foundational role and automatically inform the interpretation and application of all laws and legal relationships.

18 Applying this doctrine to constitutional rights suggests that specific constitutional provisions can have direct applicability in disputes between private parties if the provisions are sufficiently clear, precise and unconditional.

19 Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González* [2014] ECLI:EU:C:2014:317.

protects the right to personal data protection. These rules state that individuals have the right to control the processing of their personal data, including having inaccurate data corrected and certain data erased to protect their privacy.

The European Court of Justice considered whether the directive applies to search engine operators like Google and whether they are responsible for personal data appearing in their search results. The Court found that, by indexing and storing personal data, Google acts as a data controller under the directive and thus has specific obligations, including the removal of links to personal data that infringe on privacy rights when requested by the individual concerned unless there is a stronger public interest in keeping the information accessible.

Furthermore, under article 8 of the EU Charter, any interference with the right to data protection must be justified and proportionate. The Court balanced this right against the economic interest of the search engine and the public interest in accessing the indexed information. It concluded that individual rights generally override other interests, particularly when the data is outdated or irrelevant. Article 8 of the EU Charter in particular asserts that personal data must not be excessively processed relative to the purpose for which it was originally collected, highlighting the need for data relevance and the avoidance of excessive data retention. The Court, therefore, held that the rights to privacy and data protection typically surpass both the economic interests of search engines and the public's interest in accessing outdated or irrelevant information unless it remains significant for public interest purposes.

Discussions surrounding the right to be forgotten, as established through the *Google Spain* case, have also been influential beyond Europe. For instance, the Federal Institute of Access to Information and Protection of Data, an administrative body in Mexico, drew on the *Google Spain* ruling, mandating Google to remove specific URLs that disclosed personal information from the indexing of Google Mexico's search engine and to erase personal data linked to an individual.

In contrast to Mexico's adoption of the right to be forgotten, however, other jurisdictions have taken a different stance. In a contrasting decision by the First Instance Court in São Paulo, Brazil, the Court dismissed the plaintiff's right to privacy in favour of freedom of expression and the public's right to information. Specifically, the Court faced a request from a Brazilian citizen seeking to compel

Google to delete search results connected to articles about his past unlawful activities. This individual had been arrested six years prior, and the Court rejected his request based on the right to freedom of expression, as enshrined in article 220 §1 of the Brazilian Constitution. The Court reasoned that the criminal proceedings were a matter of public record, and that there was no justification for suppressing the articles, emphasizing the constitutional safeguard of free expression (Columbia University Global Freedom of Expression n.d.d).

Similarly, the Supreme Court of Argentina took a restrictive view of the right to be forgotten in *Natalia Denegri v Google Inc*.[20] Denegri, a well-known television presenter, sought the removal (or de-indexation) of videos on Google relating to her past involvement in televised scandals from the 1990s. She argued that this content, although accurate, had become irrelevant and infringed upon her privacy, honour and reputation. While a lower court initially accepted her request in part, the Supreme Court unanimously overturned that ruling. The Court emphasized that any curb on the free flow of information—such as de-indexation—constitutes a serious restraint on freedom of expression and must therefore undergo strict scrutiny. In Denegri's case, the mere passage of time did not render the past events irrelevant; the Court reasoned that she was a public figure and that restricting access to accurate public-interest information would undermine the very purpose of freedom of expression. The Court also cautioned that judges should avoid imposing standards based on subjective tastes or sensibilities, lest they open the door to undue arbitrariness.

Meanwhile, the Supreme Court of Chile dismissed a petitioner's plea to remove online media articles detailing his criminal actions, citing the public's right to information (Columbia University Global Freedom of Expression n.d.f).

These contrasting cases illustrate the challenges courts face in applying constitutional rights horizontally, particularly in the context of digital platforms. While the *Google Spain* ruling imposes obligations on private entities to protect individual rights, other courts emphasize platforms' role in upholding societal interests like freedom of expression and access to information. Both approaches have their justifications. In Mexico, for example, NGOs have criticized the right to be forgotten, particularly in contexts where politicians use this tool

20 *Denegri, Natalia Ruth v Google Inc. on Personal Rights: Related Actions* [2022] Supreme Court of Justice of the Nation CIV 50016/2016/CS1.

to erase records of their political scandals (La Red en Defensa de los Derechos Digitales n.d.). The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights has expressed concerns about the right to be forgotten, stating that applying a private system for the removal and de-indexing of online content with vague and ambiguous limits is problematic in the Americas. They emphasize that such practices could conflict with article 13 of the ACHR, which provides broad protection for freedom of expression. The rapporteur further asserts that removing content from the Internet constitutes a clear interference with freedom of expression and the public's right to access information. The concern is that the right to be forgotten could be used to suppress lawful content that is of public interest, especially information about public figures or matters affecting society (Lanza 2017).

Despite the varied judicial approaches and the complexities involved in balancing competing rights when applying rights constitutionally, all these cases have dealt with the role of platforms and fundamental rights compliance through constitutional frameworks. This commonality highlights that courts across different jurisdictions recognize the significance of constitutional principles when adjudicating matters involving private entities that have substantial influence over any fundamental rights.

In conclusion, the evolving dynamics between state and private entities in the digital domain have led many experts to call for a re-evaluation of traditional constitutional protections to address the complexities of the digital age. The horizontal application of fundamental rights, exemplified by legal developments like the *Google Spain* ruling, would represent a critical step towards ensuring that private entities wielding significant influence over public discourse, personal freedoms and rights are held to constitutional standards.

Applying fundamental rights horizontally would limit some of the powers of tech corporations to curb abuses by both state and non-state actors. It promises protection of fundamental rights amid the growing convergence of public and private spheres, thereby ensuring the digital age advances with respect to human rights and the rule of law at its core.

Applying fundamental rights horizontally would limit some of the powers of tech corporations to curb abuses by both state and non-state actors.

Ultimately, as digital technologies continue to reshape political and societal interactions, legal frameworks must evolve to address these new challenges. This evolution should include not only expanding

rights protections but also—as seen in the case law throughout this report—carefully balancing these protections against the need for economic vitality and technological progress. The ongoing discourse and legal refinements will likely continue to shape the boundaries and applications of fundamental rights in this new era.

This discussion also shows how crucial the judiciary is to safeguarding fundamental rights in this digital age, as a means of interpreting legal protections for fundamental rights, and to the evolving nature of potential threats in the digital space. Judges are charged with the challenging task of weighing the benefits of technological advances against the need to preserve fundamental freedoms like privacy, free speech and civic participation. It is a balancing act that is as complex as it is crucial.

Judicial oversight is essential to preventing rights violations such as unlawful Internet shutdowns, which can suppress free expression and limit access to information, and to countering excessive surveillance and searches that threaten privacy rights. While many fundamental rights are subject to restrictions, such limitations must be legally justified to ensure that they are necessary and proportionate. By enforcing legal protocols and upholding the rule of law, courts act as critical checks on both governmental and private powers. This judicial oversight is essential to safeguarding individual liberties and preventing the erosion of rights, particularly in an era marked by rapid technological advances.

In this context, however, a potential imperfection in both the DSA's systematic risk approach and the *Google Spain* ruling should be noted when inching closer to a notion of horizontal rights. The DSA, for example, treats fundamental rights as merely one category of risk to be assessed by large platforms, effectively relegating rights to a secondary focus. Moreover, it relies on corporate-led mitigation strategies that are often devised internally and scrutinized only ex post facto.

Similar debates arise around the *Google Spain* decision. While it arguably represents a form of horizontality by requiring search engines to balance individual privacy and data protection rights against the public's right to information, its success was largely due to its anchoring in existing data protection law explicitly applicable to private entities handling personal data. In other jurisdictions—particularly those that have rejected the right to be forgotten—courts have viewed the invocation of data protection statutes to regulate

search engine operations as tenuous or insufficiently grounded, leading to inconclusive balancing outcomes. These approaches highlight partial strategies that address the broader absence of a clear-cut constitutional principle of horizontality in the digital realm.

Having said that, critics often raise concerns about the freedom of enterprise and the risk of over-regulation stifling innovation, particularly when applying fundamental rights horizontally. They argue that imposing constitutional standards on private companies could create an unwieldy burden that hinders technological advancement and economic growth (Henshall 2023; Sayeedi 2023). Further arguments have been raised that such applications may lead to 'rights inflation' and excessive judicialization, which can create legal uncertainty and impact private autonomy (Craig 2009: 349; Frantziou 2020: 212). This concern arises from fears that expanding fundamental rights into private relationships could compel judges to exceed their traditional interpretive roles, risking not only arbitrary but also illegitimate and potentially unconstitutional law making (Frantziou 2020; Shrivastava 2023). In India, for example, the Supreme Court's decision in *Kaushal Kishor v State of Uttar Pradesh*[21] affirmed that fundamental rights under articles 19 (freedom of speech) and 21 (right to life and personal liberty) can be enforced against private entities. Although this ruling has in great part been seen as a progressive step in broadening the scope of fundamental rights, it has also sparked debate about the implications for private law and the balance of powers between the judiciary and the legislative and executive branches of government (Bilchitz and Deva 2023; Shrivastava 2023).

That said, it is not necessarily obvious that the enforcement of rights against private entities must mirror enforcement against the state. A distinct jurisprudence of horizontality could be developed to address these issues, allowing courts to adapt their approaches in a way that recognizes the unique dynamics of private relationships. Such an approach could strike a balance between ensuring that fundamental rights are respected and avoiding the overreach of judicial power. Moreover, the criticism of judicial overreach is not exclusive to the horizontal application of rights; similar criticisms can arise when courts intervene in state actions. In such cases, jurisprudence of self-restraint or dialogical remedies—where courts engage in ongoing dialogue with other branches of government rather than imposing

21 Supreme Court of India, 'Kaushal Kishore v. State of Uttar Pradesh and Others', Writ Petition (Crl.) No. 113 of 2016, <https://www.casemine.com/judgement/in/5de2ff9146571b63ad4ebf6b>, accessed 23 March 2025.

rigid solutions—has been proposed as a means to mitigate concerns about judicial activism and preserve institutional balance.

While the judiciary serves as a crucial sentinel in interpreting and enforcing fundamental rights in the digital age, it is essential to recognize that judges are only one piece of the larger puzzle of rights protection. Safeguarding liberties in the digital realm cannot be achieved by the judiciary alone; it requires the coordinated efforts of proactive legislation, robust regulatory frameworks, and the active engagement of civil society and private entities. Navigating the complex maze of challenges posed by rapid technological advancements demands a multifaceted approach.

By continually adapting and reimagining legal protections to keep pace with new digital realities, judges play a pivotal role in fortifying individual liberties.

Despite limitations and the criticisms levelled against the judiciary, its role remains irreplaceable. By continually adapting and reimagining legal protections to keep pace with new digital realities, judges play a pivotal role in fortifying individual liberties. This ongoing judicial engagement not only ensures that fundamental rights are upheld but also fosters an environment where innovation and economic growth can flourish alongside a steadfast respect for fundamental freedoms.

Chapter 4

CONCLUSION: LOOKING TO THE FUTURE

This report explored the complex interplay between rising digitalization and fundamental rights, showing that, as digital technologies rapidly evolve, a mix of challenges and opportunities emerge that directly impact our civil liberties and human rights.

As this report has outlined, fundamental rights, enshrined in national constitutions, regional instruments and international human rights law, are affected in the digital space. Thus, it is crucial to ensure that human rights apply online as well as offline. Essentially, protecting rights in the digital, online space also impacts the exercise of rights in the analogue sphere.

Furthermore, the swift evolution of technologies demands a constitutional legal framework that can respond to new challenges and developments to ensure that protections against potential abuses are both effective and relevant.

Responsiveness alone is not sufficient. As outlined in the numerous examples provided in this report, technological advancements occur at a rapid pace, continually introducing new challenges to rights protection which call for our legal and constitutional frameworks to be not only responsive but also agile, equipped to adapt to future technological innovations that are currently unpredictable. This flexibility is vital for courts, as they interpret laws within contexts that are constantly being reshaped by both technological progress and evolving societal norms. Such agility ensures that our legal system remains effective and relevant in the face of continuous digital transformation.

As digital technologies rapidly evolve, a mix of challenges and opportunities emerge that directly impact our civil liberties and human rights.

Courts are increasingly required to apply established constitutional principles in ways that account for the nuances of digital technologies.

As demonstrated in the case law presented, given the complexities surrounding fundamental rights, such as the right to digital privacy and data protection, courts are increasingly required to apply established constitutional principles in ways that account for the nuances of digital technologies. This approach involves not only reactive measures to address immediate threats but also proactive interpretation of existing constitutional provisions to protect human rights in the digital age.

Additionally, effective constitutional legal responses to the challenges posed by digital technologies must be comprehensive to cover the broad spectrum of rights that could potentially be impacted by technological advancements. The EU, for example, has pioneered a suite of robust legislation that addresses the varied societal impacts of digital technologies. The EU General Data Protection Regulation has not only set a global benchmark for data privacy but also serves as a regulatory framework for ensuring that personal data is processed transparently and securely, enhancing consumer trust. Similarly, the Digital Services Act and the Digital Markets Act are designed to ensure that digital platforms operate fairly and transparently, promoting competition and preventing the undue influence of tech giants.

Moreover, the EU's Artificial Intelligence Act represents the world's first forward-looking measure to mitigate the ethical risks posed by AI technologies, including potential rights violations, setting standards for development and usage that prioritize human oversight and transparency. The EU directive on targeted political advertising further aims to safeguard the democratic process by ensuring that political advertising is clearly distinguished from other content, thus helping to prevent covert manipulation of public opinion.

Nonetheless, the EU is not the only player in this space. Brazil has been at the forefront with its pioneering Civil Rights Framework for the Internet, a groundbreaking legal framework that enshrines Internet users' rights and sets the foundation for Internet governance. Similarly, Canada has taken significant steps by adopting its Digital Charter, aimed at ensuring that Canadians have access to a safe, secure and trustworthy digital environment. These initiatives signal a broader global movement towards new legislation, with many countries expected to introduce constitutional reforms and legal frameworks to address the challenges of the digital age.

Such legislative efforts are increasingly focused on several critical areas: protecting citizens from digital surveillance, enhancing the accountability of online platforms, creating robust safeguards for the deployment and use of AI, and refining data protection regimes to better serve the needs of the public. It is important that this happens in a way that places human rights at the centre of regulatory frameworks and legislation on digital technologies, providing greater guidance on human rights standards and addressing protection gaps created by evolving digital technologies.

As technology continues to advance, it is crucial that the constitutional protection of rights evolves concurrently to ensure that our highest laws are equipped to handle the complexities of the digital age, while upholding the fundamental rights and freedoms that form the bedrock of democratic societies. Leveraging the benefits of technological advancements while vigilantly guarding against their risks can ensure that the digital future is shaped by the values of human dignity and the rule of law.

As technology continues to advance, it is crucial that the constitutional protection of rights evolves concurrently.

GLOSSARY

Advanced algorithms
Advanced algorithms are sophisticated sets of rules and calculations designed to solve complex problems or perform specific tasks. These algorithms are often used in fields like data analysis, artificial intelligence and machine learning. They can process large amounts of data, recognize patterns, make predictions, and optimize processes with high efficiency and accuracy.

Artificial intelligence
Artificial intelligence (AI) is a broad term encompassing various concepts and technologies, making it difficult to define universally. In fact, many academic papers on the subject begin by acknowledging the lack of a single agreed-upon definition. Generally, AI can be described as 'the study of systems that perceive their environment and determine a course of action to maximize the likelihood of achieving a specific goal' (World Wide Web Foundation 2017).

In the context of this report, AI refers to the field of computer science dedicated to creating systems and machines capable of performing tasks that typically require human intelligence. These tasks include learning, reasoning, problem solving, perception, natural language processing and decision making, ranging from simple rule-based models to advanced models based on machine learning and neural networks.

Automation
Automation refers to the use of technology to perform tasks without human intervention. These tasks can include anything from simple repetitive tasks to complex processes involving decision making and problem solving. Automation is commonly employed in industries

such as manufacturing, software development, finance and logistics to increase efficiency, reduce costs and minimize human error.

Big data
Big data refers to extremely large data sets that are difficult to process and analyse using traditional data-processing techniques. Big data is characterized by its volume, velocity (speed of generation), variety (different types of data) and veracity (uncertainty of data). It is used in various fields to uncover patterns, trends and associations, particularly in relation to human behaviour and interactions.

E-governance and e-government
E-governance and e-government refer to the use of digital technologies, particularly the Internet, to deliver government services, engage with citizens and facilitate the operation of government functions. E-governance encompasses a broader scope, including interactions between government, citizens, businesses and other arms of government. E-government specifically focuses on the digital delivery of government services to the public, such as online tax filing, licence renewals and access to public records.

Information and communication technology
Information and communication technology (ICT) encompasses technologies that provide access to information and facilitate communication. ICT encompasses a wide range of digital tools, devices and systems, including computers, mobile phones, the Internet, telecommunications networks and software applications. ICT is integral to modern business operations, education, government and everyday life.

Internet of things
The Internet of Things (IoT) refers to the network of physical objects—often called smart devices—that are embedded with sensors, software and other technologies to connect and exchange data with other devices and systems over the Internet. The IoT enables automation, remote monitoring and control of these objects, ranging from home appliances to industrial machinery, leading to more efficient and intelligent systems.

Machine learning
Machine learning involves a shift from traditional programming, where computers are given explicit step-by-step instructions to solve a problem. Instead, in machine learning, a human programmer provides the computer with guidelines and rules for learning from

the data it receives. The computer then analyses the data, makes inferences and generates new rules, enabling it to deliver information and services autonomously (Internet Society 2017).

Online content moderation
Online content moderation involves the monitoring, reviewing and management of user-generated content on digital platforms, such as social media, forums and websites. The goal is to enforce community guidelines, remove harmful or inappropriate content, and ensure that online spaces are safe and respectful. Content moderation can be performed manually by humans or through automated tools using AI and machine learning.

Spyware
Spyware is a type of malicious software designed to secretly monitor and collect information from a user's device without their knowledge. It can capture sensitive data such as passwords, credit card numbers and personal communications and transmit it to third parties. Spyware is often used for illegal activities, such as identity theft, corporate espionage or unauthorized surveillance.

References

7amleh, '7amleh Center Releases Policy Paper "Facebook and Palestinians: Biased or Neutral Content Moderation Policies"', 29 October 2018, <https://7amleh.org/2018/10/29/7amleh-releases-policy-paper-facebook-and-palestinians-biased-or-neutral-content-moderation-policies>, accessed 6 May 2024

Access Now, 'New Middle East and North Africa Coalition to Combat Digital Surveillance', last updated 26 January 2023a, <https://www.accessnow.org/press-release/new-middle-east-and-north-africa-coalition-to-combat-digital-surveillance>, accessed 6 May 2024

—, 'Sheikh Jarrah: Facebook and Twitter systematically silencing protests, deleting evidence', last updated 26 January 2023b, <https://www.accessnow.org/press-release/sheikh-jarrah-facebook-and-twitter-systematically-silencing-protests-deleting-evidence>, accessed 6 May 2024

—, 'Weapons of control, shields of impunity: Internet shutdowns in 2022', last updated 24 May 2023c, <https://www.accessnow.org/Internet-shutdowns-2022>, accessed 6 May 2025

—, 'Between a Hack and a Hard Place: How Pegasus Spyware Crushes Civic Space in Jordan', 1 February 2024, <https://www.accessnow.org/publication/between-a-hack-and-a-hard-place-how-pegasus-spyware-crushes-civic-space-in-jordan>, accessed 4 October 2024

Advertising TV, 'Whopper neutrality | Burger King', YouTube, 12 February 2018, <https://www.youtube.com/watch?v=erSgUag9F_4>, accessed 24 October 2024

African Declaration on Internet Rights and Freedoms Coalition, 'African Declaration on Internet Rights and Freedoms', 2014, <https://africanInternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf>, accessed 6 May 2024

Alexy, R., *A Theory of Constitutional Rights* (Oxford: Oxford University Press, 2002)

Allegri, M. R., 'The right to be forgotten in the digital age', in F. Comunello, F. Martire and L. Sabetta (eds), *What People Leave Behind* (Cham, Switzerland: Springer, 2022), pp. 237–51, <https://doi.org/10.1007/978-3-031-11756-5_15>

Alliance for Universal Digital Rights (AUDRi), *Securing Our Human Rights in Our Digital World* (Alliance for Universal Digital Rights, 2022), <https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/230203_Alliance_for_Universal_Digital_Rights.pdf>, accessed 6 May 2024

Amelin, R., Channov, S. and Milusheva, T., 'The right to freedom of speech: Evolution in the digital age', in I. Savchenko (ed.), *Freedom and Responsibility in Pivotal Times* (London: European Proceedings, 2022), <https://doi.org/10.15405/epsbs.2022.03.6>

Amnesty International, '7 ways the world has changed thanks to Edward Snowden', 4 June 2015, <https://www.amnesty.org/en/latest/campaigns/2015/06/7-ways-the-world-has-changed-thanks-to-edward-snowden>, accessed 18 March 2025

—, 'Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally', 19 July 2021, <https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project>, accessed 6 May 2024

—, *Amnesty International Annual Report 2022/23: The State of the World's Human Rights* (London: Amnesty International, 2023), <https://www.amnesty.org/en/latest/news/2023/03/international-system-unfit-to-deal-with-global-crises-annual-report-2022>, accessed 6 May 2024

—, 'Primer: Defending the Rights of Refugees and Migrants in the Digital Age', 5 February 2024, <https://www.amnesty.org/en/documents/pol40/7654/2024/en>, accessed 4 February 2025

Article 19, *Taming Big Tech: A Pro-competitive Solution to Protect Free Expression* (London: Article 19, 2021), <https://www.article19.org/wp-content/uploads/2023/02/Taming-big-tech-UPDATE-Jan2023-P05.pdf>, accessed 24 October 2024

Association for Progressive Communications (APC), 'Online gender-based violence', [n.d.], <https://www.apc.org/en/tags/online-gender-based-violence>, accessed 24 October 2024

—, 'APC Internet Rights Charter', last updated 4 October 2024, <https://www.apc.org/en/pubs/apc-Internet-rights-charter>, accessed 6 May 2024

Atta, P. H. and Moraes, T., 'Summary report on the judgement of ADPF Nº 403 and ADI Nº 5.527: The WhatsApp case', Lapin, 29 May 2020, <https://lapin.org.br/en-gb/2020/05/29/summary-report-on-the-judgement-of-adpf-no-403-and-adi-no-5-527-the-whatsapp-case>, accessed 6 May 2024

Bilchitz, D. and Deva, S., 'The horizontal application of fundamental rights in India: "Kishor" (baby) steps in the right direction?', IACL-AIDC blog, 25 April 2023, <https://blog-iacl-aidc.org/2023-posts/2023/4/25/the-horizontal-application-of-fundamental-rights-in-india-kishor-baby-steps-in-the-right-direction>, accessed 6 May 2024

Bleyer-Simon, K., '(De)monetisation of disinformation: Can the actions of large online platforms be measured?', EUI Centre for Media Pluralism and Media Freedom and European Digital Media Observatory, 26 March 2024, <https://cmpf.eui.eu/demonetisation-of-disinformation>, accessed 24 October 2024

Boshell, P. M, 'The power of place: Geolocation tracking and privacy', Business Law Today, 25 March 2019, <https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy>, accessed 6 May 2024

Brady, W. J., Jackson, J. C., Lindström, B. and Crockett, M. J., 'Algorithm-mediated social learning in online social networks', *Trends in Cognitive Sciences*, 27/10 (2023), pp. 947–60, <https://doi.org/10.1016/j.tics.2023.06.008>

Brazil, Federative Republic of, Marco civil da Internet [Brazilian Civil Rights Framework for the Internet], Law No. 12.965/2014, <https://bd.camara.leg.br/bd/items/24856b06-35e5-433f-b6b6-56eecb09b728>, accessed 18 March 2025

Breaugh, J., Hammerschmid, G., Rackwitz, M. and Singh, R., 'What does private sector involvement in government digitalisation mean for public values?', London School of Economics [blog], 1 August 2023, <https://blogs.lse.ac.uk/europpblog/2023/08/01/what-does-private-sector-involvement-in-government-digitalisation-mean-for-public-values>, accessed 6 May 2024

Buckup, S., 'How public-private cooperation can connect and empower the "Global South"', World Economic Forum, 16 January 2023, <https://www.weforum.org/agenda/2024/01/public-private-cooperation-can-connect-and-empower-the-developing-world>, accessed 6 May 2024

Budnitsky, S., 'Kremlin tightens control over Russians' online lives – threatening domestic freedoms and the global Internet', The Conversation, 30 June 2022, <https://theconversation.com/kremlin-tightens-control-over-russians-online-lives-threatening-domestic-freedoms-and-the-global-Internet-182020>, accessed 6 May 2024

Buolamwini, J. and Gebru, T., 'Gender shades: Intersectional accuracy disparities in commercial gender classification', *Proceedings of Machine Learning Research*, 81 (2018), pp. 1–15, <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>, accessed 6 May 2024

Burrell, J., 'How the machine "thinks": Understanding opacity in machine learning algorithms', *Big Data & Society*, 3/1 (2016), <https://doi.org/10.1177/2053951715622512>

Çalı, B., 'The case for the right to meaningful access to the Internet as a human right in international law', in A. van Arnauld, K. von der Decken and M. Susi (eds), *The Cambridge Handbook of New Human Rights: Recognition, Novelty, Rhetoric* (Cambridge, UK: Cambridge University Press, 2020), <https://doi.org/10.1017/9781108676106.022>

California, State of, Department of Justice, 'California Consumer Privacy Act (CCPA) of 2018', last updated 13 March 2024, <https://oag.ca.gov/privacy/ccpa>, accessed 6 May 2024

Cats-Baril, A., 'Self-determination', Constitution Brief, September 2018, <https://www.idea.int/sites/default/files/publications/self-determination-constitution-brief.pdf>, accessed 6 May 2024

Celeste, E., *Digital Constitutionalism: The Role of Internet Bill of Rights* (Milton Park, UK: Routledge 2022), <https://doi.org/10.4324/9781003256908>

Center for Strategic and International Studies (CSIS), 'Significant Cyber Incidents Since 2006', [n.d.], <https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-04/240418_Cyber_Events.pdf?VersionId=TlrSq2hBc9eZ0dxXgNfkeJpmn169lIOh>, accessed 6 May 2024

Chan, K., 'UK health service to use Amazon Alexa to give medical advice', The Associated Press, 10 July 2019, <https://apnews.com/general-news-f6e7a41982ff4230b8d34e5648effd9b>, accessed 6 May 2024

Chan, M., Yi, J. and Kuznetsov, D., 'Government digital repression and political engagement: A cross-national multilevel analysis examining the roles of online surveillance and censorship', *The International Journal of Press/Politics*, 29/2 (2024), pp. 371–39, <https://doi.org/10.1177/19401612221117106>

Citizen Lab, The, 'Confirming large-scale Pegasus surveillance of Jordan-based civil society', 1 February 2024, <https://citizenlab.ca/2024/02/confirming-large-scale-pegasus-surveillance-of-jordan-based-civil-society>, accessed 4 October 2024

Columbia University Global Freedom of Expression, 'Bejarano v. Ministry of Defense', [n.d.a], <https://globalfreedomofexpression.columbia.edu/cases/bejarano-ricaurte-and-others-v-ministry-of-defense-and-others>, accessed 6 May 2024

—, 'Disini v. The Secretary of Justice', [n.d.b], <https://globalfreedomofexpression.columbia.edu/cases/disini-v-the-secretary-of-justice>, accessed 6 May 2024

—, 'Amnesty International Togo and Ors v. The Togolese Republic', [n.d.c], <https://globalfreedomofexpression.columbia.edu/cases/amnesty-international-togo-and-ors-v-the-togolese-republic>, accessed 6 May 2024

—, 'Charles Berbare v. Google Brasil Internet Ltda', [n.d.d], <https://globalfreedomofexpression.columbia.edu/cases/charles-berbare-v-google-brasil-Internet-ltda>, accessed 6 May 2024

—, 'Prohibition of Internet use for election campaign', [n.d.e], <https://globalfreedomofexpression.columbia.edu/cases/prohibition-of-Internet-use-for-election-campaign>, accessed 6 May 2024

—, 'Surgeon v. Court of Appeals of Santiago', [n.d.f], <https://globalfreedomofexpression.columbia.edu/cases/surgeon-v-court-of-appeals-of-santiago>, accessed 6 May 2024

—, 'Zimbabwe Lawyers for Human Rights v. Minister of State, National Security', [n.d.g], <https://globalfreedomofexpression.columbia.edu/cases/zimbabwe-lawyers-for-human-rights-v-minister-of-state-national-security>, accessed 6 May 2024

ConstitutionNet, 'Peru amends Constitution to include right to free access to the Internet', 25 September 2023, <https://constitutionnet.org/news/peru-amends-constitution-include-right-free-access-internet>, accessed 18 March 2025

Council of Europe, Parliamentary Assembly, Resolution 1987 (2014), 'The right to Internet access', 9 April 2014, <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=20870>, accessed 24 October 2024

Craig, P. P., 'The legal effect of directives: Policy, rules and exceptions', *European Law Review*, 34/3 (2009), p. 349, <https://ssrn.com/abstract=1433782>, accessed 6 May 2024

Crawford, K. and Calo, R., 'There is a blind spot in AI research', *Nature*, 538 (2016), pp. 311–13, <https://doi.org/10.1038/538311a>

Craymer, L., 'Tuvalu turns to the metaverse as rising seas threaten existence', Reuters, 15 November 2022, <https://www.reuters.com/business/cop/tuvalu-turns-metaverse-rising-seas-threaten-existence-2022-11-15>, accessed 6 May 2024

Crowther, H., '*Google v Spain*: Is there now a "right to be forgotten"?', *Journal of Intellectual Property Law and Practice*, 9/11 (2014), pp. 892–93, <https://doi.org/10.1093/jiplp/jpu148>

Custers, B., 'New digital rights: Imagining additional fundamental rights for the digital era', *Computer Law and Security Review*, 44 (2022), <https://doi.org/10.1016/j.clsr.2021.105636>

De Gregorio, G., *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge, UK: Cambridge University Press, 2022a), <https://doi.org/10.1017/9781009071215>

Douvika, E., 'Digital Democracy: Internet & Arab Spring', Institute for Internet & the Just Society, 30 August 2020, <https://www.Internetjustsociety.org/Internet-arab-spring>, accessed 6 May 2024

Edições Câmara Brasília, 'The Brazilian Civil Framework of the Internet in English', 2016, <https://docslib.org/doc/10588677/the-brazilian-civil-framework-of-the-internet-in-english>, accessed 6 May 2024

European Commission, 'EU and international partners put forward a Declaration for the Future of the Internet', 28 April 2022, <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2695>, accessed 24 October 2024

European Foundation for South Asian Studies (EFSAS), '(Mis)shaping the future of security: How encryption backdoors will affect us all', May 2021, <https://www.efsas.org/publications/articles-by-efsas/(mis)shaping-the-future-of-security-how-encryption-backdoors-will-affect-us-all>, accessed 4 October 2024

European Institute for Gender Equality (EIGE), 'Gender Equality Index 2020: Digitalisation and the Future of Work', 2020, <https://eige.europa.eu/publications-resources/toolkits-guides/gender-equality-index-2020-report/foreword?language_content_entity=en>, accessed 24 October 2024

European Parliament, 'Report with recommendations to the Commission on the right to disconnect', A9-0246/2020, 4 December 2020, <https://www.europarl.europa.eu/doceo/document/A-9-2020-0246_EN.html>, accessed 6 May 2024

European Union, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)', *Official Journal of the European Union*, L 119, 4 May 2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>, accessed 6 May 2024

—, 'European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01)', *Official Journal of the European Union*, C 23/1, 23 January 2023, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001>, accessed 18 March 2025

European Union Agency for Fundamental Rights, *Towards More Effective Policing: Understanding and Preventing Discriminatory Ethnic Profiling – A Guide* (Luxembourg: Publications Office of the European Union, 2010), <https://fra.europa.eu/sites/default/files/fra_uploads/1133-Guide-ethnic-profiling_EN.pdf>, accessed 6 May 2024

—, *Getting the Future Right. Artificial Intelligence and Fundamental Rights* (Luxembourg: European Publications Office of the European Union, 2020), <https://media.business-humanrights.org/media/documents/fra-2020-artificial-intelligence_en.pdf>, accessed 18 March 2025

Facebook, Community Guidelines, [n.d.], <https://www.facebook.com/help/477434105621119>, accessed 6 May 2024

Farrow, R., 'How democracies spy on their citizens', *The New Yorker*, 18 April 2022, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>, accessed 24 October 2024

Federal Constitutional Court (Bundesverfassungsgericht), Germany, Urteil des Ersten Senats vom 15. Januar 1958 – 1 BvR 400/51 –, Rn. 1-75, <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1958/01/rs19580115_1bvr040051.html>, accessed 6 May 2025 (in German).

Foley, R. and Swilling, M., 'How One Word Can Change the Game: Case Study of State Capture and the South African Social Security Agency', Centre for Complex Systems in Transition and Stellenbosch University, July 2018, <https://www0.sun.ac.za/cst/wp-content/uploads/2018/07/SASSA-State-Capture-_2018-07_-A4-report-for-web-standard.pdf>, accessed 6 May 2024

Fourcade, M. and Healy, K., *The Ordinal Society* (Cambridge, MA: Harvard University Press, 2024), <https://doi.org/10.4159/9780674296688>

Fowowe, S., 'Buhari declines assent to Digital Rights and Freedom Bill, four others', *The Guardian*, 20 March 2019, <https://guardian.ng/news/buhari-declines-assent-to-digital-rights-and-freedom-bill-four-others/#google_vignette>, accessed 6 May 2024

France, Republic of, Loi n° 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels [Law No. 2016-1088 of 8 August 2016 on Labour, Modernizing Social Dialogue and Securing Professional Career Paths], 10 August 2016, <https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000033001100>, accessed 6 May 2024

Frantziou, E., 'The horizontal effect of the Charter: Towards an understanding of horizontality as a structural constitutional principle', in *Cambridge Yearbook of European Legal Studies* (Cambridge, UK: Cambridge University Press, 2020), <https://doi.org/10.1017/cel.2020.7>

Freedom House, 'Freedom on the Net 2024: China', 2024, <https://freedomhouse.org/country/china/freedom-net/2024>, accessed 4 October 2024

Friedersdorf, C., 'Former national-security officials now see the peril of weakening encryption', *The Atlantic*, 30 July 2015, <https://www.theatlantic.com/politics/archive/2015/07/former-national-security-officials-see-the-peril-of-weakening-encryption/399848>, accessed 24 October 2024

Funk, A., Vesteinsson, K. and Baker, G., 'Freedom on the Net 2024: The Struggle for Trust Online', Freedom House, 2024, <https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online>, accessed 6 May 2024

Futch, D., 'Du Plessis v. De Klerk: South Africa's Bill of Rights and the issue of horizontal application', *North Carolina Journal of International Law*, 22/3 (1996), pp. 1009–37, <http://scholarship.law.unc.edu/ncilj/vol22/iss3/7>, accessed 6 May 2024

Gellman, B., Soltani, A. and Peterson, A., 'How we know the NSA had access to internal Google and Yahoo cloud data', *The Washington Post*, 4 November 2013, <https://archive.ph/4a0Kk#selection-375.0-605.33>, accessed 24 October 2024

Gill, L., Redeker, D. and Gasser, U., 'Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights', Berkman Center Research Publication No. 2015-15, 9 November 2015, <http://dx.doi.org/10.2139/ssrn.2687120>

Global Partners Digital, 'An open, interconnected and interoperable Internet (joint letter)', 13 September 2021, <https://www.gp-digital.org/an-open-interconnected-and-interoperable-Internet-joint-letter>, accessed 24 October 2024

Gohdes, A. R., *Repression in the Digital Age: Surveillance, Censorship, and the Dynamics of State Violence* (Oxford, UK: Oxford University Press, 2024), <https://doi.org/10.1093/oso/9780197743577.001.0001>

Gollom, M., 'Australia made a deal to keep news on Facebook. Why couldn't Canada?', CBC News, 3 August 2023, <https://www.cbc.ca/news/world/meta-australia-google-news-canada-1.6925726>, accessed 6 May 2024

Gonçalves da Silva, L. and Leitão, S., *Constitutional Framework of European Labour Law in Italy, France, Germany, Portugal and Spain* (Cham, Switzerland: Springer, 2023), <https://doi.org/10.1007/978-3-031-45717-3>

Gorwa, R., *The Politics of Platform Regulation: How Governments Shape Online Content Moderation* (Oxford, UK: Oxford University Press, 2024), <https://doi.org/10.1093/oso/9780197692851.001.0001>

Guariglia, M., 'Five concerns about Amazon Ring's deals with police', Electronic Frontier Foundation, 30 August 2019, <https://www.eff.org/deeplinks/2019/08/five-concerns-about-amazon-rings-deals-police>, accessed 4 October 2024

Guglya, L., '"Big" news from Geneva: Making sense of the fundamental right to digital integrity and its potential implications on digital sovereignty and beyond', EPFL Center for Digital Trust, 21 June 2023, <https://c4dt.epfl.ch/geneva-digital-sovereignty>, accessed 6 May 2024

Gutiérrez, J. D., 'UNESCO Global Judges' Initiative: Survey on the Use of AI Systems by Judicial Operators', United Nations Educational, Scientific and Cultural Organization, 2024, <https://unesdoc.unesco.org/ark:/48223/pf0000389786>, accessed 24 October 2024

S. Gutwirth, Y. Poullet, P. Hert, C. Terwangne and S. Nouwt (eds), *Reinventing Data Protection?* (Dordrecht, Netherlands: Springer, 2009), <https://doi.org/10.1007/978-1-4020-9498-9>

Haupt, C. E., 'The horizontal effect of fundamental rights', in G. De Gregorio, O. Pollicino and P. Valcke (eds), *Oxford Handbook of Digital Constitutionalism* (Oxford, UK: Oxford University Press, 2024), <https://doi.org/10.1093/oxfordhb/9780198877820.013.38>

Heikkilä, M., 'Dutch scandal serves as a warning for Europe over risks of using algorithms', Politico, 29 March 2022, <https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms>, accessed 18 March 2025

Heinmaa, A. and Kalandadze, K., *Special Voting Arrangements in Europe: Postal, Early and Mobile Voting*, Webinar Series Report (Stockholm: International IDEA, 2020), <https://doi.org/10.31752/idea.2021.3>

Henshall, W., 'E.U.'s AI regulation could be softened after pushback from biggest members', *Time*, 22 November 2023, <https://time.com/6338602/eu-ai-regulation-foundation-models>, accessed 6 May 2024

Hill, K., 'Another arrest, and jail time, due to a bad facial recognition match', *The New York Times*, updated 6 January 2021, <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>, accessed 18 March 2025

Hjort, J. and Sacchetto, C., 'Can Internet access lead to improved economic outcomes?', World Bank Blogs, 5 April 2022, <https://blogs.worldbank.org/en/digital-development/can-internet-access-lead-improved-economic-outcomes>, accessed 6 May 2024

Howard, P. N., Duffy, A., Freelon, D., Hussain, M., Mari, W. and Mazaid, M., 'Opening Closed Regimes: What Was the Role of Social Media during the Arab Spring?', Project on Information Technology and Political Islam, Working Paper 2011.1, 2011, <https://doi.org/10.2139/ssrn.2595096>

Human Rights Watch, 'Race to the Bottom: Corporate Complicity in Chinese Internet Censorship', 9 August 2006a, <https://www.hrw.org/report/2006/08/10/race-bottom/corporate-complicity-chinese-Internet-censorship>, accessed 10 October 2024

—, 'China: Internet companies aid censorship. Legislation and code of conduct needed to ensure ethical business practices', 10 August 2006b, <https://www.hrw.org/news/2006/08/10/china-Internet-companies-aid-censorship>, accessed 10 October 2024

—, 'Israel/Palestine: Facebook censors discussion of rights issues. Independent Investigation, Alignment with International Standards Needed', 8 October 2021, <https://www.hrw.org/news/2021/10/08/israel/palestine-facebook-censors-discussion-rights-issues>, accessed 6 May 2024

—, *'How Dare They Peep into My Private Life?' Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic* (Human Rights Watch, 2022), <https://www.hrw.org/sites/default/files/media_2022/10/HRW_20220711_Students%20Not%20Products%20Report%20Final-IV-%20Inside%20Pages%20and%20Cover.pdf>, accessed 20 March 2025

Huszár, F., Ktena, S. I., O'Brien, C. and Hardt, M., 'Algorithmic amplification of politics on Twitter', *Proceedings of the National Academy of Sciences*, 119/1 (2021), <https://doi.org/10.1073/pnas.2025334119>

India, Republic of, Law No. 22/2023, The Digital Personal Data Protection Act, 11 August 2023, <https://www.meity.gov.in/static/uploads/2024/02/Digital-Personal-Data-Protection-Act-2023.pdf>, accessed 6 May 2024

International IDEA, *Digital Microtargeting*, Political Party Innovation Primer 1 (Stockholm: International IDEA, 2018), <https://doi.org/10.31752/idea.2018.32>

—, 'Online Political Advertising and Microtargeting: The Latest Legal, Ethical, Political and Technological Evolutions', Webinar Series Report, 15 and 18 June 2020, <https://doi.org/10.31752/idea.2020.65>

—, *Protecting Democratic Elections through Safeguarding Information Integrity* (Stockholm: International IDEA, 2024a), <https://doi.org/10.31752/idea.2024.1>

—, 'Brazil – August 2024', Global State of Democracy Initiative, August 2024b, <https://www.idea.int/democracytracker/report/brazil/august-2024>, accessed 24 February 2025

International Telecommunication Union (ITU), 'Population of global offline continues steady decline to 2.6 billion people in 2023', 12 September 2023, <https://www.itu.int/en/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx>, accessed 6 May 2024

Internet Rights and Principles Coalition, IRPC Charter, [n.d.], <https://internetrightsandprinciples.org/charter>, accessed 6 May 2024

Internet Society, 'Artificial Intelligence and Machine Learning: Policy Paper', April 2017, <https://www.Internetsociety.org/resources/doc/2017/artificial-intelligence-and-machine-learning-policy-paper>, accessed 6 May 2024

Italian Republic, Camera dei Deputati [Chamber of Deputies], 'Declaration of Internet Rights', 2015, <https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf>, accessed 6 May 2024

—, Law No. 81/2017 on Measures for the Protection of Non-entrepreneurial Self-employment and Measures to Promote Flexible Working Arrangements, 13 June 2017

Jain, M., 'The Aadhaar card: Cybersecurity issues with India's biometric experiment', The Henry M. Jackson School of International Studies, University of Washington, 9 May 2019, <https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment>, accessed 6 May 2024

Juneja, P., *Artificial Intelligence for Electoral Management* (Stockholm: International IDEA, 2024), <https://doi.org/10.31752/idea.2024.31>

Kahn, R., 'Reno v. American Civil Liberties Union (1997)', Free Speech Center, last updated 3 January 2025, <https://firstamendment.mtsu.edu/article/reno-v-american-civil-liberties-union>, accessed 6 March 2025

Kaspersen, A., 'Can you have both security and privacy in the Internet age?', World Economic Forum 21 July 2015, <https://www.weforum.org/stories/2015/07/can-you-have-both-security-and-privacy-in-the-internet-age>, accessed 6 May 2024

Keller, D., 'Internet Platforms: Observations on Speech, Danger, and Money', Hoover Institution, Aegis Series Paper No. 1807, 13 June 2018, <https://www.hoover.org/research/internet-platforms-observations-speech-danger-and-money>, accessed 24 October 2024

Kodde, C., 'Germany's "right to be forgotten" – between the freedom of expression and the right to informational self-determination', *International Review of Law, Computers and Technology*, 30/1–2 (2016), pp. 17–31, <https://doi.org/10.1080/13600869.2015.1125154>

Komnenic, M., '109 biggest data breaches, hacks, and exposures as of 2024', Termly, 25 March 2024, <https://perma.cc/LZ7E-3TV4>, accessed 25 March 2024

Kosseff, J., *The Twenty-Six Words That Created the Internet* (Ithaca, NY: Cornell University Press, 2019), <https://doi.org/10.7591/9781501735783>

Krapiva, N., 'ECOWAS Togo court decision: Internet access is a right that requires protection of the law', Access Now, 14 July 2020, <https://www.accessnow.org/ecowas-togo-court-decision>, accessed 6 May 2024

La Moncloa, 'Carta de Derechos Digitales' [Digital Rights Charter], 2021, <https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/participacion_publica/audiencia/ficheros/SEDIACartaDerechosDigitales.pdf>, accessed 6 May 2024

Lanza, E., 'Standards for a Free, Open and Inclusive Internet', Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, OEA/Ser.L/V/II, CIDH/RELE/INF.17/17, 15 March 2017, <https://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf>, accessed 24 October 2024

La Red en Defensa de los Derechos Digitales, 'El erróneamente llamado "derecho al olvido" no es un derecho, es una forma de censura' [The erroneously named 'right to be forgotten' is not a right; it is a form of censorship], [n.d.], <https://r3d.mx/2016/07/12/el-erroneamente-llamado-derecho-al-olvido-no-es-un-derecho-es-una-forma-de-censura>, accessed 24 October 2024

Larson, J., Mattu, S., Kirchner, L. and Angwin, J., 'How we analyzed the COMPAS recidivism algorithm', Pro Publica, 23 May 2016, <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>, accessed 6 May 2024

Mac, R., 'Instagram censored posts about one of Islam's holiest mosques, drawing employee ire', BuzzFeed News, 12 May 2021, <https://www.buzzfeednews.com/article/ryanmac/instagram-facebook-censored-al-aqsa-mosque>, accessed 6 May 2024

Macaskill, E. and Dance, G., 'NSA files: Decoded – What the revelations mean for you', *The Guardian*, 1 November 2013, <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>, accessed 6 May 2024

Mitchell, A. and Diamond, L., 'China's surveillance state should scare everyone', *The Atlantic*, 2 February 2018, <https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203>, accessed 6 May 2024

Molla, R., 'Activists are pressuring lawmakers to stop Amazon Ring's police surveillance partnerships', Vox, 8 October 2019, <https://www.vox.com/recode/2019/10/8/20903536/amazon-ring-doorbell-civil-rights-police-partnerships>, accessed 4 October 2024

NETmundial, 'Internet Governance Principles', [n.d.], <https://document.netmundial.br/1-internet-governance-principles>, accessed 6 May 2024

Newman, N., Fletcher, R., Robertson, C. T., Arguedas, A. R. and Nielsen, R. K., 'Reuters Institute Digital News Report 2024', Reuters Institute for the Study of Journalism, 2024, <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf>, accessed 24 October 2024

Nigeria, Federal Republic of, Digital Rights and Freedom Bill 2019, accessible through Paradigm Initiative, 28 July 2022, <https://paradigmhq.org/report/digital-rights-and-freedom-bill-2019>, accessed 18 March 2025

Office of the United Nations High Commissioner for Human Rights, 'CCPR General Comment No. 16: Article 17 (Right to Privacy) – The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation', 8 April 1988, <https://www.refworld.org/legal/general/hrc/1988/en/27539>, accessed 24 October 2024

—, 'The UN Guiding Principles in the Age of Technology: A B-Tech Foundational Paper', September 2020, <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/introduction-ungp-age-technology.pdf>, accessed 24 October 2024

—, 'Human Rights Council discusses the right to privacy and human rights and the environment', 10 March 2022a, <https://www.ohchr.org/en/press-releases/2022/03/human-rights-council-discusses-right-privacy-and-human-rights-and>, accessed 6 May 2024

—, 'Human rights and democracy in the digital age,' 25 April 2022b, <https://www.ohchr.org/en/statements/2022/04/human-rights-and-democracy-digital-age>, accessed 16 April 2024

—, 'Spyware and surveillance: Threats to privacy and human rights growing, UN report warns', 16 September 2022c, <https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report>, accessed 6 May 2024

Organisation for Economic Co-operation and Development (OECD), 'Harnessing the Green and Digital Transitions for Gender Equality: Policy Insights from the 2024 OECD Forum on Gender Equality', OECD Public Governance Policy Papers, No. 61, 16 October 2024,

<https://www.oecd.org/en/publications/harnessing-the-green-and-digital-transitions-for-gender-equality_860d0901-en.html>, accessed 24 October 2024

Pagallo, U., *The Laws of Robots: Crimes, Contracts, and Torts* (Dordrecht, Netherlands: Springer, 2013), <https://doi.org/10.1007/978-94-007-6564-1>

Pillalamarri, A. and Stanley, C., 'Online content regulation: An international comparison', International Law and Policy Brief, 8 December 2021, <https://studentbriefs.law.gwu.edu/ilpb/2021/12/08/online-content-regulation-an-international-comparison>, accessed 6 May 2024

Pollicino, O., 'Digital private powers exercising public functions: The constitutional paradox in the digital age and its possible solutions', European Court of Human Rights, 15 April 2021, <https://www.echr.coe.int/documents/d/echr/Intervention_20210415_Pollicino_Rule_of_Law_ENG>, accessed 6 May 2024

Pollicino, O. and De Gregorio, G., 'Constitutional law in the algorithmic society', in H.-W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor and G. De Gregorio (eds), *Constitutional Challenges in the Algorithmic Society* (Cambridge, UK: Cambridge University Press, 2021), <https://doi.org/10.1017/9781108914857.002>

J. Posetti and N. Shabbir (eds), *The Chilling: A Global Study of Online Violence against Women Journalists* (Washington, DC: International Center for Journalists, 2022), <https://www.icfj.org/sites/default/files/2023-02/ICFJ%20Unesco_TheChilling_OnlineViolence.pdf>, accessed 24 October 2024

Pratama, H. M. and Salabi, N. A., *Adoption of Voting Technology: A Guide for Electoral Stakeholders in Indonesia* (Stockholm: International IDEA, 2020), <https://doi.org/10.31752/idea.2020.26>

Qian, I., Xiao, M., Mozur, P. and Cardia, A., 'Four takeaways from a Times investigation into China's expanding surveillance state', *The New York Times*, 26 July 2022, <https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html>, accessed 6 May 2024

Rainie, S. C., Kukutai, T., Walter, M., Figueroa-Rodríguez, O. L., Walker, J. and Axelsson, P., 'Issues in open data: Indigenous data sovereignty', in T. Davies, S. B. Walker, M. Rubinstein and F. Perini (eds), *The State of Open Data: Histories and Horizons* (Cape Town, South Africa, and Ottawa, Canada: African Minds and International Development Research Centre, 2019), <https://doi.org/10.5281/zenodo.2677801>

Rodrigo, Elias & Medrano Abogados, 'Ley de reforma constitucional que promueve el uso de las tecnologías de la información y reconoce el derecho de acceso a internet libre en todo el país' [Constitutional reform law that promotes the use of information technologies and recognizes the right of access to free Internet throughout the country], [n.d.], <https://perma.cc/YSD4-FY8M>, accessed 24 March 2025

Sayeedi, I., 'Last minute national objections to the EU's AI Act are a mistake. Here's why', Global Governance Institute, 27 November 2023, <https://www.globalgovernance.eu/publications/rolling-back-the-ai-act-is-a-mistake-heres-why>, accessed 6 May 2024

Secretaría General Iberoamericana (SEGIB), Carta Iberoamericana de Principios y Derechos en los Entornos Digitales [Ibero-American Charter of Principles and Rights in Digital Environments], [n.d.], <https://www.segib.org/wp-content/uploads/Carta-Iberoamericana-de-Principios-y-Derechos-en-los-Entornos-Digitales_Es.pdf>, accessed 24 October 2024

Shrivastava, A., 'Indian Supreme Court's judgment on "horizontal application" of fundamental rights: An "unconstitutional informal constitutional change"?', IACL-AIDC blog, 31 January 2023, <https://blog-iacl-aidc.org/2023-posts/2023/1/31/indian-supreme-courts-judgment-on-horizontal-application-of-fundamental-rights-an-unconstitutional-informal-constitutional-change>, accessed 6 May 2024

Silverman, C., Talbot, R., Kao, J. and Klühspies, A., 'How Google's ad business funds disinformation around the world', Pro Publica, 29 October 2022, <https://www.propublica.org/article/google-alphabet-ads-fund-disinformation-covid-elections>, accessed 24 October 2024

Smith, G. and Rustagi, I., 'When good algorithms go sexist: Why and how to advance AI gender equity', *Stanford Social Innovation Review*, 31 March 2021, <https://doi.org/10.48558/A179-B138>, accessed 24 October 2024

Sombatpoonsiri, J. and Mahapatra, S., 'Regulation or Repression? Government Influence on Political Content Moderation in India and Thailand', Carnegie Endowment for International Peace, July 2024, <https://carnegie-production-assets.s3.amazonaws.com/static/files/DDN_India%20and%20Thailand.pdf>, accessed 4 October 2024

Statista, 'Leading countries based on Facebook audience size as of April 2024', [n.d.], <https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users>, accessed 6 May 2024

Statusbrew, 'Social media for government: A complete guide', 26 December 2022, <https://statusbrew.com/insights/social-media-for-government>, accessed 6 May 2024

Stein, S. K., 'Lüth and Elfes – A German approach to a horizontal effect of fundamental rights', IACL-AIDC blog, 14 June 2022, <https://blog-iacl-aidc.org/new-blog-3/2022/6/14/lth-and-elfes-a-german-approach-to-a-horizontal-effect-of-fundamental-rights>, accessed 6 May 2024

Swiss Confederation, Constitution de la République et canton de Genève [Constitution of the Republic and Canton of Geneva], 14 October 2012, <https://silgeneve.ch/legis/data/rsg/rsg_a2_00.htm?myVer=1657287083823>, accessed 6 May 2024

Taitz, S., 'Five things to know about NSA mass surveillance and the coming fight in Congress', American Civil Liberties Union, 11 April 2023, <https://www.aclu.org/news/national-security/five-things-to-know-about-nsa-mass-surveillance-and-the-coming-fight-in-congress>, accessed 6 May 2024

Tan, J.-E., 'Digital rights in Southeast Asia: Conceptual framework and movement building', in Y. H. Khoo and D. Simanjundtak (eds), *Exploring the Nexus between Technologies and Human Rights: Opportunities and Challenges for Southeast Asia* (Bangkok: SHAPE-SEA, 2019), <https://jun-etan.com/documents/Digital-Rights-in-Southeast-Asia-Conceptual-Framework-and-Movement-Building.pdf>, accessed 6 May 2024

Taylor, L., 'Public actors without public values: Legitimacy, domination and the regulation of the technology sector', *Philosophy and Technology*, 34 (2021), pp. 897–922, <https://doi.org/10.1007/s13347-020-00441-4>

Taylor, P. M., *A Commentary on the International Covenant on Civil and Political Rights: The UN Human Rights Committee's Monitoring of ICCPR Rights* (Cambridge, UK: Cambridge University Press, 2020), <https://doi.org/10.1017/9781108689458>

Turner Lee, N. and Chin-Rothmann, C., 'Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color', Brookings Institution, 12 April 2022, <https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color>, accessed 24 February 2025

United Kingdom Government, 'Government Transformation Strategy: Better Use of Data', Policy Paper, 9 February 2017, <https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy-better-use-of-data>, accessed 6 May 2024

—, 'Online Safety Act: Explainer', 8 May 2024, <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer>, accessed 24 October 2024

United Nations, United Nations Charter, 26 June 1945, <http://www.un.org/en/charter-united-nations>, accessed 6 May 2024

—, Universal Declaration of Human Rights, 10 December 1948, <https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf>, accessed 6 May 2024

—, International Covenant on Civil and Political Rights, 16 December 1966, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>, accessed 6 May 2024

—, *The Charter of Human Rights and Principles for the Internet*, 4th edn (Internet Rights & Principles Coalition, 2014), <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf>, accessed 6 May 2024

United Nations Educational, Scientific and Cultural Organization (UNESCO), 'The Rewired Global Declaration on Connectivity for Education', [n.d.], <https://unesdoc.unesco.org/ark:/48223/pf0000380598/PDF/380598eng.pdf.multi>, accessed 20 March 2025

—, 'Code of Ethics for the Information Society proposed by the Intergovernmental Council of the Information for All Programme (IFAP)', 36 C/49, 10 October 2011, <https://unesdoc.unesco.org/ark:/48223/pf0000212696>, accessed 6 May 2024

—, *Principles for Governing the Internet: A Comparative Analysis* (Paris: UNESCO, 2015), <https://unesdoc.unesco.org/ark:/48223/pf0000234435>, accessed 6 May 2024

United Nations General Assembly, 'Follow-up to Paragraph 143 on Human Security of the 2005 World Summit Outcome', Resolution adopted by the General Assembly on 10 September 2012, A/RES/66/290, 25 October 2012, <https://documents.un.org/doc/undoc/gen/n11/476/22/pdf/n1147622.pdf>, accessed 6 May 2024

—, Resolution adopted by the General Assembly on 25 September 2015, 'Transforming our world: The 2030 Agenda for Sustainable Development', A/RES/70/1, 21 October 2015, <https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_70_1_E.pdf>, accessed 26 February 2025

—, Note by the Secretary-General, 'Promotion and protection of the right to freedom of opinion and expression', A/71/373, 6 September 2016, <https://digitallibrary.un.org/record/844396?ln=fr&v=pdf>, accessed 6 May 2024

United Nations Human Rights Council, 'Promotion, Protection and Enjoyment of Human Rights on the Internet', A/HRC/RES/20/8, 16 July 2012, <https://documents.un.org/doc/resolution/gen/g12/153/25/pdf/g1215325.pdf>, accessed 10 May 2025

—, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet', A/HRC/RES/26/13, 14 July 2014, <https://documents.un.org/doc/resolution/gen/g12/153/25/pdf/g1215325.pdf>, accessed 10 May 2025

—, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet', A/HRC/32/L.20, 27 June 2016, <https://www.article19.org/data/files/Internet_Statement_Adopted.pdf>, accessed 6 May 2024

—, 'The Right to Privacy in the Digital Age', Report of the United Nations High Commissioner for Human Rights, A/HRC/39/29, 3 August 2018, <https://www.ohchr.org/en/documents/thematic-reports/ahrc3929-right-privacy-digital-age-report-united-nations-high>, accessed 24 October 2024

—, 'Rights to Freedom of Peaceful Assembly and of Association', Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, A/HRC/41/41, 17 May 2019, <https://docs.un.org/en/A/HRC/41/41>, accessed 6 May 2024

—, 'Question of the Realization of Economic, Social and Cultural Rights in All Countries: The Role of New Technologies for the Realization of Economic, Social and Cultural Rights', A/HRC/43/29, 4 March 2020, <https://documents.un.org/doc/undoc/gen/g20/056/50/pdf/g2005650.pdf>, accessed 24 October 2024

—, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet', Resolution adopted by the Human Rights Council on 13 July 2021, A/HRC/RES/47/16, 13 July 2021a, <https://documents.un.org/doc/undoc/gen/g21/198/31/pdf/g2119831.pdf>, accessed 6 May 2024

—, 'The Right to Privacy in the Digital Age', Report of the United Nations High Commissioner for Human Rights, A/HRC/48/31, 13 September 2021b, <https://documents.un.org/doc/undoc/gen/g21/249/21/pdf/g2124921.pdf>, accessed 6 May 2024

—, 'Impact of the Digitalization of Education on the Right to Education', Report of the Special Rapporteur on the Right to Education, Koumbou Boly Barry, A/HRC/50/32, 19 April 2022a, <https://docs.un.org/en/A/HRC/50/32>, accessed 26 February 2025

—, 'Internet Shutdowns: Trends, Causes, Legal Implications and Impacts on a Range of Human Rights', A/HRC/50/55, 13 May 2022b, <https://documents.un.org/doc/undoc/gen/g22/341/55/pdf/g2234155.pdf>, accessed 6 May 2024

—, 'The Right to Privacy in the Digital Age', Report of the United Nations High Commissioner for Human Rights, A/HRC/51/17, 4 August 2022c, <https://docs.un.org/en/A/HRC/51/17>, accessed 25 February 2026

UN Women, 'Power on: How we can supercharge an equitable digital future', 24 February 2023, <https://www.unwomen.org/en/news-stories/explainer/2023/02/power-on-how-we-can-supercharge-an-equitable-digital-future>, accessed 6 May 2024

—, 'Artificial intelligence and gender equality', 28 June 2024, <https://www.unwomen.org/en/news-stories/explainer/2024/05/artificial-intelligence-and-gender-equality>, accessed 24 October 2024

US National Institute of Standards and Technology, 'NIST study evaluates effects of race, age, sex on face recognition software', 19 December 2019, <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>, accessed 18 March 2025

Vasagar, J., 'Out of office working banned by German labour ministry', *The Telegraph*, 30 August 2013

Vivarelli, A., 'The crisis of the right to informational self-determination', *The Italian Law Journal*, 1 (2020), <https://theitalianlawjournal.it/data/uploads/6-italj-1-2020/italj-vol.-06-no.-01-2020.pdf>, accessed 6 May 2024

Wachter, S., 'Affinity profiling and discrimination by association in online behavioural advertising', *Berkeley Technology Law Journal*, 35/2 (2020), <https://doi.org/10.2139/ssrn.3388639>

Wachter, S., Mittelstadt, B. and Floridi, L., 'Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation', *International Data Privacy Law*, 7/2 (2017), pp. 76–99, <https://doi.org/10.1093/idpl/ipx005>

Wachter, S., Mittelstadt, B. and Russell, C., 'Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI', *Computer Law and Security Review*, 41 (2021), <http://dx.doi.org/10.2139/ssrn.3547922>

Washington Post, *The*, 'Facebook's AI treats Palestinian activists like it treats Black activists. It blocks them.', 28 May 2021, <https://www.washingtonpost.com/technology/2021/05/28/facebook-palestinian-censorship>, accessed 6 May 2024

Weber, T. and Llave, O. V., *Right to Disconnect: Exploring Company Practices* (Luxembourg: Publications Office of the European Union, 2021), <https://www.eurofound.europa.eu/en/publications/2021/right-disconnect-exploring-company-practices>, accessed 6 May 2024

Wolford, B., 'What is GDPR, the EU's new data protection law?', GDPR.EU, [n.d.], <https://gdpr.eu/what-is-gdpr>, accessed 6 May 2024

World Health Organization, 'Infodemics and misinformation negatively affect people's health behaviours, new WHO review finds', 1 September 2022, <https://www.who.int/europe/news/item/01-09-2022-infodemics-and-misinformation-negatively-affect-people-s-health-behaviours--new-who-review-finds>, accessed 6 May 2024

World Wide Web Foundation, 'Artificial Intelligence: The Road Ahead in Low and Middle-Income Countries', June 2017, <https://webfoundation.org/docs/2017/07/AI_Report_WF.pdf>, accessed 6 May 2024

YouTube, Community Guidelines, [n.d.], <https://www.youtube.com/intl/ALL_ca/howyoutubeworks/policies/community-guidelines>, accessed 6 May 2024

Zubenko, V., 'How big data changes the scope of modern banking', Avenga, 19 September 2023, <https://www.avenga.com/magazine/how-big-data-changes-banking>, accessed 6 May 2024

Zuboff, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (London: Profile Books, 2019)

Further reading

Acland, S. and Willitts-King, B., 'Mobile phones for participation: Building responsible public-private humanitarian partnerships', Humanitarian Law & Policy blog, 7 December 2023, <https://blogs.icrc.org/law-and-policy/2023/12/07/mobile-phones-for-participation-building-responsible-public-private-humanitarian-partnerships>, accessed 6 May 2024

Angwin, J., Larson, J., Kirchner, L. and Mattu, S., 'What algorithmic injustice looks like in real life', Pro Publica, 25 May 2016, <https://www.propublica.org/article/what-algorithmic-injustice-looks-like-in-real-life>, accessed 6 May 2024

BBC, 'Spy code creator kills project after Syrian abuse', 10 July 2012, <https://www.bbc.com/news/technology-18783064>, accessed 6 May 2024

Bleyer-Simon, K., '(De)monetisation of disinformation: Can the actions of large online platforms be measured?', EUI Centre for Media Pluralism and Media Freedom and European Digital Media Observatory, 26 March 2024, <https://cmpf.eui.eu/demonetisation-of-disinformation>, accessed 24 October 2024

Brazil, Federative Republic of, Advocacia-Geral da União [Office of the Federal Attorney-General], Ação Direta de Inconstitucionalidade Nº 5527 [Direct Action of Unconstitutionality No. 5527], [n.d.], <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=560715474>, accessed 6 May 2024

Collaboration on International ICT Policy for East and Southern Africa (CIPESA), 'Litigating Internet disruptions in Africa: Lessons from Sudan', 3 March 2022, <https://cipesa.org/2022/03/litigating-Internet-disruptions-in-africa-lessons-from-sudan>, accessed 6 May 2024

Collins, K., 'Hacking team's oppressive regimes customer list revealed in hack', Wired, 6 July 2015, <https://www.wired.com/story/hacking-team-spyware-company-hacked>, accessed 6 May 2024

Colombia, Republic of, 'Paola Andrea Bonilla Castaño, nueva directora de la Comisión de Regulación de Comunicaciones (CRC)' [Paola Andrea Bonilla Castaño, new director of the Communications Regulatory Commission (CRC)], Gov.co, 1 March 2022, <https://www.crcom.gov.co/es/noticias/comunicado-prensa/paola-andrea-bonilla-castano-nueva-directora-comision-regulacion>, accessed 26 February 2025

—, 'Por medio del cual se establece el internet como derecho fundamental' [Whereby the Internet is established as a fundament right], Congreso de la República de Colombia, Cámara de Representantes [Congress of the Republic of Colombia, House of Representatives], 30 March 2022, <https://www.camara.gov.co/internet-derecho-fundamental-2>, accessed 26 February 2025

Columbia University Global Freedom of Expression, 'Bejarano v. Ministry of Defense', [n.d.], <https://globalfreedomofexpression.columbia.edu/cases/bejarano-ricaurte-and-others-v-ministry-of-defense-and-others>, accessed 6 May 2024

—, 'Mayorga Ariza v. Solano Peña', [n.d.], <https://globalfreedomofexpression.columbia.edu/cases/mayorga-ariza-v-solano-pena>, accessed 6 May 2024

—, 'Unwanted Witness-Uganda v. Attorney General', [n.d.], <https://globalfreedomofexpression.columbia.edu/cases/unwanted-witness-uganda-v-attorney-general>, accessed 6 May 2024

Confessore, N., 'Cambridge Analytica and Facebook: The scandal and the fallout so far', *The New York Times*, 4 April 2018, <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>, accessed 6 May 2024

Cronin, A. K., 'Open source technology and public-private innovation are the key to Ukraine's strategic resilience', War on the Rocks, 25 August 2023, <https://warontherocks.com/2023/08/open-source-technology-and-public-private-innovation-are-the-key-to-ukraines-strategic-resilience>, accessed 6 May 2024

De Gregorio, G., 'How does digital constitutionalism reframe the discourse on rights and powers?', Ada Lovelace Institute, 7 December 2022b, <https://www.adalovelaceinstitute.org/blog/digital-constitutionalism-rights-powers>, accessed 6 May 2024

e-Estonia, 'How did Estonia carry out the world's first mostly online national elections', 7 March 2023, <https://e-estonia.com/how-did-estonia-carry-out-the-worlds-first-mostly-online-national-elections>, accessed 6 May 2024

European Center for Constitutional and Human Rights, 'Surveillance software "made in Germany" for Turkish authorities? Public Prosecutor's Office charges FinFisher executives', [n.d.a], <https://www.ecchr.eu/en/case/surveillance-software-germany-turkey-finfisher>, accessed 6 May 2024

—, 'Gamma/FinFisher: UK rebukes German-British software company', [n.d.b], <https://www.ecchr.eu/en/case/gammafinfisher-uk-rebukes-german-british-software-company>, accessed 6 May 2024

—, 'Surveillance in Syria: European firms may be aiding and abetting crimes against humanity', [n.d.c], <https://www.ecchr.eu/en/case/surveillance-in-syria-european-firms-may-be-aiding-and-abetting-crimes-against-humanity>, accessed 6 May 2024

European Union, 'Regulation (EU) 2024/1689 of the European Parliament and of the Council', *Official Journal of the European Union*, 13 June 2024, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689>, accessed 18 March 2025

European Union Agency for Cybersecurity (ENISA), 'Threat landscape', [n.d.], <https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape>, accessed 5 February 2025

Forbidden Stories, Pegasus Project, [n.d.], <https://forbiddenstories.org/case/the-pegasus-project>, accessed 6 May 2024

Human Rights Watch, 'Meta's Broken Promises: Systemic Censorship of Palestine Content on Instagram and Facebook', 21 December 2023, <https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and>, accessed 6 May 2024

Macafee, T., McLaughlin, B. and Rodriguez, N. S., 'Winning on social media: Candidate social-mediated communication and voting during the 2016 US presidential election', *Social Media + Society*, 5/1 (2019), <https://doi.org/10.1177/2056305119826130>

McMillan, R., 'How the boy next door accidentally built a Syrian spy tool', Wired, 11 July 2012, <https://www.wired.com/2012/07/dark-comet-syrian-spy-tool>, accessed 6 May 2024

Office of the United Nations High Commissioner for Human Rights, 'Digital space and human rights', [n.d.a], <https://www.ohchr.org/en/topic/digital-space-and-human-rights>, accessed 6 May 2024

—, 'Freedom of assembly and of association', [n.d.b], <https://www.ohchr.org/en/topic/freedom-assembly-and-association>, accessed 6 May 2024

—, 'Privacy and data protection: Increasingly precious asset in digital era says UN expert', 19 October 2022, <https://www.ohchr.org/en/press-releases/2022/10/privacy-and-data-protection-increasingly-precious-asset-digital-era-says-un>, accessed 6 May 2024

Olasupo, A., 'Why Nigeria needs to sign Digital Right and Freedom Bill into law as the world goes digital', *The Guardian*, 2 July 2020, <https://guardian.ng/features/why-nigeria-needs-to-sign-digital-right-and-freedom-bill-into-law-as-the-world-goes-digital>, accessed 6 May 2024

O'Neill, P. H., 'The fall and rise of a spyware empire', MIT Technology Review, 29 November 2019, <https://www.technologyreview.com/2019/11/29/131803/the-fall-and-rise-of-a-spyware-empire>, accessed 6 May 2024

Organization for Security and Co-operation in Europe (OSCE), *Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE Participating States* (Vienna: OSCE, 2023), <https://www.osce.org/files/f/documents/2/7/539108_0.pdf>, accessed 6 May 2024

Pasquale, F., *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, MA: Harvard University Press, 2015), <https://doi.org/10.4159/harvard.9780674736061>

Peru, Republic of, Law No. 31878, 'Constitutional Reform Law Promoting the Use of Information and Communication Technologies and Recognizing the Right to Free Internet Access Nationwide', *El Peruano*, 23 September 2023, <https://busquedas.elperuano.pe/dispositivo/NL/2218362-2>, accessed 6 May 2024

Raso, F. A., Hilligoss, H., Krishnamurthy, V., Bavitz, C. and Kim, L., 'Artificial Intelligence and Human Rights: Opportunities and Risks', Berkman Klein Center Research Publication No. 2018-6, 25 September 2018, <https://doi.org/10.2139/ssrn.3259344>

Vogels, E. A., 'The State of Online Harassment', Pew Research Center, 13 January 2021, <https://www.pewresearch.org/Internet/2021/01/13/the-state-of-online-harassment>, accessed 24 October 2024

Wessler, N. F., 'The Supreme Court's most consequential ruling for privacy in the digital age: One year in', American Civil Liberties Union, 28 June 2019, <https://www.aclu.org/news/privacy-technology/supreme-courts-most-consequential-ruling-privacy-digital>, accessed 6 May 2024

Wolf, P., Nackerdien, R. and Tuccinardi, D., *Introducing Electronic Voting: Essential Considerations* (Stockholm: International IDEA, 2011), <https://www.idea.int/publications/catalogue/introducing-electronic-voting-essential-considerations>, accessed 6 May 2025

About the author

Juliane Müller is Associate Programme Officer in International IDEA's Digitalization and Democracy Programme. Previously, she worked for International IDEA's Constitution-Building Programme as a Fellow of the Carlo Schmid Programme, where she primarily focused on constitutional rights in the digital age. Prior to joining International IDEA, she worked on issues related to democracy, the rule of law and constitutional rights at various institutions and international organizations, including the Permanent Representation of Germany to the EU, the European Parliament, and the Max Planck Foundation for International Peace and the Rule of Law.

About International IDEA

The International Institute for Democracy and Electoral Assistance (International IDEA) is an intergovernmental organization with 35 Member States founded in 1995, with a mandate to support sustainable democracy worldwide.

WHAT WE DO

We develop policy-friendly research related to elections, parliaments, constitutions, digitalization, climate change, inclusion and political representation, all under the umbrella of the UN Sustainable Development Goals. We assess the performance of democracies around the world through our unique Global State of Democracy Indices and Democracy Tracker.

We provide capacity development and expert advice to democratic actors including governments, parliaments, election officials and civil society. We develop tools and publish databases, books and primers in several languages on topics ranging from voter turnout to gender quotas.

We bring states and non-state actors together for dialogues and lesson sharing. We stand up and speak out to promote and protect democracy worldwide.

WHERE WE WORK

Our headquarters is in Stockholm, and we have regional and country offices in Africa and West Asia, Asia and the Pacific, Europe, and Latin America and the Caribbean. International IDEA is a Permanent Observer to the United Nations and is accredited to European Union institutions.

OUR PUBLICATIONS AND DATABASES

We have a catalogue with more than 1,000 publications and over 25 databases on our website. Most of our publications can be downloaded free of charge.

<https://www.idea.int>

International IDEA
Strömsborg
SE-103 34 Stockholm
SWEDEN
+46 8 698 37 00
info@idea.int
www.idea.int

This report advocates for thorough protection of human rights in the digital age, emphasizing the strength of constitutional safeguards over ordinary legislation. As digital technologies increasingly influence civil and political rights, online as well as offline, robust constitutional frameworks are essential to address new challenges such as unwarranted surveillance, censorship and data monopolies. Ensuring adequate constitutional protection helps anchor fundamental rights in an evolving digital landscape.

ISBN: 978-91-7671-958-9 (PDF)