UNIVERSITY of the
WESTERN CAPE

Faculty of Law

The Regulation of Social Media Content Personalisation: An International Human Rights Perspective

A mini-thesis submitted in partial fulfilment of the requirements for the degree of Master of Laws (LLM)

By

Clifford Pierre Lewis

Student No: 4271110

Supervisor: Dr. Tinashe Kondo

13 December 2023

Examined version submitted on 21 July 2024

ABBREVIATIONS

ACHR	American Convention on Human Rights
ACHPR	African Charter on Human and Peoples' Rights
ACLU	American Civil Liberties Union
AI	Artificial Intelligence
ARPANET	Advanced Research Projects Agency Network
DSM	Digital Single Market
EC	European Commission
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
EU	European Union
GCA	Global Cybersecurity Agenda
GCI	Global Cybersecurity Index
ICTs	Information and Communication Technologies
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICJ	International Court of Justice
ICT	Information and Communications Technology
INTERPOL	International Criminal Police Organization
ITU	International Telecommunication Union
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
UNHRC	United Nations Human Rights Committee
UNODC	United Nations Office on Drugs and Crime
UPR	Universal Periodic Reviews
USA	United States of America
UTM	Universal Turing Machine

KEY WORDS AND PHRASES

Attention Economy

Democratic Participation

Facebook

International Human Rights

Social Media

Social Media Content

Social Media Content Personalisation

Soft Law

Twitter

Web 1.0

Web 2.0

TABLE OF CONTENTS

ABSTRACT

This mini-thesis critically examines the extent to which existing international, regional, and domestic legal frameworks provide effective mechanisms for preventing social media content personalisation from violating Article 25(b) of the International Covenant on Civil and Political Rights. Through a comprehensive analysis of human rights law and emerging cyber law, the study explores the complex interplay between psycho-social petterns of engagement, social media algorithms, and the human right of democratic participation.

The research employs historical, analytical, and comparative methodologies, and draws on literature from law, psychology and technology to evaluate legal instruments and enforcement mechanisms across international, regional, and domestic contexts. It identifies significant gaps in current frameworks, including challenges related to the inter-actor interconnectedness of human rights in cyberspace, jurisdictional issues arising from the borderless nature of social media, and evidentiary difficulties in establishing direct links between algorithmic content curation and human rights violations.

The mini-thesis argues that while progress has been made in developing cyber law, particularly in the European context, existing regulations insufficiently address the nuanced threats posed by social media content personalisation to democratic processes. It highlights the need for more robust, harmonised legal approaches that balance cybersecurity, user protection, and fundamental rights. The study concludes with recommendations for legal reform at international, regional, and domestic levels, emphasising the importance of algorithmic transparency, enhanced enforcement mechanisms, and a more nuanced understanding of the societal impacts of social media algorithms on political discourse and democratic participation.

CHAPTER 1: INTRODUCTION AND BACKGROUND

1.1. Introduction

> "Now we all have a platform, but what really scares me is these massive corporations that just have no standards for values at all. 'It's not my problem, it's your problem. But I'll take your money and we'll go public.'…Nobody's gonna remember what you tweeted, but you will never forget all that hateful shit that you read every single day that made you sick at school and made it hard for you to read, that made it hard for you to understand, that made it hard for you to focus, get a boyfriend, make a friend, be able to have sex…"
>
> - Lady Gaga, at the Yale School of Management Emotion Revolution Summit 2015[1]

This quote highlights the problem of an absence of a clear regulatory framework that governs the practice of social media content personalisation. This practice has been shown to create online environments that are hostile and harmful to users. As a means of exploring possibilities for the creation of such a framework, this mini-thesis critically explores the relationship between social media and international human rights. In particular, it examines how the practice of content personalisation by social media corporations within an 'Attention Economy' might be interfering with users' enjoyment of the 'universal and equal suffrage' component and the 'free expression of the will of the electors' aspect of the international human right to participate in public affairs, as enshrined in Article 25(b) of the International Covenant on Civil and Political Rights (ICCPR).

Both primary and secondary sources of information are used simultaneously in order to apply historical, analytical, and comparative methods of inquiry. This chapter provides an introduction to the mini-thesis by presenting the relevant background of these themes, a delineation of the research problem, research questions, objectives of the study, and a defence for the significance of the study. This is followed by an outline of the methodologies employed for conducting this research project, and the chapter concludes with an overview of the mini-thesis's chapters.

[1] Born This Way Foundation, and Yale Center for Emotional Intelligence. 'Keynote Address: Lady Gaga'. *Emotion Revolution Summit* (2015).

1.2. Background

The latest entry in The Matrix film franchise in 2021 offered a timely reminder from science fiction of the now decades-old apprehension of our doom coming at the digital behest of runaway artificial intelligence. As far as science 'fact' goes, however, during a 2017 TED address, former Google design ethicist, Tristan Harris, warned that the current state of artificial intelligence (AI) in social media poses a much clearer and present danger to humanity, than digital doom borne out of fiction[2]. More specifically, the age of social media has seen the emergence of an "Attention Economy", that treats human attention as a scarce commodity[3], the extraction and exploitation of which has raised much concern[4]. While the current state of AI in social media raises several concerns, in order to sufficiently address the trajectory of developments in AI in social media, it is important to trace the historical origins of the internet.

"The internet" started as an academic research project in 1969 and evolved to become a commercially available network connecting individuals and organisations in the 1990s[5]. Since the boom in its commercial use in the 1990s, the internet has evolved and continues to evolve from the so-called Web 1.0, to the Web 2.0 of today, and soon Web 3.0 of the future. On the Web 1.0 of the 1990s, the majority of users were consumers of content, with only a few content creators. Personal websites were common, consisting of mostly static web pages and directories that helped users find the content they were interested in consuming[6]. The early 2000s saw the emergence of Web 2.0, which emphasised user-generated content, usability, and interoperability[7]. Of its many features, Web 2.0 allows for interaction and collaboration among individuals who create user-generated content within virtual communities. With the evolution from Web 1.0 to Web 2.0, and the removal of barriers to participation and content creation, the world arguably shifted from the 'Information Age' to the 'Age of Curation', where the value of knowledge is no longer a given, but subject to scrutiny for its credibility[8]. The Web 2.0 internet, as we know it today, represents millions of distinct individuals and organisations,

[2] Harris T, 'How a handful of tech companies control billions of minds every day' TED April 2017.
[3] Davenport TH and Beck JC, *The Attention Economy: Understanding the New Currency of Business* (Boston, MA: Harvard Business School Press, 2001) 187.
[4] Bhargava VR and Velasquez M, 'Ethics of the attention economy: The problem of social media addiction' *Business Ethics Quarterly* vol 31 no 3 (2021) 321-359.
[5] Cerf V, 'How the internet came to be' in Aboba B (ed) *The Online User's Encyclopedia* (Boston, MA: Addison-Wesley, 1993) 103-137.
[6] Hiremath BK and Kenchakkanavar AY, 'An alteration of the Web 1.0, Web 2.0 and Web 3.0: A comparative study' *Imperial Journal of Interdisciplinary Research* vol 2 no 4 (2016) 705-710.
[7] O'Reilly T, *What Is Web 2.0* (Sebastopol, CA: O'Reilly Media, Inc., 2009) 10.
[8] Jansson J and Hracs BJ, 'Conceptualizing curation in the age of abundance: The case of recorded music' *Environment and Planning A: Economy and Space* vol 50 no 8 (2018) 1602-1625.

producing content, maintaining their own networks, and negotiating interconnection agreements[9].

Web 2.0 represented a fundamental disruption in the way people used the internet and interacted with one another[10]. Of the new ways of interacting that emerged, social media sites have arguably been one of the most disruptive forces within the internet. Social media platforms – most notably Facebook and Twitter – have allowed people to connect with each other at a level that speaks to deeply held values and beliefs[11]. The disruption in how people engage one another, brought about by social media, has since not remained restricted to cyberspace, but has indeed spilled over into real-world consequences[12]. Terrorists broadcast their attacks live[13], 'Twitter feuds' result in real-world casualties[14], and viral misinformation threatens public health[15].

Furthermore, technological advances have resulted in the internet becoming central to the public dissemination of information and, as a result, provides an unprecedented platform for the exercise of various protected freedoms[16]. However, as the volumes of information disseminated become increasingly abundant[17] while humans' mental capability for receiving information remains finite[18], user attention effectively becomes a scarce resource for those who generate revenue from the consumption of online content[19]. Resultantly, social media corporations adopt 'Attention Economics' in building their user interfaces, in order to ensure

[9] Perera C, Ranjan R, Wang L, Khan SU and Zomaya AY 'Privacy of Big Data in the Internet of Things Era' (2015) 17(3) IT Professional 32.
[10] Ornes S, 'The Internet of Things and the Explosion of Interconnectivity' (2016) 113(40) Proceedings of the National Academy of Sciences 11059.
[11] Saputra M and Siddiq IHA, 'Social Media and Digital Citizenship: The Urgency of Digital Literacy in the Middle of a Disrupted Society Era' (2020) 15(7) iJET 156.
[12] Singer PW and Brooking ET, *LikeWar: The Weaponization of Social Media* (Houghton Mifflin 2018) 188.
[13] Conway M and Dillon J, 'Future Trends: Live-Streaming Terrorist Attacks?' (2016) VOX-Pol 4.
[14] Menkhaus K, 'Al-Shabaab and Social Media: A Double Edged-Sword' (2014) 20(11) Brown Journal of World Affairs 309.
[15] Yang A et al, 'The Battleground of COVID-19 Vaccine Misinformation on Facebook: Fact Checkers vs. Misinformation Spreaders' (2021) 2(4) *Harvard Kennedy School Misinformation Review* 1.
[16] Gosztonyi G, 'The European Court of Human Rights: Internet Access As a Means of Receiving and Imparting Information and Ideas' (2020) 6(2) International Comparative Jurisprudence 134.
[17] Daniels T and Hepburn C, *On! The Future of Now: Making Sense of Our Always On, Always Connected World* (Crowdcentric Media 2014).
[18] Kiyonaga A and Egner T, 'Working Memory as Internal Attention: Toward an Integrative Account of Internal and External Selection Processes' (2013) 20(2) *Psychonomic Bulletin & Review* 228.
[19] Myllylahti M, 'An Attention Economy Trap? An Empirical Investigation into Four News Companies' Facebook Traffic and Social Media Revenue' (2018) 15(4) *Journal of Media Business Studies* 237.

users are presented with content that is most relevant, of interest, and personalised, based on their unique user profile[20].

Personalising the content that gets pushed to individual users' social media feeds makes a lot of business sense, as social media corporations' revenues are directly contingent on user engagement[21]. The practice of personalisation, however, becomes problematic if done with impunity. Having become the principal means by which most people receive and impart information and ideas, the internet is inextricably linked with modern democracies[22]. In fact, the borderless nature of social media and the dominance of private corporations in the filtering and dissemination of information has altered the balance of societal power and subverted constitutional equilibria globally[23]. Arguably, the most high profile example of this subversion of constitutional equilibria is the current political landscape of the United States (US). Analyses of online commentary regarding the 2016 US Presidential Election have suggested significant breakdowns in- and violations of democratic norms[24]. These trends reached a crescendo on January 6, 2021, when a mob of Trump supporters, heavily influenced by misinformation and extremist rhetoric consumed on social media, stormed the US Capitol Building in an attempt to overturn the 2020 presidential election results[25]. The events of January 6th are only one high-profile example of how social media content personalisation can interfere with democratic participation. This mini-thesis focuses on the sinister, less visible, and systemic interference with democratic processes on a global scale.

This inherent potential for misuse, either as an indirect consequence of maximising revenue or the direct result of interference with democratic processes, presents a significant risk to the rights of the general public as content personalisation can be designed in a manner to subvert

[20] Shashi Shekhar, Rohit Agrawal, and Karm Veer Arya, 'An Architectural Framework of a Crawler for Retrieving Highly Relevant Web Documents by Filtering Replicated Web Collections', in *2010 International Conference on Advances in Computer Engineering* (IEEE, 2010), pp. 29–33 <https://doi.org/10.1109/ACE.2010.64>.
[21] Winter S, Maslowska E and Vos AL, 'The Effects of Trait-Based Personalisation in Social Media Advertising' (2021) 114 *Computers in Human Behavior* 106525.
[22] Sunstein CR, 'Is Social Media Good or Bad for Democracy?' (2018) 15.27 The SUR File on Internet and Democracy 83.
[23] Celeste E, 'Terms of Service and Bills of Rights: New Mechanisms of Constitutionalisation in the Social Media Environment?' (2019) 33.2 *International Review of Law, Computers & Technology* 122.
[24] Chen GM et al, 'Breakdown of Democratic Norms? Understanding the 2016 US Presidential Election Through Online Comments' (2019) 5.2 Social Media + Society 1.
[25] LNg LHX, Cruickshank IJ and Carley KM, 'Cross-Platform Information Spread during the January 6th Capitol Riots' (2022) 12.1 Social Network Analysis and Mining 1.

people's rights[26] and function opaquely, resisting public audit, and limiting opportunities for oversight from regulatory agencies[27].

1.3. The research problem: A social issue that requires legal intervention

The ICCPR requires of state parties to protect, respect and fulfil the right of its citizens to 'universal and equal suffrage' in their participation in conducting public affairs[28], including the right to vote and to run for public office. Additionally, Article 25(b) of the ICCPR also requires that participation in the conduct of public affairs represent 'the free expression of the will of the electors'.[29] This research argues that social media corporations' practices of maximising engagement through content personalisation within an 'Attention Economy' interfere with users' ability to express their will by universal and equal suffrage as part of the human right to participate in public affairs. Furthermore, this research proposes that the existing regulatory frameworks to which social media corporations are subject to, are insufficient for the protection of these specific human rights.

Concerns for human rights in the context of the digital realm have largely been focussed on either the right to privacy[30] or the right to freedom of expression[31]. From these perspectives, the internet is thus conceptualised as primarily an information and communication tool that has the potential to affect the enjoyment of international human rights[32]. The internet, however, is far more than a mere optional communication tool. Rather, the internet has become a fundamental mechanism for the full realisation of all human rights and fundamental freedoms, including democracy and social justice[33]. More specifically, in the context of social media, while the roles and responsibilities of international corporations in privatised moderation, censorship, and 'down-ranking' of content have garnered much attention in recent years[34]

[26] Martin K, 'Ethical Implications and Accountability of Algorithms' (2019) 160.4 Journal of Business Ethics 835.
[27] Mittelstadt B, 'Auditing for Transparency in Content Personalisation Systems' (2016) 10 International Journal of Communication 4991.
[28] International Covenant on Civil and Political Rights, art 25(a) and (b), 2200A(XXI), 23 March 1979.
[29] Czapanskiy KS and Manjoo R, 'The Right of Public Participation in the Law-Making Process and the Role of Legislature in the Promotion of This Right' (2008) 19(1.12) Duke Journal of Comparative & International Law 1.
[30] International Covenant on Civil and Political Rights, art 7, 2200A(XXI), 23 March 1976.
[31] International Covenant on Civil and Political Rights, art 19, 2200A(XXI), 23 March 1976.
[32] Liu H-Y, 'The Digital Disruption of Human Rights Foundations' in *Human Rights, Digital Society and the Law: A Research Companion* (Routledge 2019) 75.
[33] Franklin M, Bodie R, Hawtin D, and Moreira M, *The Charter of Human Rights and Principles for the Internet (7th Ed.)* (Geneva, Switzerland: United Nations Internet Governance Forum: Internet Rights & Principles Coalition, 2019) Franklin M et al, *The Charter of Human Rights and Principles for the Internet* (7th edn, Internet Rights & Principles Coalition, Geneva 2019).
[34] Hintz A, 'Social Media Censorship, Privatized Regulation and New Restrictions to Protest and Dissent' in Dencik L and Leistert O (eds), *Critical Perspectives on Social Media and Protest: Between Control and Emancipation* (Rowman & Littlefield 2015) 109.
Land MK, 'Against Privatized Censorship: Proposals for Responsible Delegation' (2020) 60(2) *Virginia Journal of International Law* 363.

content curation practices such as prioritisation and ‘up-ranking’ have received far less scrutiny[35]. More specifically, the Council of Europe identifies the following areas of concern regarding social media content curation practices[36]:

- threats to independent media; and
- the potential for state capture; and
- prioritisation as a form of propaganda; and
- threats to self-determination; and
- a lack of intermediaries’ transparency.

While content personalisation is common practice, recent surveys show that an overwhelming majority of Facebook users feel they have little to no control over the content that appears in their newsfeed, and that less than 30% of users feel it is acceptable to be shown targeted advertising or political messages[37]. Furthermore, the personalisation of social media content by private corporations has been shown to result in fragmentation, polarisation and extremism that extend from cyberspace into the real world[38]. Of even greater concern is the unknown extent to which politicians and nations exploit these societal divisions to disrupt democratic processes in order to promote their own interests[39]. Here, the argument can be made that the observed negative impacts of social media on democracies worldwide are as a direct result of a regulatory vacuum with regard to content personalisation.

Therefore, this research argues that social media corporations' practices of maximising engagement through content personalisation within an 'Attention Economy' interfere with users' ability to express their will by universal and equal suffrage as part of the international human right to participate in public affairs. Furthermore, this research proposes that the existing

Etzioni A, 'Should We Privatize Censorship?' (2019) 36(1) Issues in Science and Technology 19.
Morgan JA, 'Private Censorship on Social Media: A Comparative Analysis of the Horizontal Application of Fundamental Rights' SSRN (2021) 4012102.
Ganesh B and Bright J, 'Countering Extremists on Social Media: Challenges for Strategic Communication and Content Moderation' (2020) 12(1) Policy and Internet 6.

[35] McGregor L, Murray D and Ng V, 'International Human Rights Law as a Framework for Algorithmic Accountability' (2019) 68(2) International and Comparative Law Quarterly 309; Winter S, Maslowska E and Vos AL, see above; Bennett WL, 'The Personalisation of Politics: Political Identity, Social Media, and Changing Patterns of Participation' (2012) 644(1) Annals of the American Academy of Political and Social Science 20.

[36] Mazzoli EM and Tambini D, ‘Prioritisation Uncovered: The Discoverability of Public Interest Content Online’, Council of Europe Study DGI(2020)19 (2020) 3.

[37] Westbrook L, Pera A, Neguriță O, Grecu I and Grecu G, ‘Real-Time Data-Driven Technologies: Transparency and Fairness of Automated Decision-Making Processes Governed by Intricate Algorithms’ (2019) 11(1) Contemporary Readings in Law and Social Justice 45.

[38] Kubin E and von Sikorski C, 'The Role of (Social) Media in Political Polarization: A Systematic Review' (2021) 45(3) Annals of the International Communication Association 188.

[39] Sunstein.

regulatory frameworks to which social media corporations are subject to, are insufficient for the protection of this specific human right.

1.4. Research question

This mini-thesis poses the central question: To what extent do existing international, regional, and domestic legal frameworks provide effective mechanisms for preventing social media content personalisation from violating Article 25(b) of the ICCPR?

1.5. Research objectives

The overall objective of the research is to better understand the links between social media content personalisation and the right to participate in public affairs, and to position the regulation of social media as a mechanism for the protection of international human rights. The high-level research objectives are delineated as follows:

- To trace the emergence of social media content personalisation, in the context of human rights, as justification for specialised regulation that guides social media content personalisation practices.
- To identify regional and international instruments that protect the human right to participate in public affairs.
- To determine to what extent social media content personalisation practices align with- or contradict the 'universal and equal suffrage' and 'free expression of the will of the electors' aspects of the international human right to participate in public affairs as guaranteed by Article 25(b) of the ICCPR.
- Assess the threats posed to global democracies by a vacuum in existing social media regulation.
- Trace cross-jurisdictional developments in social media regulation in relation to content censorship, ranking and prioritisation.
- Unpack links between social media engagement within an "Attention Economy" and the participation in public affairs at a domestic level.
- Offer recommendations for the development of regulation to prevent social media content personalisation practices from interfering with the enjoyment of the 'universal and equal suffrage' and 'free expression of the will of the electors' aspects of the international human right to participate in public affairs as guaranteed by Article 25(b) of the ICCPR.

1.6. Significance of the study

This research critically examines the legal implications of current content personalisation practices adopted by social media corporations on the international human right to express one's will through the participation in public affairs by universal and equal suffrage[40]. By analysing existing legal frameworks and regulations, as well as relevant legal theories and scholarly works, this study aims to identify the challenges and opportunities for the advancement of soft law and binding legal instruments towards the protection of human rights within the cyber realm. The study aims to produce clear recommendations for future avenues of legal theorising as well as guidelines for improving regulatory frameworks to better protect the international human right to express one's will through the participation in public affairs by universal and equal suffrage in the context of social media content personalisation. Given the increasing importance of social media in democratic participation[41] and the potential negative impacts of content personalisation on democratic processes[42], it is crucial to understand the legal implications and opportunities for addressing them. This research will make a significant theoretical and legal contribution by providing a comprehensive analysis of this issue and offering practical recommendations for addressing it.

1.7. Research methodology

This research represents a desktop study, drawing on both primary and secondary sources. Primary sources include case law, policies and legislation, while secondary sources include journal articles, academic books, newspapers and web publications. This mini-thesis, which is complex in nature, is situated at the intersection of cyber law and international human rights law, and sits firmly upon concerns of psychological and sociological wellbeing. Using a combination of methods aids the thorough exploration of the distinct sub-themes that collectively represent the interconnectedness of social media content personalisation and the international human right to express one's will through participation in public affairs by universal and equal suffrage. Specifically, by adopting a historical, analytical and comparative approach, this study is able to trace the emergence of legal doctrine, examine how that doctrine has been translated into legal instruments, and compare the application of various instruments

[40] International Covenant on Civil and Political Rights, art 25(b), 2200A(XXI), 23 March 1979.
[41] Bennett.
[42] Tufekci Z, 'How Social Media Took Us from Tahrir Square to Donald Trump' (2018) 14.18 MIT Technology Review 1; Pomerantsev P, 'To Unreality—and Beyond' (2019) 6.1 Journal of Design and Science.

across different contexts[43]. A historical approach is used to trace the development of cyber law as it pertains to social media regulation. Historical methods are also used to frame the evolution of international human rights as it pertains to the right to participate in public affairs. Thus, the historical context is as important in understanding legal frameworks as it is in examining statutes and case law[44]. Analytical legal research, in turn, aims to determine how courts and other legal actors currently apply a particular rule or principle[45]. This mini-thesis's analytical approach recognises that there are often multiple ways of interpreting legal sources[46], and critically examines the content of legal texts, questioning and evaluating different interpretations of their meaning[47]. Finally, the analysis concludes with a comparative exploration of social media regulation at an international, regional and local level. Specific regions that are included in the comparative analysis include Europe and the United States as home to social media giants such as Twitter and Facebook, as well as acute sites of political disruption that have been linked to social media. Comparative legal research is particularly useful when the legal issue under investigation is not contained within any one specific jurisdiction[48] – as is the case with both international human rights and social media content personalisation. Most importantly, comparative law research can reveal gaps in legal scholarship and practice[49].

1.8. Chapter outline

This mini-thesis consists of the following chapters:

Chapter 1: Introduction

Chapter 2: Conceptual Framework

Chapter 3: International Framework

Chapter 4: Regional Framework

Chapter 5: Domestic Framework

Chapter 5: Conclusion and recommendations

[43] Bakshi PM, 'Legal Research and Law Reform' in Verma SK and Wani A (eds), *Legal Research Methodology* (2nd edn, Indian Law Institute 2001) 111.
[44] Ellinger EP and Keith KJ, 'Legal Research: Techniques and Ideas' in Verma SK and Wani A (eds), *Legal Research Methodology* (2nd edn, Indian Law Institute 2001) 219.
[45] Dixon M, McCorquodale R and Williams S, *Cases & Materials on International Law* (6th edn, Oxford Press 2016) 485.
[46] Wróblewski J, 'Legal Reasoning in Legal Interpretation' (1969) 12(48) Logique et Analyse 3.
[47] TBustamante T, 'On the Argumentum Ad Absurdum in Statutory Interpretation: Its Uses and Normative Significance' in Dahlman C and Feteris E (eds), *Legal Argumentation Theory: Cross-Disciplinary Perspectives* (Springer 2013) 21.
[48] Bignami F, 'Introduction. A New Field: Comparative Law and Regulation' in Bignami F and Zaring D (eds), *Comparative Law and Regulation: Understanding the Global Regulatory Process* (Edward Elgar Publishing 2016) 1.
[49] French TR, 'Minding the Gap: 21st Century International Foreign and Comparative Law Research Issues' (2007) 35 Syracuse Journal of International Law and Commerce 159.

CHAPTER 2: CONCEPTUAL FRAMEWORK

2.1. Introduction

This chapter presents the complex interplay between social media, content personalisation practices, and international human rights. It argues that while social media has revolutionised large-scale information dissemination, commercially-driven content personalisation practices by social media corporations pose significant challenges to the universality and application of human rights, particularly in terms of participation in the conduct of public affairs. The chapter begins with a historical overview of international human rights, examining key instruments such as the UDHR and ICCPR, and the role of bodies such as the UN Human Rights Council and Committee. It then explores the evolution of the internet and social media, unpacking the impact of platforms such as Facebook, Twitter, and TikTok on public discourse and democratic processes. The concept of the 'Attention Economy' is also introduced, highlighting the ethical dilemmas posed by the algorithmic content curation that underpins content personalisation practices. The chapter concludes by presenting evolutionary psychology and socio-political context as conceptual lenses, that offer insights into why the regulation of social media – or lack thereof – has material implications for the enjoyment of human rights.

2.2. International Human Rights

Against the backdrop of the Second World War, and its "barbarous acts which […] outraged the conscience of mankind"[50], world leaders decided to complement the United Nation's (UN) existing Charter to maintain international peace and security[51], with a blueprint which would guarantee the rights of every person. The drafting of what would later become the Universal Declaration of Human Rights (UDHR) commenced in 1946[52]. The UN Commission on Human Rights, which later became the UN Human Rights Council[53], was established[54], and the UDHR was adopted at the UN General Assembly during its meeting in Paris on 10 December 1948 by the majority of member states, with only eight abstentions[55].

[50] Universal Declaration of Human Rights, Preamble, 217 A (III), 10 December 1948.
[51] United Nations Charter, art 1, 1 UNTS XVI, 1945.
[52] United Nations, 'History of the Declaration'. Available at United Nations website (accessed 3 May 2022.
[53] UN General Assembly, 'Resolution on the Human Rights Council', A/RES/60/251, 15 March 2006.
[54] Britannica, 'The UN Commission on Human Rights (1946–2006) and the UN Human Rights Council'. Available at Britannica website (accessed 3 May 2022).
[55] Politico, 'United Nations adopts Universal Declaration of Human Rights, Dec. 10, 1948'. Available at Politico website.

Through a resolution of the General Assembly on 15 March 2006, the UN Commission on Human Rights was replaced by the UN Human Rights Council[56]. The UN Human Rights Council is an inter-governmental body comprised of 47 UN member states which promotes the protection of international human rights, by assessing instances of human rights violations and making recommendations to address them[57]. The UN Human Rights Council meets at the UN office in Geneva and has a mandate to promote "universal respect for the protection of all human rights and fundamental freedoms for all and address situations of violations of human rights, including gross and systematic violations, and make recommendations thereon"[58]. Conversely, the UN Human Rights Committee is a body of independent experts with a mandate to monitor the implementation of the directives on international human rights provided by the UN Human Rights Council[59]. Thus, where the UN Human Rights Council is established by the General Assembly Resolution of 2006 and promotes the protection of international human rights, the UN Human Rights Committee is established by, and monitors the implementation of, the ICCPR[60].

The ICCPR is a key instrument that establishes the basic civil and political rights that must be protected by state parties. These rights include the right to life[61], freedom of expression[62], freedom of religion[63], the prohibition of discrimination[64], and the right to participate in the conducting of public affairs,[65] among others. The ICCPR is a binding international treaty, and along with the UDHR and the International Covenant on Economic, Social and Cultural Rights (ICESCR), serves as the structural cornerstone for protecting human rights internationally. Under Article 40 of the ICCPR, state parties are required to submit periodic reports to the UN Human Rights Committee detailing the measures they have taken to give effect to the rights recognised in the ICCPR, and the Committee conducts Universal Periodic Reviews (UPR) with each state party to assess their compliance with the Covenant[66].

The Committee reviews and collates information from (a) reports submitted by the state party, (b) information from other UN bodies, and (c) information from civil society organisations to

[56] UN General Assembly 'Resolution on the Human Rights Council' A/RES/60/251, 15 March 2006.
[57] UNHRC 'Welcome to the Human Rights Council'. Available at OHCHR website (accessed 3 May 2022).
[58] UN General Assembly 'Resolution on the Human Rights Council' A/RES/60/251, 15 March 2006.
[59] United Nations 'Mandate of UN Human Rights'. Available at OHCHR website (accessed 3 May 2022).
[60] ICCPR, art 28, para 1.
[61] ICCPR, art 6, para 1
[62] ICCPR, art 19, para 2.
[63] ICCPR, art 2, para 1.
[64] ICCPR, art 26.
[65] ICCPR, art 25(a) and (b).
[66] ICCPR, art 40, para 1.

provide state parties with a list of issues pertaining to the state's protection, respect and fulfilment of the human rights of all individuals within its territory and subject to its jurisdiction[67]. Through the ICCPR, the UN Human Rights Council, together with the UN Human Rights Committee, works to ensure that the basic civil and political rights are protected and upheld for all individuals around the world, regardless of their race, gender, religion or national status. The work of these bodies is founded on the principles of constructive dialogue, objectivity, and universality[68]. The universality of international human rights is a crucial cornerstone of the international order. All state parties to international treaties and protocols such as the ICCPR and the ICESCR are bound by the principle of the universality of human rights, including the right to life, liberty, and security of person[69] and the right to participation in public affairs[70]. This principle of the universality is what makes human rights transcend jurisdictions and applicable to diverse cultural contexts[71].

As social media corporations increasingly adopt sophisticated algorithmic methods to curate and personalise online content in order to optimise user engagement, it warrants an inquiry into these practices' compatibility with international human rights instruments such as the ICCPR. For example, the right to take part in the conduct of public affairs, which is protected under Article 25 of the ICCPR[72], may be compromised if social media companies are curating content in a way that restricts access to certain voices or perspectives. Similarly, Article 25 may also be violated if social media algorithms, directly or indirectly, perpetuate bias and discrimination, which may not only limit the universal and equal suffrage of individuals' participation in the conduct of public affairs, but may also hinder the free expression of the will of the electors. It is, therefore, paramount that the practice of content personalisation be thoroughly examined in the context of human rights to ascertain regulatory gaps.

2.3. The internet

Modern computing arguably started with the tragic brilliance of Alan Turing, an erudite British mathematician, logician, cryptanalyst, philosopher, theoretical biologist, and computer pioneer[73]. Living through the torment that was the life of a gay man in 1950s Britain, his life

[67] ICCPR, art 2, para 1.
[68] UN General Assembly 'Resolution on the Human Rights Council' (2006) 60/251.
[69] Universal Declaration of Human Rights, art 1, 217 A (III).
[70] ICCPR, art 25.
[71] Engle E, 'Universal Human Rights: A Generational History' (2006) 12 Annual Survey of International & Comparative Law 219.
[72] ICCPR, art 25(a).
[73] Teuscher C, *Alan Turing: Life and Legacy of a Great Thinker* (Springer 2013) 23.

came to a tragic end by his own hand[74], but not before producing some of the most significant earlier works in the field of computer science[75]. In 1935, Turing wrote about a computing device that had an infinite memory and a scanner that moved symbol by symbol across the memory, reading what it found and writing new symbols. A program of instructions that is also stored in the memory as symbols controls how the scanner behaves. Modern terminology refers to Turing's invention as the Universal Turing Machine (UTM).[76] In this sense, all modern computers are, in essence, UTMs[77].

Innovative thinkers like Alan Turing, paved the way for significant development of electronic digital computing over the course of the 20th century. In the 1940s and 1950s, researchers and engineers began to build computers that used electronic digital circuits, rather than mechanical or electro-mechanical devices[78]. These early electronic computers were large, expensive, and difficult to program, but they had the potential to be much faster and more powerful than their predecessors[79]. Another key development in the mid-20th century was the advent of computer networking. In the 1960s and 1970s, researchers began to explore the idea of connecting computers together to share resources and information[80]. This led to the development of the first wide-area networks (WANs), such as the Advanced Research Projects Agency Network (ARPANET), which was created by the US Department of Defence in 1969[81].

The development of computer languages and software also played a key role in the evolution of computer science, from the work of Turing and the emergence of the internet. Languages such as FORTRAN, LISP, and COBOL were developed in the 1950s and 1960s, and they made it possible to write programs that could be run on the new electronic computers[82]. These languages also made it possible to create more sophisticated programs and applications, which paved the way for the development of the internet and other advanced technologies[83].

[74] Doan L, 'Queer History Queer Memory: The Case of Alan Turing' (2017) 23(1) GLQ: A Journal of Lesbian and Gay Studies 113.
[75] Teuscher.
[76] Copeland BJ and Proudfoot D, 'Alan Turing's Forgotten Ideas in Computer Science' (1999) 280(4) Scientific American 98.
[77] Leeuwen JV and Wiedermann J, 'The Turing Machine Paradigm in Contemporary Computing' in Engquist B and Schmid W (eds), *Mathematics Unlimited—2001 and Beyond* (Springer 2001) 1139.
[78] Dertouzos ML and Moses J, *The Computer Age: A Twenty-Year View* (MIT Press 1980).
[79] Ceruzzi PE, *A History of Modern Computing* (MIT Press 2003).
[80] Peterson LL and Davie BS, *Computer Networks: A Systems Approach* (6th edn, Morgan Kaufmann 2022).
[81] Denning PJ, 'The Science of Computing: The ARPANET after Twenty Years' (1989) 77(6) American Scientist 530.
[82] Mogensen TÆ, 'A Brief History of Programming Languages' in *Programming Language Design and Implementation. Texts in Computer Science* (Springer 2002) 1.
[83] Tanenbaum AS, *Computer Networks* (Pearson Education 2013) 666.

Today, it is hard to imagine life without the internet. We use it for every conceivable facet of our lives, from work, to education, to business, to leisure and everything in between. The internet has become so fundamental in the way we live our lives that a debate has emerged regarding whether or not access to the internet should be considered a fundamental human right[84]. Arriving at a point where the status of the internet could be argued to be a basic fundamental right has been a fairly rapid process of development and evolution. The first iteration, Web 1.0, was originally developed by the US Department of Defence as a network for academics and researchers to communicate[85]. By the early 1990s, the network had expanded to include commercial interests and became commercially available to the general public[86]. The first website, info.cern.ch, was launched in 1991[87], and the first commercial website went live in 1995[88]. Web 1.0 was static, with some significant barriers to entry, and did not facilitate collaboration or dynamic content creation[89].

Web 2.0, as the evolutionary successor to Web 1.0, represents a manifestation of the continuous interaction between the human rights movement and information and communication technology[90]. In contrast to pre-2000 notions of freedom of information, a one-way flow of information is not communication; rather, communication entails active two-way dialogue, where the communication *process* is as important as the information it conveys[91]. The fundamental structural shift from one-way information flow to dynamic engagement created the perfect environment for social media platforms to emerge. The rise of social media platforms, such as Facebook and Twitter, has arguably been one of the most profound by-products of a global communication network which allowed for real-time engagement[92]. Social media has empowered people and organisations alike in facilitating connections, and enabling the sharing of information[93], while at the same time creating spaces conducive to conflict, hate, bigotry and predatory behaviour[94].

[84] Tully S, 'A Human Right to Access the Internet? Problems and Prospects' (2014) 14(2) Human Rights Law Review 175.
[85] Cerf.
[86] Steele C, 'A Look Back at the Earliest Websites' PC Mag (2014).
[87] CERN, 'The Birth of the Web'. Available at CERN website.
[88] Nix E, 'The World's First Web Site' History Channel (2018).
[89] Hiremath and Kenchakkanavar.
[90] Birdsall W, 'Web 2.0 as a Social Movement' (2007) 4 Webology 234.
[91] D'Arcy J, 'Direct Broadcast Satellites and the Right to Communicate' (1969) 118 EBU Review 14.
[92] Miller D, Cost E and Haynes N *How the World Changed Social Media* (UCL Press 2016) 150.
[93] Lin J, 'Social Media Has Changed the Lives of Modern Society' Summit News (2020).
[94] Tufekci Z, 'How Social Media Took Us from Tahrir Square to Donald Trump' (2018) 14.18 MIT Technology Review 1; Pomerantsev P, 'To Unreality—and Beyond' (2019) 6.1 Journal of Design and Science.

Recent developments indicate that 'the internet' is poised for another evolutionary leap in the near future[95]. The next stage in the internet's evolution will be characterised by artificial intelligence, virtual reality, augmented reality, and blockchain technology. Web 3.0 will deepen the human-machine interface and be more intuitive[96]. As we stand on the precipice of such developments, it is imperative that we learn from and improve on shortfalls in how we engage with the current version of the internet to avoid future evolutions perpetuating economic, political, and cultural fragmentation. Ascertaining regulatory gaps with regard to social media content personalisation is one avenue for addressing these shortfalls.

2.4. From the Information Age to the Age of Curation

Gone are the days when knowledge was the sole province of libraries and learned men. Easily accessible information has grown, and continues to grow, at astronomical rates. As a result, without a way to assess the relevance and quality of information, people are either overwhelmed or easily manipulated by untrustworthy sources. This rapid expansion of the volume and accessibility of information has given rise to the "Age of Curation", where the maxim 'Knowledge is Power' has become antiquated. Power now resides in one's ability to curate and select trusted content in a way that adds value.

In his 2010 article in Wired, Eliot van Buskirk, posits that we are currently living in the "Age of Curation". In this digital age, there is an overwhelming abundance of music, software, websites, news feeds, and people, all of which can be overwhelming and difficult to navigate. Van Buskirk argues that in this time of digital excess, curation is becoming increasingly important as a means of sorting through and making sense of the vast amount of information that is available to us.[97] Curation is the act of carefully selecting, organising, and presenting information and resources, so that they are more easily accessible and useful to the audience[98]. As such, curation is becoming an increasingly valuable skill for navigating today's digital landscape[99].

From a socio-economic and socio-political perspective, it can be argued that the ability to effectively discern between credible and unreliable information is not only a valuable skill, but,

[95] Barassi V and Treré E, 'Does Web 3.0 Come after Web 2.0? Deconstructing Theoretical Assumptions through Practice' (2012) 14(8) New Media & Society 1269.
[96] Centieiro H, 'The Insane Future of Web 3.0 and the Metaverse' Medium (2022).
[97] van Buskirk E, 'Overwhelmed? Welcome the Age of Curation' WIRED (2010).
[98] Abe A, 'Data Mining in the Age of Curation' in IEEE 12th International Conference on Data Mining Workshops (2012) 27.
[99] Beagrie N, 'Digital Curation for Science, Digital Libraries, and Individuals' (2008) 1(1) International Journal of Digital Curation 3.

indeed, one of survival in the modern era[100]. With the proliferation of internet fraud, online misinformation, and outright fake news, it is crucial to be able to identify trustworthy sources of information[101]. However, the need for digital curation skills extends beyond just identifying potential threats of fraud or deception. It is also crucial for everyday life and tasks. With the vast amount of information available online, it can be challenging to determine which sources are most relevant and reliable for making specific decisions, whether it be for shopping, healthcare, or personal finance. Being able to curate credible content with nuance, is essential for obtaining accurate and actionable information that can help us navigate our daily lives.[102]

The concept of content curation, and the power it holds, is of central importance to this mini-thesis. In order for a user to engage with online content in a meaningful way, content must be curated, either by the user themselves, or by a trusted third party. This process of curation might be as simple as applying effective keywords and phrasing while using a search engine such as Google, or as complex as data aggregation, synthesis, mapping and sequencing[103]. More and more, corporations that trade in data endeavour to perform the process of content curation on its users' behalf, regardless of whether the need for curation is simple or complex[104]. Big data organisations, such as social media companies, realise the power content curation holds and use various strategies to get users to relinquish this power in return for a wide variety of perceived benefits such as connecting with others, entertainment, staying current with world events, finding consumer goods, to name a few[105]. Relinquishing one's power to curate content starts a chain reaction with potentially devastating consequences.

2.5. Social media

Social media is a collective of various online platforms that allow users to create and share electronic content. Social media allows users to engage with one another and share information. It provides a platform to discuss common interests and helps people connect with others who have similar interests. Although social media platforms all have specific use policies and

[100] Eshet-Alkalai Y, 'Digital Literacy: A Conceptual Framework for Survival Skills in the Digital Era' (2004) 13 Journal of Educational Multimedia and Hypermedia 93.
[101] Graham R and Triplett R, 'Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization' (2017) 38(12) Deviant Behavior 1371.
[102] Leahy D and Dolan D, 'Digital Literacy: A Vital Competence for 2010?' in IFIP TC 3 International Conference on Key Competencies in the Knowledge Society (KCKS)/Held as Part OfWorld Computer Congress (WCC) (2010) 210.
[103] Good R, 'Content Curation Approaches: Types and Formats' Medium (2018).
[104] Westbrook et al.
[105] Oberlo, 'Why Do People Use Social Media' (2022).

community guidelines[106], barriers to access are virtually non-existent[107]. Anyone can, therefore create a social media account and start interacting with others. Consequently, over the last decade[108], those with political interests have seized this opportunity to grow their support base[109], disseminate important public information[110], and shape public opinion[111]. Beneath the apparent utility of social media for the participation in the conduct of public affairs, however, hides a double-edged sword. As privately-run social media corporations make profit-driven decisions, these platforms can easily disrupt participation as much as they can facilitate it. For example, Twitter's recent decision to eliminate free API access and replace it with high-priced subscription plans[112] has led to public service organisations like the Metropolitan Transportation Authority in New York City severing ties with the platform, resulting in the loss of real-time service alerts for public transport users[113]. The seemingly inherent tension between public service and commercial interests becomes particularly evident when examining specific social media platforms, such as Facebook, which have become an influential force in the realm of politics and public affairs[114].

Facebook is the world's largest social media platform, with more than 2 billion active monthly users[115]. With such a broad reach, Facebook is the ideal launchpad, for not only business interests, but socio-political interests as well. Facebook's structure has evolved from a simple networking tool, to a robust platform that offers functionality that allows one to create custom campaigns and track them over time to see how effective they are in garnering user engagement. The higher the engagement with the platform, the better the engagement with the campaign creator's content, the more the campaign creator can spend on their campaigns, adding up to higher revenues for Facebook. Facebook thus have a vested interest in keeping users engaged for as long as possible[116].

[106] Jiang JA et al, 'Characterizing Community Guidelines on Social Media Platforms' in ACM Conference on Computer Supported Cooperative Work (2020) 287.
[107] Allcott H and Gentzkow M, 'Social Media and Fake News in the 2016 Election' (2017) 31(2) Journal of Economic Perspectives 211.
[108] Nahon K, 'Where There Is Social Media There Is Politics' in Bruns A et al (eds), *The Routledge Companion to Social Media and Politics* (Routledge 2015) 39.
[109] Bennett.
[110] Heldman AB, Schindelar J and Weaver JB III, 'Social Media Engagement and Public Health Communication: Implications for Public Health Organizations Being Truly "Social"' (2013) 35(1) Public Health Reviews 1.
[111] Carson D, 'A Content Analysis of Political Discourse on TikTok' (2021) 415 Student Research Submissions.
[112] Binder M, 'WordPress Drops Twitter Social Sharing Due to API Price Hike' Mashable (1 May 2023).
[113] Hanif I, 'New York City Subway Ends Twitter Service Alerts after Musk Imposes Price Tag on API' Neowin (28 April 2023).
[114] Vaidhyanathan S, *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy* (Oxford University Press 2018) 165.
[115] Westbrook et al.
[116] Magalhães JC, 'Do Algorithms Shape Character? Considering Algorithmic Ethical Subjectivation' (2018) 4(2) Social Media and Society.

Facebook's business model and algorithms have been criticised for undermining various rights, including the human right to participate in the conduct of public affairs[117]. The platform's emphasis on maximising user engagement and advertising revenue has led to the promotion of sensational or divisive content, which distorts public discourse and undermines the ability of users to engage in informed online discussion[118]. Additionally, Facebook's use of personalisation algorithms has been accused of creating "echo chambers" where users are only exposed to information that confirms their existing beliefs, further exacerbating the polarisation of public discourse[119]. Most recently, Meta, Facebook's parent company, reached a $725 million settlement agreement in a class action lawsuit concerning, among other issues, its involvement in the Cambridge Analytica scandal, in which user data was improperly used to support Donald Trump's 2016 presidential campaign[120]. As a result, the platform has been criticised for playing a significant role in the deterioration of democratic discourse, particularly in the context of transparent democratic processes[121].

Far less in the way of functionality, Twitter is most commonly known as a platform where one can share one's thoughts in 140 characters or less. Despite these functional limitations, Twitter has been wildly successful since its creation in 2006 and is estimated to have over 328 million users[122]. Twitter pioneered the use of the hashtag as a means of quickly reaching content with specific themes. The practice of 'tagging' one's content with a hashtag has since been adopted by other platforms as well; however, this functionality is arguably still best deployed in Twitter by adding a layer of analytics to it to show users which topics are trending at any given time. Twitter, therefore, also holds great utility as a platform for creating a sense of urgency among users. Like Facebook, Twitter also promotes paid content and collects advertising revenue, and thus also has a vested interest in keeping users engaged for as long as possible[123].

Twitter's brevity and real-time nature have made it a valuable tool for breaking news and public discourse[124]. However, it is this defining feature that has led to challenges in conveying

[117] Benesch S, 'But Facebook's Not a Country: How to Interpret Human Rights Law for Social Media Companies' (2020) 38 Yale Journal on Regulation Bulletin 86.
[118] Kim YM et al, 'The Stealth Media? Groups and Targets behind Divisive Issue Campaigns on Facebook' (2018) 35(4) Political Communication 515.
[119] Del Vicario M et al, 'Echo Chambers: Emotional Contagion and Group Polarization on Facebook' (2016) 6 Scientific Reports 1.
[120] James C, 'Your Share of the $725 Million Facebook Settlement Will Be Tiny' The Wall Street Journal (New York City, 19 April 2023) [accessed 26 April 2023].
[121] Vaidhyanathan.
[122] Miller et al.
[123] Reuters, 'Big Tech Starts Requiring Vaccines; Twitter Closes Re-Opened U.S. Offices' Thomson Reuters (28 July 2021).
[124] Petrović S et al, 'Can Twitter Replace Newswire for Breaking News?' in 7th International Conference on Weblogs and Social Media (2013) 713.

complex ideas or provide context, which has been found to result in the spread of misinformation and misunderstandings[125]. Furthermore, Twitter's algorithmic curation of trending topics amplifies certain voices and perspectives while suppressing others, thereby skewing public discourse. Additionally, while Twitter has taken steps to address problematic content, the social media giant has been criticised for falsehoods being exceedingly more likely to be retweeted than truthful tweets[126]. These concerning trends, in the context of the platform's advertising-based business model have also received much criticism for incentivising the spread of sensational and divisive content rather than accurate and objectively informative content[127]. Such are these so-called "filter bubbles" that they distort public discourse through intellectual isolation and undermine the ability of users to engage in meaningful dialogue or make informed decisions[128].

Billionaire Tech-Industrialist, Elon Musk, started the process of acquiring the US-based social media corporation Twitter, Inc. on 14 April 14 2022, and completed the acquisition on 27 October 27 2022. Musk had already started purchasing shares in the company in January of 2022, and by April, he had become the largest shareholder with a 9.1 percent stake in the company[129]. Since the multi-billion Dollar takeover, Musk has all but torpedoed the once pioneering technology company[130]. Thousands of employees have been let go, and the company's structure and direction have become increasingly uncertain[131]. Musk's management style has been characterised by swift dismissals, a disregard for labour relations, and a lack of concern for the well-being of employees[132]. Among the most disturbing events that have transpired during the ongoing period of transition, include a refusal by the new CEO to consider any advice from Twitter's Trust and Safety team, who indicated the exceptionally high risks associated with Musk's planned paid account verification roll-out, which culminated in the resignation of Senior Director of Trust and Safety, Yoel Roth[133]. After abruptly departing

[125] Muneer A and Fati SM, 'A Comparative Analysis of Machine Learning Techniques for Cyberbullying Detection on Twitter' (2020) 12(11) Future Internet 1.
[126] Langin K, 'Fake News Spreads Faster than True News on Twitter—Thanks to People, Not Bots: Tweets Containing Falsehoods Were 70% More Likely to Be Retweeted than Truthful Tweets' Science (8 March 2018).
[127] Anand BN, 'The US Media's Problems Are Far Bigger Than Fake News and Filter Bubbles' in Doyle E (ed), *Domestic Extremism* (Greenhaven Publishing 2022) 138.
[128] Grossetti Q, Du Mouza C and Travers N, 'Community-Based Recommendations on Twitter: Avoiding The Filter Bubble' Web Information Systems Engineering (2019) 1.
[129] Zahn M, 'A Timeline of Elon Musk's Tumultuous Twitter Acquisition' ABC News (11 November 2022).
[130] Aten J, 'This Change Is How You Know Elon Musk's Twitter Experiment Has Already Failed: Musk Keeps Thinking He Can Make Twitter Better by Making It Worse' Inc. Africa (16 February 2023).
[131] Ortutay B and O'Brien M, 'Twitter Slashes Its Staff as Musk Era Takes Hold on Platform' AP News (5 November 2022).
[132] Hogler R, 'Why it May Not Matter Whether Elon Musk Broke US Labor Laws with His Mass Firings at Twitter' The Conversation (2022).
[133] Schiffer Z, Newton C and Heath A, 'Tears, Blunders and Chaos: Inside Elon Musk's Twitter' The Guardian (29 January 2023).

Twitter, Roth and other former Twitter executives were also called to testify before the US House Oversight Committee, convened to scrutinise the nature of Twitter's involvement in alleged political misconduct by the Biden family[134]. Testimonies from Roth and other former Twitter executives exposed the alarming realities of harassment and abuse within the company, and while these revelations are deeply troubling[135], some have speculated that Musk's acquisition of the platform was driven not by a desire for business success, but rather by a strategic political agenda to reshape its influence on public discourse[136].

One of the more recent additions to the social media landscape is TikTok. TikTok is a popular short-form video-sharing platform that has rapidly grown in popularity among users of all ages, and particularly among young people[137]. The platform allows users to create and share videos, often set to music, with a variety of editing tools and effects. TikTok has been shown to be a viable means for experts to combat rampant misinformation during the COVID-19 pandemic[138], has served as an invaluable tool for political mobilisation in the most recent US presidential elections[139], and acted as a conduit for Australian communities to process the collective trauma of the 2019-2020 bushfire disaster[140]. Despite its popularity and utility as a platform for creative expression and communication, TikTok has come under severe scrutiny, resulting in outright bans in some countries[141]. Most notably, TikTok has been highly criticised for its high risk of addiction, concerns regarding user data privacy[142], and the manner in which it has been shown to shape public discourse[143].

TikTok has been accused of being instrumental in orchestrating interference with transparent democratic processes[144], of enabling social structures that maintains the systemic exclusion of certain voices from public discourse[145], and has been argued to be inherently hostile to

[134] Herb J et al, 'Twitter Execs Acknowledge Mistakes with Hunter Biden Laptop Story but Say No Government Involvement' CNN Politics (8 February 2023).
[135] Paul K, 'Ex-Twitter Exec Details "Homophobic and Antisemitic" Abuse over Handling of Hunter Biden Story' The Guardian (8 February 2023).
[136] Seymour R, 'Elon Musk Never Cared If Twitter Was a Business Failure – He Wants a Political Win' The Guardian (22 November 2022).
[137] Auxier B and Anderson M, 'Social Media Use in 2021' Pew Research Center (April 2021).
[138] Ostrovsky AM and Chen JR, 'TikTok and Its Role in COVID-19 Information Propagation' (2020) 67(5) *Journal of Adolescent Health* 730.
[139] Herrman J, 'TikTok Is Shaping Politics. But How?' The New York Times (28 June 2020).
[140] Brown Y, Pini B and Pavlidis A, 'Affective Design and Memetic Qualities: Generating Affect and Political Engagement through Bushfire TikToks' (2022) Journal of Sociology 14407833221110268.
[141] Gray JE, 'The Geopolitics of "Platforms": The TikTok Challenge' (2021) 10(2) *Internet Policy Review* 1.
[142] Meral KZ, 'Social Media Short Video-Sharing TikTok Application and Ethics: Data Privacy and Addiction Issues' in Taskiran MN and Pinarbasi F (eds), *Multidisciplinary Approaches to Ethics in the Digital Era* (IGI Global 2021) 147.
[143] Zeng J and Abidin C, '"#OkBoomer, Time to Meet the Zoomers": Studying the Memefication of Intergenerational Politics on TikTok' (2021) 24(16) Information Communication and Society 2459.
[144] Herrman.
[145] Guzman A, 'TikTok and the Public Sphere: Examining the Structure of Online Discourse' (Texas State University 2021).

productive political discussions[146]. These concerns and allegations recently reached a fever pitch when TikTok CEO Shou Zi Chew testified before the US Congress in March of 2023, addressing, among others, concerns about China's influence, privacy, and content moderation[147]. Chew denied that the Chinese government had control over ByteDance[148], the parent company of TikTok, and emphasised the company's efforts to protect user data and moderate harmful content[149]. However, legislators expressed scepticism over TikTok's autonomy and ability to ensure user safety[150]. Furthermore, Chew denied allegations of censoring content related to sensitive issues for the Chinese government, such as the persecution of Uighur Muslims and the 1989 Tiananmen Square massacre[151].

The criticisms of social media platforms, as seen in the examination of Facebook, Twitter and TikTok, highlight a fundamental tension between commercial gain and user wellbeing. The common theme across these criticisms is the apparent manipulation of user engagement and attention for the sake of commercial gain. This raises the question of why it seems that all social media platforms seem to inevitably produce and reproduce polarisation and fragmentation. It appears that this is the natural progression when the key objective of the platform is to maintain user attention, thus creating an 'Attention Economy'. This highlights the importance of understanding the implications of such an 'Attention Economy' on human rights, particularly the right to participate in public affairs.

2.6. Content personalisation in the Attention Economy

The concept of an 'Attention Economy' is based on the same principle as most other forms of economic study, namely scarcity[152]. The scarce commodity here is the attention of human internet users. The 'Attention Economy', however, is not a phenomenon exclusive to social media. Broadcast media, especially news networks, have been acutely aware of the limited amount of attention that can be extracted from a group of potential viewers[153]. This problem of

[146] Boppana S, 'TikTok Is Bad for Political Discourse and Furthers Polarization' The Johns Hopkins News-Letter (1 October 2022).
[147] Kern R, 'TikTok's CEO Did Not Pass the Vibe Check at His First Hill Hearing' Politico (23 March 2023) [accessed 5 May 2023].
[148] Yilek C, 'TikTok CEO Faces Intense Questioning from House Committee amid Growing Calls for Ban' CBS News (23 March 2023).
[149] Shepardson D and Ayyub R, 'TikTok Congressional Hearing: CEO Shou Zi Chew Grilled by US Lawmakers' Reuters (24 March 2023) [accessed 5 May 2023].
[150] Thorbecke C, 'TikTok CEO in the Hot Seat: 5 Takeaways from His First Appearance before Congress' CNN Business (23 March 2023).
[151] Aschieris S, '6 Highlights of TikTok CEO's Testimony Before House Panel' The Daily Signal (23 March 2023) [accessed 5 May 2023].
[152] Wayne SJ and Rubinstein D, 'Extending Game Theoretic Propositions about Slack and Scarcity in Managerial Decision Making' (1992) 45(5) Human Relations 525.
[153] Myllylahti.

scarcity is exacerbated in the context of social media, because as the supply of online content expands infinitely, the demand for it has an upper limit in the form of the finite capacity of human attention[154].

Social media platforms did not always curate digital content on behalf of their users. In the early years of the social media boom, users essentially had the sole responsibility of curating their own content. This curation was typically the product of following accounts of interest, joining groups and subscribing to regular content. 2007 saw the introduction of the first 'social media algorithm' by Facebook, with Instagram implementing similar mechanisms in 2016 and others following in the same direction shortly after[155].

Meticulous research has developed, and continues to develop, models based on user data that can predict the likelihood of engagement. These engagements are not necessarily with primary content. Certain forms of secondary content such as Facebook comment sections[156], 'retweets' in the case of Twitter[157], or 'stitches' in the case of TikTok[158], have also been shown to trigger high levels of engagement. These engagement models are made up of many different factors. Some of the more commonly used factors include user demographics, such as age, gender, or nationality; user activity such as number of site visits and click rates, and communication trends such as the frequency and nature of comment, to name a few[159].

The seminal documentary film, *The Social Dilemma*, provides a critical examination of the negative impacts of social media on society. One of the key issues the film addresses is the engagement business model employed by social media companies. This model relies on user engagement as a primary metric to drive advertising revenue. To achieve this, companies use personalised algorithms that are designed to learn from users' behaviour and preferences, and to use that information to show them more of the content they are most likely to engage with. The film goes on to argue that this business model is inherently problematic for various reasons. First, these algorithms indiscriminately tailor content to individual user preferences and biases, resulting in the proliferation of echo chambers, where users are only exposed to a narrow range

[154] Kiyonaga and Egner.
[155] Edward, 'The Man Behind the Curtain: The Algorithms of Social Media' Inkspire (2018).
[156] Yoon G et al, 'Attracting Comments: Digital Engagement Metrics on Facebook and Financial Performance' (2018) 47(1) Journal of Advertising 24.
[157] Bhattacharya S, Srinivasan P and Polgreen P, 'Engagement with Health Agencies on Twitter' (2014) 9(11) PLoS One e112235.
[158] Alley A and Hanshew J, 'A Long Article about Short Videos: A Content Analysis of US Academic Libraries' Use of TikTok' (2022) 48(6) The Journal of Academic Librarianship 102611.
[159] Cloarec J, 'The Personalisation–Privacy Paradox in the Attention Economy' (2020) 161 Technological Forecasting and Social Change 120299.

of viewpoints, which reinforces existing biases and a lack of understanding of different perspectives. Additionally, the homogenisation of content, as algorithms increasingly prioritize the most popular content, has a detrimental effect on public discourse and democracy, as it can stifle the exchange of diverse ideas and promote populist ideologies.[160]

This practice of content personalisation based on personal and private facets of users' lives, raises several ethical and legal questions. Many social media users do not realise that sophisticated algorithms push specific content to their feeds with the singular goal of maximising engagement, while many others assume these algorithms are user-centric when in fact, they are platform-centric[161]. In fact, some critics go so far as to say that search and recommender algorithms of some social media platforms are 'misinformation engines' that drive engagement with zero regard to ethical practice or its subsequent impact[162]. Here it is difficult to ascertain if fragmentation, polarisation and extremism[163] as a result of social media content personalisation is an unintended consequence or if it is a deliberate component of social media corporations' engagement strategies.

The problematic nature of deploying specialised algorithms to extract value from the 'Attention Economy' by way of content personalisation presents an even more dire state of affairs when examining these practices from an evolutionary psychology perspective. A significant body of knowledge suggests that humans' capacity for reasoning is primarily a social adaptation, rather than an adaptation to the physical environment[164]. It is argued that our ability for reasoning evolved to help us persuade others towards group cohesion, rather than to discover objective truths. From this perspective, reasoning is not a wholly rational process but rather a social one, that has evolved as an adaptation that has ensured our survival and ascent to the top of the food chain by enforcing hyper-sociability[165]. Thus, cognitive mechanisms that underlie reasoning are not designed to solve abstract problems, but to facilitate communication and cooperation that serve the group[166]. Inherent in these cognitive functions is a strong in-group bias[167], and as such, echo chambers and filter bubbles that reinforce existing biases and a lack of

[160] Orlowski J, *The Social Dilemma* (Netflix 2020).
[161] Sonboli N et al, 'Fairness and Transparency in Recommendation: The Users' Perspective' in 29th ACM Conference on User Modeling, Adaptation and Personalisation (2021) 274.
[162] Bernal P, *The Internet, Warts and All: Free Speech, Privacy and Truth* (Cambridge University Press 2018).
[163] Kubin and von Sikorski.
[164] Heyes C et al, 'Knowing Ourselves Together: The Cultural Origins of Metacognition' (2020) 24(5) Trends in Cognitive Sciences 349.
[165] Mercier H and Sperber D, *The Enigma of Reason* (Harvard University Press 2017).
[166] Stanovich KE and West RF, 'Evolutionary versus Instrumental Goals: How Evolutionary Psychology Misconceives Human Rationality' in Over DE (ed), *Evolution and the Psychology of Thinking* (Psychology Press 2004) 176.
[167] Molenberghs P, 'The Neuroscience of In-Group Bias' (2013) 37 Neuroscience and Biobehavioral Reviews 1530.

understanding of different perspectives seem inevitable in the absence of regulatory guidelines that expressly prohibit its occurrence. Additionally, given the commercial incentive to create such highly engaging, yet destructive and polarising, online spaces, it is unlikely that social media corporations would alter content personalisation practices unless they are legally required to do so.

2.7. Conclusion

This chapter established the conceptual framework necessary for understanding the complex interplay between psycho-social processes, social media content personalisation, and international human rights. The evolution of the internet from Web 1.0 to Web 2.0 has fundamentally altered how information is disseminated and consumed, with social media platforms emerging as powerful intermediaries in this process. The rise of the Attention Economy has incentivised these platforms to employ sophisticated algorithms for content personalisation, ostensibly to enhance user experience but also to maximise engagement and, by extension, profit.

Thess practices raise significant ethical and legal concerns, particularly in relation to the human right to participate in the conduct of public affairs. The chapter has demonstrated how content personalisation, driven by commercial interests, can lead to the creation of echo chambers and filter bubbles, potentially distorting public discourse and undermining democratic processes. This is particularly problematic when viewed through the lens of evolutionary psychology, which suggests that humans are inherently susceptible to tribal thinking and confirmation bias.

The tension between the commercial imperatives of social media companies and the principles of universal human rights underscores the need for robust legal frameworks to govern content personalisation practices. As we move forward, it is crucial to consider how these practices may interfere with individuals' ability to express their will freely and participate equally in public affairs, as guaranteed by international human rights instruments. This sets the stage for a deeper examination of existing legal mechanisms and their adequacy in addressing these emerging challenges in subsequent chapters.

CHAPTER 3: INTERNATIONAL FRAMEWORK

3.1. Introduction

This chapter examines pertinent international legal structures related to the human right to participate in the conduct of public affairs and the regulation of social media. It starts with a delineation between 'Soft Law' and 'Hard Law' and distinguishes legal guidelines and principles from legally enforceable rules and regulations. The chapter introduces the human right to self-determination as a central principle upon which subsequent arguments regarding the status of international social media regulation are based, and frames the human right to participate in the conduct of public affairs as a direct extension of this fundamental right. The chapter also presents an overview of the practical enforcement mechanisms of international human rights and the evolving landscape of international cyber law. The chapter then concludes with an analysis of social media regulation in the context of human rights, at an international level.

3.2. 'Soft Law' and 'Hard Law'

In the preceding chapters, reference is made to International Human Rights. Many of the instruments governing this area of law are forms of 'Soft Law'. 'Soft Law' is an umbrella term for those legal instruments that are non-binding, such as the UDHR, General Comments, Treaty Bodies Reports, normative resolutions and recommendations, among others[168]. 'Soft Law' instruments exist predominantly in the context of international law, and are defined in opposition to clearer categories found in binding 'Hard Law' instruments. Despite being non-binding and being without enforcement mechanisms, 'Soft Law' instruments serve as a moral standard for states as it pertain to its conduct regarding specific matters of international concern[169]. As such, 'Soft Law' provides the essential structure for the interpretation and understandings of binding legal rules that, in turn, create expectations about future conduct[170]. For such interpretations, the concept of universality is central to 'Soft Law' instruments. Specifically, in the case of this study, human rights are argued to be universal and applicable to all individuals, by virtue of their humanity, regardless of the cultural context[171].

[168] Kenneth W. Abbott and Duncan Snidal, 'Hard and Soft Law in International Governance', *Legalization and World Politics*, 54(3) 2000, 421–56.
[169] Dinah Shelton, 'Soft Law', in *Routledge Handbook of International Law*, ed. by David Armstrong (New York: Routledge, 2009), pp. 68–80.
[170] Andrew T. Guzman and Timothy L. Meyer, 'International Soft Law', *Journal of Legal Analysis*, 2(1) 2010, 171–226 <https://doi.org/10.1093/acprof:oso/9780199299874.003.0005>.
[171] Eric Engle, 'Universal Human Rights: Generational History', *Annual Survey of International & Comparative Law*, 12(1) 2012 219.

The principle of universality, inherent to 'Soft Law' instruments, such as the UDHR, plays an important role in guiding the drafting of binding 'Hard Law' instruments like the ICCPR. For example, the right to freely express one's will through participation in public affairs by universal and equal suffrage is contained as a guiding principle in Article 21 of the UDHR[172], and is codified in Article 25 of the ICCPR[173] in order to create an obligation onto state parties to take action towards protecting, respecting and fulfilling this right. Such obligations drive the development of regional and domestic legal frameworks that are compatible with local norms and customs, and allow state parties to fulfil their commitment. As a result, the guiding ethos of the principle set out by the international 'Soft Law' instrument, trickles down to the domestic level.[174] Another example of how 'Soft Law' guides binding legal processes, can be seen in the periodically released General Comments of the *Human Rights Committee*[175]. General Comment 25 on the provisions of Article 25 of the ICCPR, for example, provides clarity on the meaning and scope of this provision regarding participation in the conduct of public affairs, providing guidance on how it should be implemented in practice[176]. Additionally, by virtue of the principle of universality, 'Soft Law' instruments also play an integral role in promoting the awareness and understanding of human rights among governments, civil society organisations, and individuals, as a tool for advocacy and education[177].

This notion of culturally-transcendent moral guidelines, however, is a point of significant contention among legal scholars, practitioners, and policymakers[178]. Proponents of cultural relativism argue that 'universal human rights' fail to take into account the cultural and historical context of different societies, and as such, represent legal mechanisms that are imposed by Western powers rather than common moral perspectives that naturally occur across diverse cultures and communities[179]. Article 2 of the ICCPR states that "each State Party to the present

[172] Article 21 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948*.
[173] Article 25 (a) and (b) of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979*.
[174] Sylvia I. Karlsson-Vinkhuyzen and Antto Vihma, 'Comparing the Legitimacy and Effectiveness of Global Hard and Soft Law: An Analytical Framework', *Regulation and Governance*, 3.4 (2009), 400–420 <https://doi.org/10.1111/j.1748-5991.2009.01062.x>.
[175] Philip Alston, 'The Historical Origins of the Concept of "General Comments" in Human Rights Law', in *The International Legal System in Quest of Equity and Universality*, ed. by Laurence Boisson de Chazournes and Vera Gowlland-Debbas (The Hague: Brill Nijhoff, 2001), pp. 763–76.
[176] UN Human Rights Committee, 'General Comment No. 25 on Article 25 of the International Covenant on Civil and Political Rights, on the Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service', *CCPR/C/21/Rev.1/Add.7, Adopted on 12 July 1996*.
[177] Charles Woolfson, 'Working Environment and 'Soft Law'in the Post-Communist New Member States', *Journal of Common Market Studies*, 44.1 (2006), 195–215.
[178] Ulf Johansson Dahre, 'Searching for a Middle Ground: Anthropologists and the Debate on the Universalism and the Cultural Relativism of Human Rights', *International Journal of Human Rights*, 21.5 (2017), 611–28 <https://doi.org/10.1080/13642987.2017.1290930>.
[179] Richard Mullender, 'Human Rights: Universalism and Cultural Relativism', *Critical Review of International Social and Political Philosophy*, 6.3 (2003), 70–103 <https://doi.org/10.1080/1369823032000233564>.

Covenant undertakes to respect and to ensure to all individuals…the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion".[180] From the wording of this provision, one is able to glean the position of nominal guidance such as the ICCPR, that the individual can be separated from the group – the very position challenged by advocates of cultural relativism[181]. For example, General Comment 28 on Article 3 of the ICCPR holds that State Parties "should ensure that traditional, historical, religious or cultural attitudes are not used to justify violations of women's right to equality before the law"[182]. This provision, again, assumes that rights by virtue of being a woman can be separated from traditional, historical, or religious views of gender[183]. Universality thus appears to be incompatible with the cultural embeddedness of the individual. Therefore, in light of the aforementioned, and given that various non-Western nations with absolute monarchies have also ratified the ICCPR (such as Qatar, Bahrain, and Eswatini[184]), this mini-thesis considers only those binding 'Hard Law' legal frameworks that are compatible with Article 25 of the ICCPR, in that they provide legally enforceable mechanisms for democratic forms of government.

Binding and enforceable 'Hard Law' instruments exist at an international, regional and national level, with their binding nature being the key defining feature[185]. The ICCPR itself is an international 'Hard Law' instrument, as the provisions contained therein create obligations upon state parties to protect, respect and fulfil the human rights of all individuals within its territory and subject to its jurisdiction[186]. The ICCPR is also a 'Hard Law' instrument by virtue of the First Optional Protocol that sets out a system by which the *Human Rights Committee* may receive and consider complaints regarding claims of human rights violations[187]. At a regional level, most notably, 'Hard Law' instruments pertaining to human rights include the European Convention for the Protection of Human Rights and Fundamental Freedoms

[180] Article 2, para. 1 of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979*.
[181] Fernand de Varennes, 'The Fallacies in the Universalism Versus Cultural Relativism Debate in Human Rights Law', *Asia-Pacific Journal on Human Rights and the Law*, 1 (2006), 67–84.
[182] Para. 5 of the 'CCPR General Comment No. 28: Article 3 (The Equality of Rights Between Men and Women)', *CCPR/C/21/Rev.1/Add.10, adopted 29 March 2000*.
[183] Binder, G. (1999) 'Cultural Relativism and Cultural Imperialism in Human Rights Law', *Buffalo Human Rights Law Review*, 211, pp. 211–221.
[184] United Nations, 'Parties to the International Covenant on Civil and Political Rights', *Available at: Https://Treaties.Un.Org/Pages/ViewDetails.Aspx?Src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en (Accessed on 11 June 2022)*.
[185] Daragh Murray, 'How International Humanitarian Law Treaties Bind Non-State Armed Groups', *Journal of Conflict and Security Law*, 20.1 (2015), 101–31.
[186] Article 2, para. 1 of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979*.
[187] Article 1 of the UN General Assembly, 'Optional Protocol to the International Covenant on Civil and Political Rights', *2200A(XXI), Adopted 23 March 1976* <https://www.ohchr.org/Documents/ProfessionalInterest/ccpr-one.pdf>.

(ECHR)[188], the American Convention on Human Rights (ACHR)[189], and the African Charter on Human and Peoples' Rights (ACHPR)[190]. The most commonly referred to 'Hard Law' instruments are those of sovereign nations, which carry penalties for not meeting one's obligations within its jurisdiction[191]. The borderless nature of social media, necessitates the regulation of the impact of social media content personalisation practices on human rights to be considered from both a 'Hard Law' and 'Soft Law' perspective.

3.3. The human right to self-determination

Human rights are interconnected and indivisible[192]. As such, the human right to participate in public affairs is inextricably linked, and arguably an extension of-, to the human right to self-determination[193]. At this point, it is important to consider self-determination and the free expression of the will of the electors as central to any discussion regarding the 'right to participation' in public affairs. This is because any interference with the 'right to self-determination' or the free expression of electors' will, outside of the specific context of participation in public affairs, could impede the enjoyment of said 'right' through universal and equal suffrage. The right to self-determination is an implicit aspect of several provisions of the UDHR, including Article 1, which establishes the foundation for the protection of individual autonomy and the free exercise of individual will[194], Article 18, which recognises the right to freedom of thought[195], and Article 19, which recognises the right to freedom of opinion and expression[196]. The right to self-determination is also explicitly codified in 'Hard Law' instruments, such as Article 1 of the ICCPR[197]. These provisions thus serve to establish the principle of self-determination as a fundamental aspect of human rights[198]. As suggested by the concerns raised in the documentary film, *The Social Dilemma*, social media corporations'

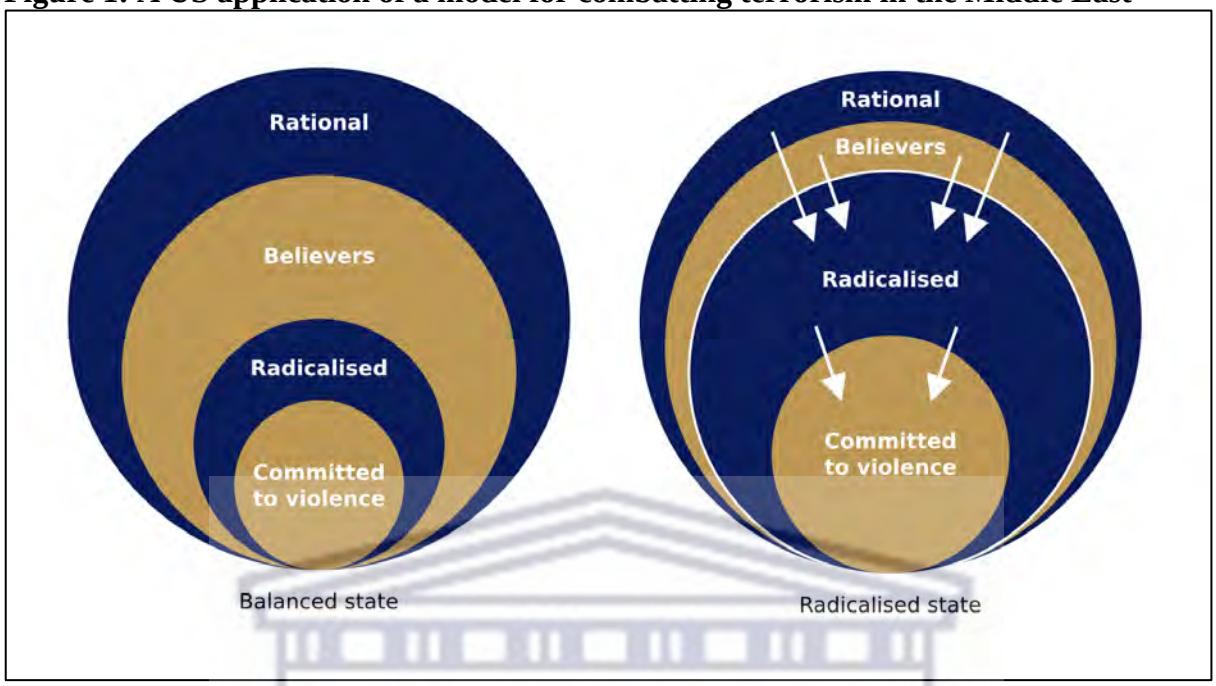
[188] Council of Europe. 'European Convention on Human Rights', *CoE Treaty Series 005, adopted on 4 November 1950.*
[189] Organization of American States. 'American Convention on Human Rights', *No. 17955 Vol. 1144, I-17955, adopted on 22 November 1969.*
[190] ACHPR, *CAB/LEG/67/3.*
[191] Gregory C. Shaffer and Mark A. Pollack, 'Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance', *Minnesota Law Review*, 94.3 (2010), 706–99.
[192] E.U. Petersmann, 'On "Indivisibility" of Human Rights', *European Journal of International Law*, 14.2 (2003), 381–85 <https://doi.org/10.1093/ejil/14.2.381>.
[193] Burak Cop and Dogan Eymirliglu, 'The Right of Self-Determination in International Law towards the 40th Anniversary of the Adoption of ICCPR and ICESCR', *Perceptions: Journal of International Affairs*, 10.4 (2018), 115–46.
[194] Article 1 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948.*
[195] Article 18 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948.*
[196] Article 19 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948.*
[197] Article 1(3), para. 1 of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979.*
[198] Elizabeth Rodríguez-Santiago, 'The Evolution of Self-Determination of Peoples in International Law', in *The Theory of Self-Determination*, ed. by F.R.. Tesón (Cambridge: Cambridge University Press, 2016), pp. 201–41.

revenue models produce practices such as content personalisation[199] that pose a real threat to the human right to self-determination[200].

In a delightfully sarcastic critique of the state of US political discourse on social media, entitled "School for Stochastic Swifties", anonymous political commentator, @enlighten.mentality, points out how "well-meaning Americans" are complicit in perpetuating propaganda that feeds the radicalisation that inevitably results in acts of violence. Their commentary applies two frameworks, namely (a) 'Stochastic Terrorism' and (b) a model for combatting terrorism in the Middle East developed by US Counter Intelligence.[201] While not a legal definition, Stochastic Terrorism refers to the use of politically motivated language to incite acts of violence against civilian populations while maintaining an apparent distance from said acts of violence[202]. The specific example this post examines, is the worrisome trend in US right-wing media to liken any form of LGBTQ-inclusivity, such as family-friendly drag performances, gender-affirming care, or even the acknowledgement from a teacher that some students in their class may have same-sex parents, to the sexualisation of children[203]. Such discourse constitutes Stochastic Terrorism as it has been demonstrated to create environments of hate and bigotry that have led to acts of unspeakable violence against the LGBTQ+ community[204]. In applying a model for combatting terrorism in the Middle East, TikTok user @enlighten.mentality demonstrates how right-wing extremism has become a leading terrorism threat in the West[205]. Figure 1 represents a graphic depiction of the application of this model. Each sphere represents a different depth of commitment to a given ideology. Each sphere also has its own thought leaders that sustain the respective depth of commitment to the ideology, however, all groups are the most responsive to thought leaders within the dominant sphere of influence.[206]

[199] Orlowski.
[200] Kubin and von Sikorski.
[201] @enlighten.mentality, 'School for Stochastic Swifties', *TikTok* <https://vm.tiktok.com/ZMYjvxAD7/>.
[202] Molly Amman and J. Reid Meloy, 'Stochastic Terrorism: A Linguistic and Psychological Analysis', *Perspectives on Terrorism*, 15.5 (2021), 2–13.
[203] Christopher Wiggins, 'Attacks on the LGBTQ+ Community Amount to Stochastic Terrorism', *Advocate*, 16 August 2022 <https://www.advocate.com/politics/2022/8/16/attacks-lgbtq-community-amount-stochastic-terrorism>.
[204] Nancy Unger, 'That the Worst Shooting in US History Took Place in a Gay Bar Is Unsurprising', *History News Network*, 13 June 2016 <https://www.advocate.com/politics/2022/8/16/attacks-lgbtq-community-amount-stochastic-terrorism>.
[205] Daniel Koehler, *Violence and Terrorism from the Far-Right: Policy Options to Counter an Elusive Threat* (The Hague: International Centre for Counter-Terrorism, 2019) <https://doi.org/10.19165/2019.2.02>.
[206] @enlighten.mentality.

Figure 1: A US application of a model for combatting terrorism in the Middle East



Adapted from McCants et al. (2006) via @enlighten.mentality

Within a "balanced state" the outer, more rational spheres, make up the largest population of any ideology, which act as a mediating force, tempering the impact of extreme beliefs. Those voices in the outer spheres are able to do so through rational actors who are balanced, intellectually empathetic and receptive to different beliefs and values.[207] However, as TikTok user @enlighten.mentality explains, if otherwise rational "well-meaning" individuals do not exercise critical thought and become complicit in disseminating propaganda, believing that their words are harmless, it creates an immoral belief structure that feeds a "radicalised state", where violent and extremist voices become the dominant sphere of influence within the ideology[208]. The application of the model presented in Figure 1 to the US context offers a conceptual framework for exploring how Stochastic Terrorism manifests in the West. More specifically, from this model, one can argue that content personalisation's inevitable echo chambers and filter bubbles provide the required (im)balance of an amplification of harmful ideas without a challenge to their validity, for immoral belief structures to flourish, and for otherwise rational people to engage in Stochastic Terrorism. Considering growing anti-LGBTQ+ sentiments in the US as an example again, it can be argued that such a "radicalised state" has indeed occurred as a direct result of "ordinary people" allowing themselves to

[207] William McCants, Jarret Brachman, and Joseph Felter, *Militant Ideology Atlas: Research Compendium* (West Point, NY: Combating Terrorism Center, 2006).
[208] Hannah Arendt, *Eichmann in Jerusalem: A Report on the Banality of Evil*, 2nd edn (London: Penguin, 2006) <https://doi.org/10.1057/palgrave.cpt.9300095>.

become complicit in the incitement of acts of violence by amplifying immoral belief structures about LGBTQ+ people.

In the preceding chapter, the evolutionary psychology perspective that humans' capacity for reasoning evolved primarily as a social adaptation for group cohesion, rather than for discovering objective truths, was discussed[209]. Here, the co-opting and perversion of "ordinary people's" capacity for free will, thought and opinion, towards radicalisation and the incitement of violence[210], seem inevitable when one considers that social media content personalisation involves the perpetual exposure of inherently tribal creatures to content that reinforces existing biases and a lack of understanding of different perspectives[211]. From this position, one can make the argument that social media content personalisation poses a material threat to the human right to self-determination.

There is thus a conceptual link between the right to self-determination and most other fundamental human rights, including more specifically, the right to participate in the conduct of public affairs. At a most basic level, the right to self-determination is considered as the foundation for the right to participate in the conduct of public affairs[212]. Self-determination includes determining one's own political status, and determining how that status impacts the establishment of one's own government[213]. If the right to self-determination, therefore, is to be fully realised, it would require free, universal, and equal participation in the government of their own country.

3.4. The human right to participate in the conduct of public affairs

The political landscape in many global democracies has undergone major shifts in recent years, with populism seemingly gaining significant momentum – most notably in Europe and the United States[214]. Political scholars and analysts assert that the internet, and more specifically social media, has been central in fuelling economic, political, and cultural fragmentation[215],

[209] Mercier and Sperber.
[210] Arendt.
[211] Orlowski.
[212] G. Ó. Erlingsson and J. Ödalen, 'A Normative Theory of Local Government: Connecting Individual Autonomy and Local Self-Determination with Democracy.', *Lex Localis*, 15.2 (2017), 329.
[213] Article 1(1), para. 1 of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979*.
[214] Bart Bonikowski, 'Three Lessons of Contemporary Populism in Europe and the United States Populism in the Twenty-First Century', *Brown Journal of World Affairs*, 23.1 (2016), 9–24.
[215] Zeynep Tufekci, 'How Social Media Took Us from Tahrir Square to Donald Trump', *MIT Technology Review*, 14.18 (2018), 1–12;
Peter Pomerantsev, 'To Unreality—and Beyond', *Journal of Design and Science*, 6.1 (2019) <https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html>.

both internationally and domestically[216]. Social media has low barriers to entry[217], provides a cost-effective platform for reaching supporters[218], relies on user-generated content[219], and allows for the effortless collection of user information that may be deployed for manipulation or surveillance[220]. It is thus not surprising that communication technologies such as social media have fundamentally changed how we produce, consume, and disseminate information, and connect with others on matters of socio-political import.

The human right to participate in the conduct of public (political) affairs is enshrined in Article 25 of the ICCPR, which recognises the right of every citizen to take part in the governance of their country, either directly or through freely chosen representatives[221], and to vote and be elected in periodic elections[222]. This right is integral to the maintenance of democratic societies and is directly connected to the principles of self-determination and the protection of individual autonomy[223]. The human right to participate in the conduct of public affairs, however, is not contained discretely within Article 25 of the ICCPR. Rather, it springs forth from Articles 1, 2 and 21 of the UDHR, which emphasise the equality of all individuals and the right to take part in the governance of one's country, which are fundamental principles underlying the right to participate in public affairs. Article 1 of the UDHR proclaims that all human beings are born free and equal in dignity and rights, setting the foundation for equal participation in political processes[224]. Article 2 asserts that everyone is entitled to all the rights and freedoms set forth in the UDHR without discrimination, which would require the conducting of public affairs should not be negatively influenced by factors such as race, colour, sex, language, religion, national or social origin, property, birth or other status[225]. Article 21 provides, outright, for the right to participate in the governance of one's country and the importance of free and fair elections[226]. Together, these provisions highlight the interconnected nature of the human right

[216] Ágnes Gulyás, 'Social Media and Journalism', in *The Routledge Companion to Digital Journalism Studies*, ed. by Bob Franklin and Scott Eldridge (New York: Routledge, 2016), pp. 396–406.
[217] Nahon.
[218] Ankit Kashyap and Mehak Jonjua, 'Social Media - A New Digital Power to Influence Voters', *International Journal of Scientific and Technology Research*, 9.4 (2020), 693–99.
[219] Angella J. Kim and Kim K.P. Johnson, 'Power of Consumers Using Social Media: Examining the Influences of Brand-Related User-Generated Content on Facebook', *Computers in Human Behavior*, 58 (2016), 98–108 <https://doi.org/10.1016/j.chb.2015.12.047>.
[220] Samuel Ribeiro-Navarrete, Jose Ramon Saura, and Daniel Palacios-Marqués, 'Towards a New Era of Mass Data Collection: Assessing Pandemic Surveillance Technologies to Preserve User Privacy', *Technological Forecasting & Social Change*, 167 (2021), 120681.
[221] Article 25(a) of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979.*
[222] Article 25(b) of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979.*
[223] A. Aviram and A. Assor, 'In Defence of Personal Autonomy as a Fundamental Educational Aim in Liberal Democracies: A Response to Hand', *Oxford Review of Education*, 36.1 (2010), 111–26.
[224] Article 1 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948.*
[225] Article 2 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948.*
[226] Article 21 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948.*

to participate in the conduct of public affairs and its fundamental link to other human rights, such as the rights to equality, non-discrimination, and self-determination.

Within the context of social media content personalisation, numerous factors present a threat to the human right to participate in the conduct of public affairs. One such factor is the limited scope of information to which users are exposed, which undermines their ability to make informed decisions about political issues that affect them and others[227]. This limitation of exposure to diverse thought inevitably creates polarisation, as users become snared in a narrow worldview[228]. The creation of such insular online environments is not an unintended consequence, but a deliberate outcome of social media algorithms, which are engineered to maximise user engagement within the Attention Economy[229]. By exploiting humans' tribal inclinations[230], these algorithms push content that affirms users' existing biases and beliefs[231], at the expense of balanced information that fosters healthy public discourse. Crumbling common ground and a diminished willingness to engage in constructive dialogue with others, jeopardise the broader socio-political landscape and undermine the foundation of democratic processes[232], which are necessary for the enjoyment of the human right to participate in the conduct of public affairs.

Insular online environments affect the participation in the conduct of public affairs for both individuals within these closed information ecosystems and those on the periphery. Revenue models that require content that is guaranteed to be engaged with is pushed to social media users, also risks the suppression of dissenting voices and minority opinions. The silencing of minority opinions also promotes an imbalanced public discourse that stifles necessary critical debate and perpetuates the rise of populism within the global political landscape[233]. Political polarisation and social fragmentation may thus occur not only through insulation, but also through exclusion and suppression. Differing perspectives, struggling to gain traction undermine the pluralistic nature of democratic processes and hampers the ability of individuals to engage in meaningful dialogue on matters of public concern.

[227] Del Vicario et al.
[228] Kubin and von Sikorski.
[229] Sonboli N, Smith JJ, Cabral Berenfus F, Burke R, and Fiesler C, 'Fairness and Transparency in Recommendation: The Users' Perspective', in *29th ACM Conference on User Modeling, Adaptation and Personalisation*, 2021, pp. 274–79 <https://doi.org/10.1145/3450613.3456835>.
[230] Mercier and Sperber.
[231] Orlowski.
[232] Kubin and von Sikorski.
[233] J. Petrov, 'The Populist Challenge to Human Rights', *International Journal of Constitutional Law*, 18.2 (2020), 476–91 <https://doi.org/10.1093/jhuman/hux007>.

Current practices in social media content personalisation seem at best irresponsible and at worst, a calculated attempt to erode democratic values. This suggests another potential threat to the human right to participate in the conduct of public affairs, namely the lack of transparency regarding algorithmic practices of social media corporations[234]. The case of foreign involvement in the 2016 US presidential election, through the use of social media[235], serves as a prime example of the potential for undue influence a lack of transparency in content personalisation practices can have on the right to freely express one's will through participation in public affairs by universal and equal suffrage[236]. Russian operatives were found to have created fake social media accounts and pages to spread divisive messages and misinformation during the 2016 election[237], which highlights the vulnerabilities in current practices. It has been shown that social media algorithms can be designed to function opaquely, resist audit, and limit opportunities for oversight[238]. A lack of transparency regarding the algorithmic practices of social media corporations in curating content raises concerns about the potential for manipulation and undue influence on public opinion[239]. As highlighted by the Council of Europe, the opacity of these algorithms makes it difficult for users to understand how and why certain content is being presented to them, which may compromise their ability to effectively participate in public affairs[240].

The risks associated with a lack of transparency in algorithmic practices extend beyond government interference. Numerous recent incidents have demonstrated that social media content personalisation provides an opportune environment for private corporations to exert undue influence over individuals seeking to exercise their right to participate in the conduct of public affairs[241]. Some large corporations have vested interests in specific political outcomes, and have been found to use their financial reach to promote political content that aligns with their corporate agendas, while suppressing opposing viewpoints[242]. This manipulation of

[234] H. J. Watson and C. Nations, 'Addressing the Growing Need for Algorithmic Transparency', *Communications of the Association for Information Systems*, 45.1 (2019), 26.
[235] Adam Badawy, Emilio Ferrara, and Kristina Lerman, 'Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign', in *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 2017, pp. 258–65.
[236] Article 25(b) of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979.*
[237] U.S. Department of Justice, *Report on the Investigation into Russian Interference in the 2016 Presidential Election (Mueller Report)*, *Government Publishing Office*, 2019.
[238] Brent Mittelstadt, 'Auditing for Transparency in Content Personalisation Systems', *International Journal of Communication*, 10 (2016), 4991–5002.
[239] Liu.
[240] Mazzoli and Tambini.
[241] Akturan Ulu, 'Green Walk and Green Talk: How Oil Companies Position Themselves in Social Media', in *9th Annual Conference of the EuroMed Academy of Business*, 2016, pp. 51–63.
[242] David Armstrong, 'Inside Purdue Pharma's Media Playbook: How It Planted the Opioid "Anti-Story"', *ProPublica*, 2019 <https://www.fiercepharma.com/pharma/inside-purdue-pharma-s-media-playbook-how-it-planted-opioid-anti-story>.

information can compromise the integrity of public discourse, as users are exposed to a biased selection of content, obscuring the diversity of perspectives and opinions essential for democratic processes to function effectively.

It is also important to consider the growing reliance on social media for information and public discourse and its potential to exacerbate the digital divide. Public discourse on the relationships between social media and politics is often dominated by accounts from developed nations where there is the assumption that most people have adequate access to the internet and social media. This is not necessarily the case in developing nations.[243] Inadequate consideration of digital literacy and access to social media in assumptions about democratic processes poses a significant threat to the human right to participate in the conduct of public affairs. As individuals without access to the internet or digital literacy skills become increasingly excluded from the online public sphere, their ability to participate in public affairs may be significantly diminished.[244] This can lead to further marginalisation of already disadvantaged communities, undermining the principle of "universal and equal suffrage" regarding the participation in the conduct of public affairs[245].

To address threats to the human right to participate in the conduct of public affairs, encompassing both universal and equal suffrage and the free expression of the will of the electors, posed by social media, existing international and domestic legal frameworks for the regulation of social media need to be scrutinised for possible gaps, overlaps, and contradictions – most centrally, the regulatory vacuum with regards to social media content personalisation. Existing legal frameworks should be evaluated for their effectiveness in promoting transparency in algorithmic practices, safeguarding against undue influence from governments and private corporations, and ensuring equal access to online platforms for all individuals, regardless of their socio-economic status or location.

3.5. Undue influence on human right to participate in the conduct of public affairs

The legal concept of 'undue influence' is defined differently, based on the jurisdiction[246]. Mary Joy Quinn, retired Director of the Probate Court at San Francisco Superior Court in San

[243] E. Zhuravskaya, M. Petrova, and R. Enikolopov, 'Political Effects of the Internet and Social Media.', *Annual Review of Economics*, 12 (2020), 415–38.
[244] M.E. Susilo, S. Afifi, and S. Yustitia, 'Hoax as a Reflection on the Low Digital Literacy in Indonesia', in *2nd International Conference on Social, Economy, Education and Humanity*, 2019, pp. 165–74.
[245] Article 25(b) of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979.*
[246] Stacey Wood and Pi Ju Liu, 'Undue Influence and Financial Capacity: A Clinical Perspective', *Generations*, 36.2 (2012), 53–58.

Francisco, CA, frames the concept of 'undue influence' as a growing problem that has been consistent only in its ability to elude definition within the US legal system. Quinn asserts that the diverse circumstances in which undue influence may manifest are central to the difficulty of legislating a comprehensive definition. In an effort to provide a structured framework for evaluating undue influence, the state of California has introduced legal tests, related to victim vulnerability, the influencer's apparent authority, tactics employed by the influencer, and the equity of the result.[247] Existing case law such as the Matter of the Probate of the WILL of Katherine WALTHER, Deceased, 159 N.E.2d 665, 6 N.Y.2d 49, 188 N.Y.S.2d 168 (NY Ct. App. 1959)[248] and the Matter of Lewis, 2018 NY Slip Op 50599(U) (Sur. Ct. Kings Cty. 2018)[249] in the state of New York, and In re Carpenter's Estate, 253 So. 2d 697, 702 (Fla. 1971)[250] and *Hack v Janes*, 878 So.2d 440, 443 (Fla. Dist. Ct. App. 2004)[251] in the state of Florida, suggest that other considerations such as the relationship between the parties, the opportunity for exertion of influence, the motive to unduly influence, the actual exertion of influence, and extenuating circumstances have also been considered to be material in US cases of alleged undue influence.

Defining undue influence, also referred to as inappropriate- or illegitimate influence, within European Union (EU) legal systems is as complex as it is in the US, owing to the greater diversity in legal frameworks, principles, and jurisprudence across member states. As a consequence, a uniform legal definition of undue influence remains elusive at the supranational level.[252] One area where undue influence has been addressed in EU law is in the context of the Unfair Commercial Practices Directive, which aims to protect consumers from unfair business-to-consumer commercial practices, including those that involve the exertion of undue influence[253]. This Directive provides a non-exhaustive list of unfair commercial practices, defining undue influence as "exploiting a position of power in relation to the consumer so as to apply pressure, even without using or threatening to use physical force, in a way which

[247] Joy Mary Quinn, 'Defining Undue Influence: A Look at the Issue and at California's Approach', *BIFOCAL: A Journal of the ABA COmmission on Law and Aging*, 35.3 (2014), 72–75.
[248] 'The Matter of the Probate of the WILL of Katherine WALTHER, Deceased', *159 N.E.2d 665, 6 N.Y.2d 49, 188 N.Y.S.2d 168, NY Ct. App.*, 1959.
[249] 'The Matter of Lewis', *2018 NY Slip Op 50599(U), Sur. Ct. Kings Cty.*, 2018.
[250] 'In Re Carpenter's Estate', *253 So. 2d 697, 702, Fla.*, 1971.
[251] 'Hack v Janes', *878 So.2d 440, 443 (Fla. Dist. Ct. App.)*, 2004.
[252] Antunes T, 'Artificial Intelligence as an Undue Influence in Criminal Trials: Issuing the Use of Algorithms under the Principle of Independence of Judges in Europe', in *Artificial Intelligence from the Perspective of Law and Ethics: Contemporary Issues, Challenges and Perspectives* (Košice, Slovakia, 2022).
[253] Luis González Vaqué, 'Directive 2005/29/EC on Unfair Commercial Practices and Its Application to Food-Related Consumer Protection', *European Food and Feed Law Review*, 10.3 (2015), 210–22.

significantly limits the consumer's ability to make an informed decision"[254]. However, the scope of this definition is limited in to consumer protection and does not address the broader contexts in which undue influence may occur.

When assessing undue influence within domestic legal systems, EU member states use civil law[255], common law[256], and mixed legal frameworks[257] to engage with similar challenges as those encountered in the United States. In many European jurisdictions, the factors considered in determining undue influence often encompass elements such as the nature and extent of the influence[258], the vulnerability of the influenced party[259], the degree of dependence or trust between the parties[260], and the fairness of the outcome[261]. For example, the French Civil Code contains a provision that "should a constraint exploit a party's state of dependence and obtain an undertaking to which said party would not have agreed in the absence of such constraint, and gains from it a manifestly excessive advantage" it would constitute illegitimate influence by virtue of a defect in consent and serve as grounds to nullify a contract[262]. Similarly, the concept of undue influence is not explicitly codified within Germany's legal system, however, there are legal institutions that serve similar functions and purposes as undue influence. For example, the German Civil Code contains a provision that any "legal transaction exploiting the predicament, inexperience, lack of judgment or considerable weakness of will of another" is void[263]. Conversely, in the common law jurisdiction of the United Kingdom (UK), a significant body of case law addressing undue influence exists. These include high profile cases such as *Lloyds Bank v Bundy* (1975)[264], where Lloyds' fiduciary duty of care was breached resulting in

[254] Article 2(j) of European Council, 'Unfair Commercial Practices Directive', *2005/29/EC, Adopted 11 June 2005* <https://doi.org/10.1007/978-3-540-71882-6_7>.
[255] Pierre-Henri Conac, Luca Enriques, and Martin Gelter, 'Constraining Dominant Shareholders' Self-Dealing: The Legal Framework in France, Germany, and Italy', *European Company and Financial Law Review*, 4.4 (2007), 491–528 <https://doi.org/10.1515/ecfr.2007.025>.
[256] M. R. Haberfeld, Joseph F. King, and Charles Andrew Lieberman, 'The United Kingdom and Ireland', in *Terrorism Within Comparative International Context*, 2009, pp. 39–59.
[257] Michael Milo and Jan Smits, 'Trusts in Mixed Legal Systems: A Challenge to Comparative Trust Law', *European Review of Private Law*, 8.3 (2000), 421–26 <https://doi.org/10.54648/273248>.
[258] Ildefonso Hernández-Aguado and Elisa Chilet-Rosell, 'Pathways of Undue Influence in Health Policy-Making: A Main Actor's Perspective', *Journal of Epidemiology and Community Health*, 72.2 (2018), 154–59 <https://doi.org/10.1136/jech-2017-209677>.
[259] Peisah C, Finkel, CS, Shulman K, Melding P, Luxenberg J and Heinik J, 'The Wills of Older People: Risk Factors for Undue Influence', *International Psychogeriatrics*, 21.1 (2009), 7–15 <https://doi.org/10.1017/S1041610208008120>.
[260] Andrew P. Bell, 'Abuse of a Relationship: Undue Influence in English Law and French Law', *European Review of Private Law*, 15.4 (2007), 555–99 <https://doi.org/10.54648/erpl2007030>.
[261] R.J. Scalise, 'Undue Influence and the Law of Wills: A Comparative Analysis', *Duke Journal of Comparative International Law*, 19 (2008), 41–106.
[262] Article 1143 of the Corps législatif, 'Code Civil [Civil Code], République Française', 1804.
[263] § 138(2) of the Deutscher Reichstag, 'Bürgerliches Gesetzbuch [Civil Code], Bundesrepublik Deutschland.', *Enacted on 18 August 1896*.
[264] 'Lloyds Bank Ltd v Bundy', *[1975] QB 326*.

undue influence, and *Royal Bank of Scotland v Etridge* (2001)[265], where the House of Lords provided guidance on the issue of undue influence in the context of joint property transactions.

For all the heterogeneity in approaches to defining undue influence across different jurisdictions, domestic legal frameworks appear to converge on the themes of intention to exploit, inequity in outcomes, and restrictions placed on one's capacity to make one's own decisions. These common themes speak directly to the right to self-determination as an implicit aspect of several provisions of the UDHR, including Article 1, which recognises individual autonomy[266], Article 18, which recognises the right to freedom of thought[267], and Article 19, which recognises the right to freedom of opinion and expression[268].

The ability to express one's free will in the participation in the conduct of public affairs by universal and equal suffrage is contingent upon individuals having access to balanced and diverse information, a transparent and accountable public sphere, and an environment free from undue influence[269]. In the context of social media content personalisation, various factors have been identified that can undermine the full realisation of this right, as they create opportunities for undue influence on public opinion and political processes[270].

Undue influence, therefore, as intentional exploitation to achieve inequitable outcomes[271] offers a pragmatic means of determining whether a person or group's right to self-determination has been compromised. Furthermore, since self-determination is fundamental for exercising the right to participate in the conduct of public affairs by universal and equal suffrage, the concept of undue influence could be deployed as a proverbial Swiss Army Knife to examine diverging legal frameworks for their adequacy to protect against human rights infringements at the hands of social media content personalisation practices.

3.6. International human rights enforcement mechanisms

The ICCPR, which protects the human right to participate in the conduct of public affairs, is an international 'hard law' instrument. Under Article 2(3)(a), it is accompanied by enforcement mechanisms, requiring each state party to ensure that any person whose rights or freedoms as

[265] 'Royal Bank of Scotland Plc v Etridge', *(No 2), [2001] UKHL 44 (Oct. 11, 2001)*.
[266] Article 1 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948.*
[267] Article 18 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948*.
[268] Article 19 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948*.
[269] R. Briffault, *Dollars and Democracy: A Blueprint for Campaign Finance Reform* (New York: Fordham University Press, 2020).
[270] Fay Niker, Peter B. Reiner, and Gidon Felsen, 'Perceptions of Undue Influence Shed Light on the Folk Conception of Autonomy', *Frontiers in Psychology*, 9 (2018), 1–11 <https://doi.org/10.3389/fpsyg.2018.01400>.
[271] Rick Bigwood, 'Undue Influence: "Impaired Consent" or "Wicked Exploitation"?', *Oxford Journal of Legal Studies*, 16.3 (1996), 503–15.

recognised under the Covenant are violated shall have an effective remedy[272]. One of the primary mechanisms is the individual complaints procedure established under the first Optional Protocol to the ICCPR. This mechanism allows individuals, as well as advocacy groups acting on their behalf, to submit written communications to the UN *Human Rights Committee* (UNHRC).[273] Before submitting a complaint, domestic remedies must be exhausted, meaning that the individual or group has pursued all available legal avenues within their own country to seek redress[274]. Claims brought to the Committee prior to any legal proceedings before the appropriate domestic courts, are wholly rejected[275]. The UNHRC then examines the communication and issues a report on the matter[276], which may include recommendations for remedial actions to be taken by the state party[277]. Under Article 4 of the Optional Protocol, the state party is required to submit written statements clarifying the matter and any subsequent remedy to the UNHRC within six months[278]. The UNHRC's findings regarding claims of human rights violations are not binding in itself, and it thus primarily relies on diplomatic and political pressure to encourage state parties to comply with its recommendations[279].

Another mechanism for redress is the Universal Periodic Review (UPR) process, a peer-review system under the auspices of the UNHRC. The UPR assesses the human rights situation in all UN member states every four to five years, providing an opportunity for states to report on their human rights achievements and challenges. During the UPR process, other states can pose questions, make recommendations, and share best practices to improve the human rights situation in the country under review. Civil society organisations can also submit information and engage in advocacy efforts.[280] While the UPR is a valuable tool for monitoring the status of human rights globally and fostering dialogue, the process relies on the voluntary commitment of state parties to implement the suggested changes[281]. Pressure and scrutiny from

[272] Article 2(3)(a) of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979*.
[273] Article 1 of the UN General Assembly, 'Optional Protocol to the International Covenant on Civil and Political Rights'.
[274] Article 2 of the UN General Assembly, 'Optional Protocol to the International Covenant on Civil and Political Rights'.
[275] UNHRC, 'Italy Failed to Rescue More than 200 Migrants, UN Committee Finds', *Office of the United Nations High Commissioner for Human Rights*, 2021.
[276] Article 3 of the UN General Assembly, 'Optional Protocol to the International Covenant on Civil and Political Rights'.
[277] Article 4(1) of the UN General Assembly, 'Optional Protocol to the International Covenant on Civil and Political Rights'.
[278] Article 4(2) of the UN General Assembly, 'Optional Protocol to the International Covenant on Civil and Political Rights'.
[279] Gino Pauselli, Francisco Urdinez, and Federico Merke, 'Shaping the Liberal International Order from the Inside: A Natural Experiment on China's Influence in the UN Human Rights Council', *SSRN Electronic Journal*, 2022 <https://doi.org/10.2139/ssrn.4299087>.
[280] Elvira Domínguez Redondo, 'The Universal Periodic Review of the UN Human Rights Council: An Assessment of the First Session', *Chinese Journal of International Law*, 7.3 (2008), 721–34.
[281] F. Cowell, 'Understanding the Legal Status of Universal Periodic Review Recommendations', *Cambridge International Law Journal*, 7.1 (2018), 164–84.

other UN member states[282] and influential civil society organisations[283] has been found to be instrumental in facilitating the implementation of UPR recommendations. This enforcement framework has mixed results in protecting human rights at an international level. For example in the case of *Horvath v Australia* (2009), the UNHRC found that following an unlawful police raid, the rights provided for under Articles 2(a), 7, 9(1), and 17(1) were violated[284] and required the state to provide adequate compensation, to take steps to prevent similar violations, and to review its legislation to ensure conformity with the requirements of the Covenant[285], with which the Australian government to a large extent complied[286]. Conversely, in the case of *Yevdokimov and Rezanov v Russian Federation* the UNHRC found that the state party was in violation of Article 25 alone and in conjunction with Article 2(3) of the ICCPR[287], depriving the authors of their right to vote, and required the state party to amend its legislation to comply with the Covenant[288]. In subsequent communications, the state party responded to claims by the author and stated that claims were not supported by sufficient evidence and thus lacked merit both procedurally and substantively[289].

Therefore, while enforcement mechanisms exist, protecting human rights at an international level appears to not be without its challenges. Most notably, not all UN member states are party to the relevant international human rights instruments, such as the ICCPR[290] and the first Optional Protocol[291]. Additionally, as demonstrated by international case law, even parties to the ICCPR and the first Optional Protocol might not recognise the outcomes and recommendations of the UNHRC. Furthermore, the key requirement for exhausting all domestic remedies can be a lengthy and resource-intensive process, potentially discouraging individuals from pursuing their claims at the international level[292]. What emerges from a consideration of the benefits and limitations of enforcement mechanisms is that, at an

[282] Edward McMahon and Marta Ascherio, 'A Step Ahead in Promoting Human Rights? The Universal Periodic Review of the UN Human Rights Council', *Global Governance*, 18.2 (2012), 231–48 <https://doi.org/10.1163/19426720-01802006>.
[283] Lawrence C. Moss, 'Opportunities for Nongovernmental Organization Advocacy in the Universal Periodic Review Process at the UN Human Rights Council', *Journal of Human Rights Practice*, 2.1 (2010), 122–50 <https://doi.org/10.1093/jhuman/hup031>.
[284] Paragraph 8.8 of 'Horvath v Australia', *No. 1885/2009, U.N. Doc. CCPR/C/110/D/1885/2009.*
[285] Paragraph 10 of 'Horvath v Australia'.
[286] 'Horvath v Australia (HRC, 2014)', *Remedy Australia*.
[287] Paragraph 8 of 'Yevdokimov and Rezanov v Russian Federation', *CCPR/C/101/D/1410/2005.*
[288] Paragraph 9 of 'Yevdokimov and Rezanov v Russian Federation'.
[289] 'Views Adopted by the Committee under Article 5(4) of the Optional Protocol, Concerning Communication No. 2059/2011', *CCPR/C/116/D/2059/2011*.
[290] United Nations, 'Parties to the International Covenant on Civil and Political Rights'.
[291] United Nations Treaty Collection, 'Parties to the First Optional Protocol to the International Covenant on Civil and Political Rights', *Available at: Https://Treaties.Un.Org/Pages/ViewDetails.Aspx?Src=IND&mtdsg_no=IV-5&chapter=4&clang=_en (Accessed on 13 June 2022)* (United Nations Treaty Collection, 2022).
[292] Alice Storey, 'Challenges and Opportunities for the United Nations' Universal Periodic Review: A Case Study on Capital Punishment in the United States', *UMKC Law Review*, 90.1 (2020), 129–52.

international level, the protection of human rights relies heavily on cooperation between states, international organisations, and civil society, rather than on strict enforcement mechanisms as typically seen within domestic legal systems. The central value of the UNHRC and processes such as the UPR, is to serve as persuasive guidance and a catalyst for collaborative efforts towards advancing the rights to self-determination and the participation in public affairs.

3.7. International cyber law

The existing international cyber law landscape and its potential to address the implications of social media content personalisation in relation to Article 25(b) of the ICCPR is complex with multiple, sometimes conflicting, layers of jurisdiction, enforcement, and differing levels of specificity and inclusivity. Cognisant of the multifaceted and complex nature of cybercrime, the UN has taken steps towards a comprehensive international convention aimed at combating this growing menace. Through decision 74/567 of 14 August 2020, the General Assembly established an open-ended ad hoc intergovernmental committee of experts to expand the mandate of the United Nations Office on Drugs and Crime (UNODC) with the development of a comprehensive international convention on cybercrime[293]. Commencing with the organisational sessions in May 2021[294], and again in February of 2022[295], the committee instituted a procedural and logistical framework for the substantive deliberations that were to follow. During the first[296] and second[297] session, in March and June of 2022 respectively, delegates deliberated upon proposed provisions regarding nominal rules and offences, including the development of a legal framework that aims to encompass the diverse range of illicit activities enabled by digital technology. The necessity for international cooperation, preventive measures, and technical assistance to bolster the global capacity to counter

[293] General Assembly, 'Decision 74/567 on Establishing an Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes', *A/74/L.84, Adopted in New York on 14 August 2020*.
[294] United Nations Office on Drugs and Crime, 'Logistical and Procedural Information for the Holding of the Organizational Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes', *A/AC.291/CRP.3, Adopted 12 May 2021* <https://coronavirus.health.ny.gov/covid-19-travel-advisory;>.
[295] General Assembly, 'Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on Its Session on Organizational Matters', *A/AC.291/6, Adopted in New York on 24 February 2022* <www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-session->.
[296] General Assembly, 'Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on Its First Session', *A/AC.291/7, Adopted in New York on 11 March 2022* <www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.>.
[297] General Assembly, 'Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on Its Second Session', *A/AC.291/10, Adopted in Vienna on 27 June 2022* <www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home>.

cybercrime was also discussed. Over the course of the third[298] and fourth[299] sessions, in September 2022 and January 2023, discussions centred around mechanisms of implementation, considering the viability and effectiveness of different enforcement strategies, balancing the preservation of individual rights with the need for robust legal intervention. During the most recent session in April of 2023, a new methodology for conducting the Committee's work was adopted, facilitating broader stakeholder engagement and ensuring a more collaborative approach to the convention drafting process[300]. The current status of the UN Cybercrime Treaty is ongoing, and in the draft negotiation phase, with the concluding session being planned for February of 2024[301].

While the UN's efforts towards a comprehensive cybercrime convention is a significant step in shaping the international cyber law, it's important to note other landmark work in this sphere. One such precedent, which has been instrumental in influencing the dialogue around international cyber law, is the Budapest Convention on Cybercrime. This regional instrument was adopted by the Council of Europe in 2001, and has since attained a quasi-global status, having been ratified by many countries outside of the European region[302]. The Convention stands as one of the earliest and most influential international treaties focused on internet and computer crime, aiming to harmonise national laws and foster international cooperation[303]. The Convention is structured around several key areas, namely substantive law, procedural law, jurisdiction, and international cooperation. Under its provisions on substantive law, the Convention defines a range of cybercrimes, setting a baseline for harmonisation across national legislations[304]. Procedural law provisions aim to equip member states with the necessary investigative tools for the detection, investigation, and prosecution of such offences[305]. Its

[298] General Assembly, 'Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on Its Third Session', *A/AC.291/14, Adopted in New York on 9 September 2022* <www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_third_session/main.html>.
[299] General Assembly, 'Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on Its Fourth Session', *A/AC.291/17, Adopted in Vienna on 2 February 2023* <www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fourth_session/main.html.>.
[300] General Assembly, 'Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes Fifth Session', *A/AC.291/L.10, Adopted in Vienna on 21 April 2023* <www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/Revised_meth>.
[301] United Nations Office on Drugs and Crime, 'Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes', *Meetings of the Ad Hoc Committee*, 2023 <https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home> [accessed 28 May 2023].
[302] Alexander Seger, 'The Budapest Convention 10 Years on: Lessons Learnt', in *Cybercriminality: Finding a Balance between Freedom and Security*, ed. by Stefano Manacorda, Roberto. Flor, and Joon Oh. Jang (Courmayeur: ISPAC, 2012), pp. 167–78.
[303] Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation', *Monash University Law Review*, 40.3 (2014), 698–736 <http://www.youtube.com/yt/press/statistics.html>.
[304] Chapter II, Section 1 of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[305] Chapter II, Section 2 of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.

jurisdictional provisions, in turn, allow for a broad scope of application of the convention within domestic legal frameworks[306]. Given the borderless nature of cybercrime, the Convention also emphasises the imperative of international cooperation, and contains extensive provisions for swift assistance between member states in relation to both investigations and legal proceedings[307]. Yet, despite its wide acceptance as a cornerstone for combating cybercrime, the Budapest Convention has also faced substantial criticism, most notably from civil liberties advocacy groups. For example, the American Civil Liberties Union (ACLU) contends that the Convention insufficiently safeguards privacy rights, and could lead to misuse by governments, thereby infringing upon the civil liberties protected under international human rights instruments such as the ICCPR[308].

While notably the first international treaty seeking to address cybercrime, the Budapest Convention, does not create an enforcement body akin to the UN Human Rights *Council*[309] or a treaty-monitoring body like the *Human Rights Committee*[310] for the ICCPR. Rather, its enforcement relies on the implementation and enforcement of its provisions by the signatory states themselves[311]. The convention's provisions on international cooperation are also central to its enforcement, which includes measures ranging from information sharing[312] to extradition[313]. While the enforcement of international human rights protections does involve a degree of cooperation between states and international bodies[314], the nature of cybercrime often necessitates a distinct form of international collaboration[315]. Indeed, such is the necessity of international collaboration in addressing cybercrime that a Second Additional Protocol to the Budapest Convention on enhanced cooperation and disclosure of electronic evidence was adopted by the Council of Europe on 12 May 2022[316]. Such hard law developments, embodied in the Second Additional Protocol, reflect a response to ongoing discourse and critique in the

[306] Article 22 of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[307] Chapter III of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[308] American Civil Liberties Union, 'The Seven Reasons Why the Senate Should Reject the International Cybercrime Treaty', 2021 <https://www.aclu.org/other/seven-reasons-us-should-reject-international-cybercrime-treaty> [accessed 27 May 2023].
[309] UNHRC. *Welcome to the Human Rights Council*. *Available at: https://www.ohchr.org/en/hr-bodies/hrc/about-council* (Accessed on 3 May 2022).
[310] United Nations. *Mandate of UN Human Rights*. *Available at: https://www.ohchr.org/en/about-us/mandate-un-human-rights* (Accessed on 3 May 2022).
[311] Article 22 of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[312] Article 27 of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[313] Article 24 of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[314] Moss.
[315] Paragraph 243 of the 'Explanatory Report to the Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[316] Preamble of the 'Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence', *ETS No. 224, Adopted in Strasbourg on 12 May 2022.*

field of international cyber law[317]. This protocol, ratified by 36 states globally[318], specifically enhances cooperation[319], facilitates the disclosure of electronic evidence[320], and enables joint investigations[321], while also providing human rights safeguards, including the right to privacy[322]; through the protection of personal data[323]. Should a breakdown in cooperation among member states occur, Article 45 of the Budapest Convention provides for dispute resolution through the International Court of Justice (ICJ), though this is conditional on mutual recognition of the court's jurisdiction by the parties involved[324] and is, in practice, rarely used due to the ICJ's limited enforcement powers[325] and its inability to adjudicate cases involving non-state actors[326].

While the Budapest Convention and its subsequent protocols represent significant strides in addressing the complexities of cybercrime, they build upon and operate alongside longer-standing frameworks for international cooperation in communications, such as those provided by the International Telecommunication Union (ITU)[327]. As a result of the International Telegraph Conference held in Paris in 1865, the ITU was originally established by 20 European states as the International *Telegraph* Union, tasked with managing intercontinental telegraph infrastructure[328]. Starting out as the first independent international organisation, the ITU was later incorporated as a specialised agency of the UN, where it has continued to dynamically adapt its mandate in response to the rapid advancement of communication technologies[329]. Shaping technical standards and managing the international radio-frequency spectrum to enhance global access to Information and Communication Technologies (ICTs), the ITU's

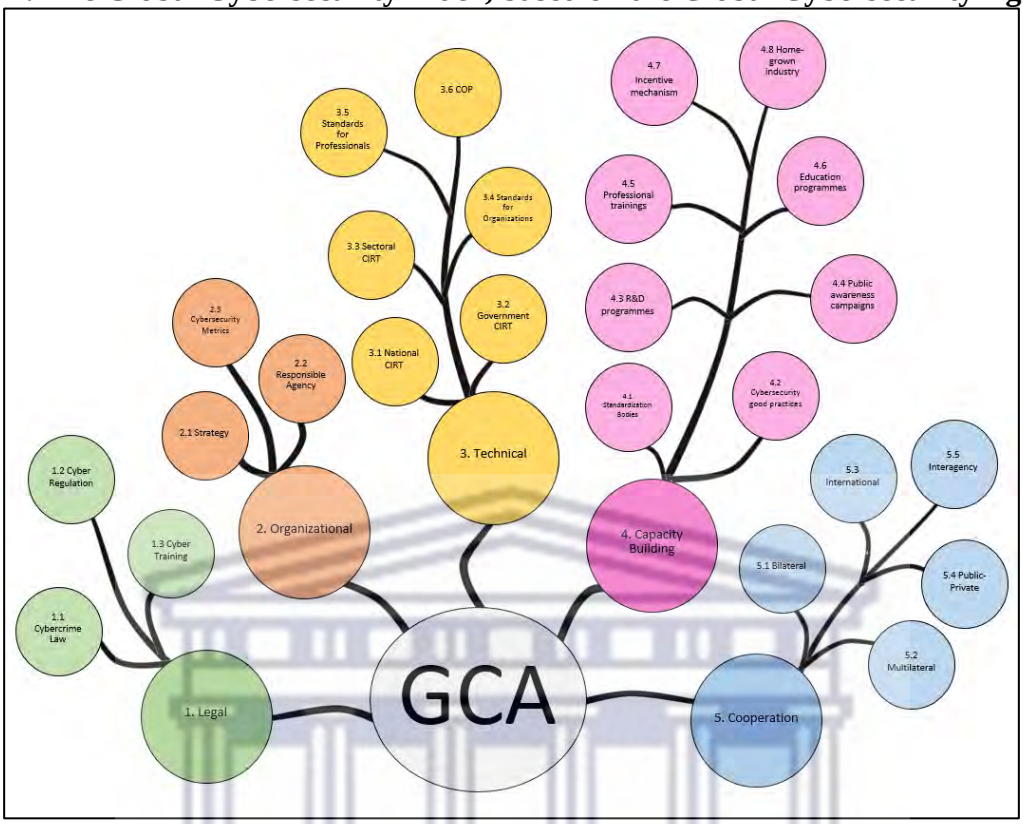
[317] American Civil Liberties Union.
[318] Council of Europe, 'Albania Becomes 36th State to Sign the Second Additional Protocol to Convention on Cybercrime', *News*, 2023.
[319] Article 8 of the 'Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence'.
[320] Article 9 of the 'Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence'.
[321] Article 12 of the 'Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence'.
[322] Article 17 of the 'International Covenant on Civil and Political Rights'.
[323] Article 14 of the 'Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence'.
[324] Article 45 of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[325] Aloysius P. Llamzon, 'Jurisdiction and Compliance in Recent Decisions of the International Court of Justice', *European Journal of International Law*, 18.5 (2008), 815–52 <https://doi.org/10.1093/ejil/chm047>.
[326] G.I. Hernandez, 'Non-State Actors from the Perspective of the International Court of Justice', in *Participants in the International Legal System: Multiple Perspectives on Non-State Actors in International Law*, ed. by J. d'Aspremont (London: Routledge, 2011), pp. 140–64.
[327] Patryk Pawlak, 'Capacity Building in Cyberspace as an Instrument of Foreign Policy', *Global Policy*, 7.1 (2016), 83–92 <https://doi.org/10.1111/1758-5899.12298>.
[328] J. Kniestedt, 'The 1st 20 Years in the Development of the International-Telegraph-Union: Review on the International Telegraph Conference in Berlin in 1885', *Telecommunication Journal*, 55.9 (1988), 610–14.
[329] George A Codding, 'The International Telecommunications Union: 130 Years of Telecommunications Regulation Telecommunications Regulation', *Denver Journal of International Law & Policy*, 23.3 (1995), 501–11 <https://digitalcommons.du.edu/djilp/vol23/>.

primary role remains centred around standardisation and coordination[330], despite lacking enforcement mechanisms akin to international human rights courts or tribunals[331].

One of the more recent initiatives within the ITU is the Global Cybersecurity Agenda (GCA), which was launched in 2007. This strategic framework aims to enhance international cooperation, seeking to engage a wide range of stakeholders, from governments and industry to academia and civil society, in a concerted effort to ensure international digital security. With its comprehensive approach, the GCA addresses numerous aspects including legal measures, technical and procedural standards, organisational structures, capacity building, and, importantly, international cooperation.[332] Building on the five pillars of the GCA – legal measures, technical standards, organisational structures, capacity building, and international cooperation – another initiative by the ITU is the Global Cybersecurity Index (GCI), which specifically assesses the commitment of countries to cybersecurity[333]. By means of a focussed survey, the GCI measures various countries' engagement in these critical areas, drawing on inputs from experts to assign weights, thereby deriving an overall GCI score[334]. Published periodically, the GCI serves as a global reference, providing a nuanced perspective of international cybersecurity commitments. The most recent Index showed that out of the 193 ITU member states, only 20 had passed data protection regulations, four are in a draft stage, and 11 do not have any regulations in place. Conversely, it also indicated that many countries had enacted new cybersecurity regulations to address online safety and privacy.[335]

[330] Eva S. Ferre-Pikal, 'Frequency Standards, Characterization', ed. by Kai Chang, *Encyclopedia of RF and Microwave Engineering* (Hoboken, New Jersey: Wiley-Interscience, 2005), 1720–29 <http://www.mrw.interscience.wiley.com/erfme>.
[331] James J Moylan, 'The Role of the International Telecommunications Union for the Promotion of Peace through Communication Satellites Promotion of Peace through Communication Satellites', *Case Western Reserve Journal of International Law*, 4.1 (1971), 61–78 <https://scholarlycommons.law.case.edu/jilAvailableat:https://scholarlycommons.law.case.edu/jil/vol4/iss1/5>.
[332] Stein Schjølberg, *ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG)* (Geneva, Switzerland, 2007) <http://www.itu.int/osg/csd/cybersecurity/gca/hleg/members.html>.
[333] International Telecommunication Union, 'Global Cybersecurity Index Guidelines for Member States', *ITU/BDT Cyber Security Programme*, Version 0.9 (2019).
[334] International Telecommunication Union, 'GCI Weightage Expert Group Terms of Reference', *ITU/BDT Cyber Security Program*, 2020.
[335] International Telecommunication Union, *Global Cybersecurity Index 2020: Measuring Commitment to Cybersecurity* (Geneva, Switzerland, 2021).

Figure 2: The Global Cybersecurity Index, based on the Global Cybersecurity Agenda



Source: International Telecommunication Union[336]

Beyond its role in establishing the ad hoc committee for the elaboration of a comprehensive international convention on countering the use of ICTs for criminal purposes[337], the UNODC has also been instrumental in assisting member states to implement and enforce existing international and national cyber laws[338]. The organisation's Global Programme on Cybercrime, for example, offers assistance to developing countries, aiming to strengthen their capacity to combat cybercrime effectively[339]. This is achieved through the provision of technical support, training, and guidance in drafting and implementing relevant legislation that aligns with international standards[340]. It also promotes comprehensive and proactive approaches, and the strengthening of international cooperation among the different jurisdictions[341]. Thus, unlike mechanisms that rely solely on international law enforcement agencies or political pressure,

[336] International Telecommunication Union, 'GCI 2017', *ITU-D Cybersecurity*, 2017 <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx> [accessed 19 May 2023].
[337] General Assembly, 'Decision 74/567 on Establishing an Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes'.
[338] Allison Peters and Amy Jordan, 'Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime', *Journal of National Security Law & Policy*, 10 (2019), 487–524 <https://perma.cc/A4YA-X5X6.>.
[339] United Nations Office on Drugs and Crime, 'Global Programme on Cybercrime ', 2023 <https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html> [accessed 30 May 2023].
[340] United Nations Office on Drugs and Crime, 'Promoting Technical Assistance and Capacity-Building to Strengthen National Measures and International Cooperation against Cybercrime', *Resolution 22/8 Adopted on 10 September 2013*.
[341] United Nations Office on Drugs and Crime, 'Strengthening International Cooperation to Combat Cybercrime', *Resolution 22/7 Adopted on 10 September 2013*.

the UNODC operates through a blend of diplomacy, development, and legal aid, enhancing the practical application of cyber law and bolstering the international response to the multifaceted challenges posed by cybercrime[342]. While the UNODC serves in this capacity, there are other key actors also contributing significantly to the enforcement of cyber law at the international level, such as INTERPOL.

The International Criminal Police Organization (INTERPOL) is a multinational body that enables and enhances cooperation between law enforcement agencies of its 194 member states. Established in 1923, its broad mandate covers various forms of transnational crime, including cybercrime.[343] Its Cybercrime Directorate is a functional unit specifically created to tackle the burgeoning issue of cybercrime, offering a distinct yet complementary approach to international cyber law enforcement compared to international human rights law enforcement mechanisms[344].

Unlike the enforcement mechanisms associated with international human rights, which primarily rely on diplomatic and political pressure to ensure compliance with its decisions, INTERPOL's Cybercrime Directorate facilitates international police cooperation, by lending its expertise to national law enforcement agencies, and provides practical support, such as digital forensics, strategic analysis, operational assistance, and capacity building[345]. The INTERPOL Cybercrime Directorate does not contradict or replace existing international, regional or domestic legal frameworks. Rather, it collaborates extensively with the UN[346], the EU[347] and the AU[348], enabling a more coordinated, efficient, and effective global response to borderless cybercrime[349].

Cybercrime and cyber law at the international level are relatively new areas of jurisprudence. Compared to human rights law, the international legal framework for cyber law is less developed and less cohesive but has seen commendable progress in the past few decades.[350]

[342] United Nations Office on Drugs and Crime, *UNODC Strategy 2021 - 2025* (Vienna, 2021).
[343] INTERPOL, 'INTERPOL 1923 – How Our History Started ', 2023 <https://www.interpol.int/en/Who-we-are/INTERPOL-100/1923-how-our-history-started> [accessed 30 May 2023].
[344] Cybercrime Directorate, *National Cybercrime Strategy Guidebook* (Lyon, France, 2021).
[345] Cybercrime Directorate, *Global Cybercrime Strategy* (Lyon, France, 2017).
[346] INTERPOL, 'INTERPOL and the United Nations ', 2023 <https://www.interpol.int/en/Our-partners/International-organization-partners/INTERPOL-and-the-United-Nations> [accessed 30 May 2023].
[347] INTERPOL, 'INTERPOL and the European Union ', 2023 <https://www.interpol.int/en/Our-partners/International-organization-partners/INTERPOL-and-the-European-Union> [accessed 30 May 2023].
[348] INTERPOL, 'INTERPOL and the African Union ', 2023 <https://www.interpol.int/en/Our-partners/International-organization-partners/INTERPOL-and-the-African-Union> [accessed 30 May 2023].
[349] Dirga Agung, 'The Role of Interpol in the Settlement of Cybercrime Cases under the Budapest Convention on Cybercrimes', *International Journal of Global Community*, 5.1 (2022), 49–56.
[350] C. Reed and A. Murray, *Rethinking the Jurisprudence of Cyberspace* (Cheltenham: Edward Elgar Publishing, 2018).

The Budapest Convention's acceptance beyond its original regional boundaries, coupled with the UN's ongoing initiatives towards a comprehensive cybercrime treaty, serves as a testament to a burgeoning consensus at the international level. This accord acknowledges the need for harmonised legal measures to effectively navigate and counter the multifaceted and cross-border challenges posed by cybercrime.[351] Yet, many challenges in achieving such harmonisation persist. The constant advancement of technology continues to introduce new threats and opportunities for abuse, requiring an equally constant evolution and adaptation of laws and regulations[352]. Efforts to shape an international consensus on cybercrime, rooted in a bedrock of cooperation that has proven fundamental to addressing this borderless issue, face multifaceted obstacles. These include the complexities of legal pluralism[353], shifting political dynamics[354], and the enduring friction between security needs and the preservation of individual liberties[355].

3.8. Analysis at international level

In an effort to prevent the Second World War's "barbarous acts which […] outraged the conscience of mankind"[356] from ever happening again, the UDHR serves as a global roadmap for the freedom and equality for all human beings, everywhere. As a 'soft law' instrument, the UDHR requires binding 'hard law' instruments and associated enforcement mechanisms. The ICCPR is one such key binding international treaty, which aims to cultivate a harmonised legal environment among state parties that advances the recognition, safeguarding, and fulfilment of civil and political rights[357]. While becoming firmly established over many decades, these fundamental legal instruments are being increasingly reinterpreted and reanalysed to take into account the unique challenges and opportunities emerging in the digital age[358]. A reading of Article 25 of the ICCPR suggests that meaningful participation in the governance of one's nation significantly influences the realisation of the freedom and equality envisioned by the UDHR[359]. Consequently, the right to engage in the conduct of public affairs through universal

[351] Tatiana Tropina, 'Cybercrime: Setting International Standards', in *Routledge Handbook of International Cybersecurity*, ed. by Eneken Tikk and Mika Kerttunen (Oxon: Routledge, 2020), pp. 148–60.
[352] Adam Kavon Ghazi-Tehrani and Henry N. Pontell, 'Phishing Evolves: Analyzing the Enduring Cybercrime', *Victims and Offenders*, 16.3 (2021), 316–42 <https://doi.org/10.1080/15564886.2020.1829224>.
[353] Lia Yuwannita, 'The Development of Law in The Digital Era Towards Globalization', in *Roceedings from the 1st International Conference on Law and Human Rights* (Jakarta, Indonesia, 2021) .
[354] Gomgom TP Siregar and Sarman Sinaga, 'The Law Globalization in Cybercrime Prevention', *International Journal of Law Reconstruction*, 5.2 (2021), 211–27 <https://doi.org/10.26532/ijlr.v5i2.17514>.
[355] Article 14 of the 'Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence'.
[356] Preamble of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948.*
[357] Preamble of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979.*
[358] Liu.
[359] Article 25(a) of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979.*

and equal suffrage, and in a manner that represents the free expression of the will of the electors, is considered a fundamental component in achieving the aspirations embodied in the UDHR[360].

An examination of social media's role in the modern global political landscape highlights the urgent need for critical assessment of the adequacy of current international legal frameworks in protecting the right to freely express one's will through the participation in the conduct of public affairs by universal and equal suffrage[361]. This necessity is amplified when one considers the complexities and challenges introduced by the digital environment, which demand a more nuanced understanding of rights and responsibilities that emerge from cyberspace[362]. An analysis of the ICCPR and its enforcement through the UNHRC and UPRs in the context of social media content personalisation suggests three interrelated areas of concern, namely the inter-actor interconnectedness of human rights enjoyment, the transnational influence of social media platforms, and the evidentiary challenges posed by the digital sphere.

The first concern is borne of the implicit assumption within the existing framework that the enjoyment of a specific human right by one individual can occur fully and independently of another individual exercising the same right within the jurisdiction of the same state party. The interplay between politics, social media, populism, and phenomena such as stochastic terrorism challenges this assumption[363]. These phenomena, as they manifest in cyberspace, highlight the complexities of interpreting and applying international human rights instruments in the digital age[364]. Stochastic terrorism, for example, involves the dissemination of extremist ideologies that may incite violence, potentially discouraging minority groups from exercising their rights. Algorithmic content personalisation may inadvertently foster political polarisation and social fragmentation that obstruct the free flow of information, limit exposure to differing opinions, and inhibit informed decision-making, all of which are crucial for meaningful participation in the conduct of public affairs. These dynamics, in turn, highlight the necessity for international cyber law to provide clear and robust guidelines for the behaviour of state and non-state actors in cyberspace[365]. Consequently, this complex relationship necessitates a nuanced understanding

[360] Article 25(b) of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979.*
[361] Sunstein.
[362] Nicola Lucchi, 'Internet Content Governance and Human Rights', *Vanderbilt Journal of Entertainment and Technology Law*, 16.4 (2014), 809–56.
[363] Benesch.
[364] Liu.
[365] Philip M. Napoli, 'Social Media and the Public Interest: Governance of News Platforms in the Realm of Individual and Algorithmic Gatekeepers', *Telecommunications Policy*, 39.9 (2015), 751–60 <https://doi.org/10.1016/j.telpol.2014.12.003>.

of the inter-actor interconnectedness of human rights and the potential for interference in their enjoyment in cyberspace.

Another aspect of the existing international framework that warrants attention stems from the assumption that human rights protection can be secured linearly between the individual, the state party, and the UNHRC. The intricacies of international cyber law, including issues of jurisdiction, data sovereignty, and cross-border data flows, within which social media exists[366], challenges this assumption, as the practices of a social media corporation in one jurisdiction can have significant ramifications on human rights in another state party's jurisdiction. This transnational aspect complicates the process of exhausting domestic remedies, as a party who wishes to bring a complaint for the violation of Article 25, may not be situated within the jurisdiction where such remedies are available. The UNHRC has taken some initial steps in this direction, such as the multiple extensions of the mandate[367] of the Special Rapporteur on the right to freedom of opinion and expression[368]. However, the effectiveness of such measures in ensuring the protection of human rights within the context of algorithmic personalisation remains uncertain[369], and thus further reforms are required to adequately address the legal challenges associated with the borderless nature of social media. This emphasises the importance of progressive developments in international cyber law, such as the Second Additional Protocol to the Budapest Convention[370] and the UN's ongoing efforts in developing a comprehensive international convention on cybercrime[371], in shaping these reforms towards ensuring the protection of human rights in the digital age.

Finally, evidentiary challenges posed by the nebulous nature of social media's impact on the enjoyment of human rights, also raise concern. Establishing a direct causal link between algorithmic content personalisation practices and the violation of an individual's right to participate in the conduct of public affairs may be a formidable task for parties wishing to bring a complaint to the UNHRC, given the complexity and borderless nature of the digital sphere. The burden of proof, a cornerstone principle across international legal frameworks, may need to be revisited and adapted to accommodate the unique challenges presented by the internet

[366] Perera et al.
[367] OHCHR, 'Special Rapporteur on Freedom of Opinion and Expression'.
[368] UN General Assembly, 'Resolution on the Special Rapporteur on the Right to Freedom of Opinion and Expression', *A/HRC/RES/43/4, Adopted 30 June 2020* <https://doi.org/10.1017/s0020818300031660>.
[369] Irene Khan, 'Myanmar: Social Media Companies Must Stand up to Junta's Online Terror Campaign Say UN Experts', *Special Rapporteur on the Right to Freedom of Opinion and Expression*, 2023.
[370] Article 14 of the 'Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence'.
[371] General Assembly, 'Decision 74/567 on Establishing an Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes'.

and more specifically social media. Therefore, the complex interplay between global politics and social media exposes the need for existing international legal instruments and their related enforcement mechanisms to be revisited in order to address difficulties in satisfying the burden of proof as a result of the borderless nature of the digital environment.

CHAPTER 4: REGIONAL FRAMEWORK

4.1. Introduction

This chapter considers regional frameworks, and the extent to which they provide effective mechanisms for preventing social media content personalisation from violating Article 25(b) of the ICCPR. More specifically, the chapter presents detailed discussions on how the right to participate in the conduct of public affairs is codified in the European, American and African regions by drawing on regional hard law and soft law instruments, region-focussed legal scholarship and case law. These discussions are then juxtaposed with detailed discussions on developments in cyber law within each of the three regions. These comparisons of human rights and cyber law landscapes then culminate in an analysis at regional level.

4.2. The right to participate in the conduct of public affairs in Europe

In the aftermath of the Second World War, which prompted global human rights developments[372], European nations were also driven to establish regional mechanisms to address their own unique challenges. The devastation of the war, along with longstanding political rivalries, economic disparities, and national animosities, compelled European leaders to seek ways to overcome internal differences and restore Europe's global leadership. This motivation arose in part due to the failure of major inter-war efforts to achieve European unity. Various attempts at European cooperation and integration were initiated, such as the Benelux Customs Union, the Brussels Treaty, and the European Economic Cooperation Convention. Recognising the need for a broader organisation to serve as the centre of West European authority and to express the growing feeling of European unity, the Council of Europe was established in 1949 as an international organisation dedicated to promoting human rights, democracy, and the rule of law in Europe[373]. Comprised of 46 member states, the Council is founded on the Statute of the Council of Europe, which sets out its objectives and establishes its main bodies[374]. It serves as a platform for cooperation and dialogue on matters of human rights protection among European nations, and its work has been instrumental in shaping the development of human rights standards and norms throughout the continent. In accordance with the Statute, the bodies of the Council of Europe are the Committee of Ministers and the Parliamentary Assembly[375]. Furthermore, a landmark human rights treaty, the European

[372] Preamble of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948.*
[373] G.L. Powell, 'The Council of Europe', *International Law Quarterly*, 3.2 (1950), 164–96 <https://heinonline.org/HOL/License>.
[374] Chapter III of the 'Statute of the Council of Europe', *ETS No. 001, Adopted in London on 5 May 1949 in London*.
[375] Article 10 of the 'Statute of the Council of Europe', *ETS No. 001, Adopted in London on 5 May 1949 in London*.

Convention on Human Rights (ECHR), was created in the aftermath of the Second World War[376]. The ECHR was adopted on 4 November 1950 and, as a condition of membership, entered into force on 3 September 1953 by all Council of Europe member states[377]. This treaty has since remained the primary human rights instrument in the region[378].

Section 2 of the ECHR establishes the mechanisms by which the European Court of Human Rights (ECtHR) oversees the enforcement of the ECHR and its Protocols[379]. Most notably, Article 34 of the Convention contains provisioning for the ECtHR to "receive applications from any person, non-governmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties" [380], while Article 35 sets out the admissibility criteria for applications to the ECtHR. These criteria are similar to those set out by Article 2 of the First Optional Protocol to the ICCPR[381], and include the exhaustion of domestic remedies, a six-month time limit after the final domestic decision, and the prohibition of anonymous applications [382].

Aiding the enforcement of the ECHR is the Council of Europe's Committee of Ministers[383]. While the ECtHR is responsible for reviewing and ruling on cases brought before it, the Committee of Ministers supervises the implementation of these rulings. In addition to its role as the principal decision-making body of the Council of Europe, this committee, which is composed of the foreign ministers of all member states, also ensures the effective implementation of ECtHR judgments. If a violation of the Convention is identified by the ECtHR, the Committee of Ministers employs political persuasion and collaboration to ensure member states adopt measures to rectify the situation and prevent future violations. In so doing, the Committee aids in the monitoring of states' compliance with their obligations under the Convention[384].

[376] Jeffrey A. Brauch, 'The Margin of Appreciation and the Jurisprudence of the European Court of Human Rights: Threat to the Rule of Law', *Columbia Journal OfEuropean Law*, 11 (2004), 113.
[377] Council of Europe, '46 Member States', *Administrative Entities*.
[378] J.G. Merrills and A.H. Robertson, *Human Rights in Europe A Study of the European Convention on Human Rights* (Manchester: Manchester University Press., 2022) 311.
[379] Section 2 of the 'European Convention on Human Rights', *CoE Treaty Series 005, Adopted on 4 November 1950* <https://doi.org/10.1017/S0008197300013908>.
[380] Article 34 of the 'European Convention on Human Rights', *CoE Treaty Series 005, Adopted on 4 November 1950* <https://doi.org/10.1017/S0008197300013908>.
[381] Article 2 of the UN General Assembly, 'Optional Protocol to the International Covenant on Civil and Political Rights'.
[382] Article 35 of the 'European Convention on Human Rights', *CoE Treaty Series 005, Adopted on 4 November 1950* <https://doi.org/10.1017/S0008197300013908>.
[383] Daryna V. Abbakumova, 'Procedural Aspects of the Functioning of the Committee of Ministers of the Council of Europe', *Journal of Eastern European Law*, 57.4 (2018), 25.
[384] Olga Benes, 'Implementation of the Rulings of the European Court of Human Rights: The Latest Decisions of the Committee of Ministers', *Studii Juridice Universitare*, 2021, 50.

Protocol No. 1 to the ECHR was adopted as an additional agreement to the Convention due to disagreements among signatories[385]. It consists of three separate rights, regarding the protection of property[386], the right to education[387], and the right to free elections[388]; alongside three additional Articles regarding the application of the Protocol[389]. While the majority of Council of Europe member states have ratified Protocol No. 1, some, such as Monaco and Switzerland, have signed but not yet ratified it[390]. Article 3 of Protocol No. 1 shares a common objective with Article 25 of the ICCPR[391], as both provisions strive to ensure the right to participate in the conduct of public affairs by way of free and fair democratic processes[392]. Under Article 3, states have a positive obligation to create conditions for free and fair elections, and a negative obligation to refrain from interfering with electoral processes[393]. While Article 3 does not mandate a specific electoral system, and grants member states considerable discretion in regulating elections, the free expression of one's will is central, and states are required to provide compelling justifications for denying voting rights to individuals or specific groups of people[394]. Under this protocol, member states, referred to as "High Contracting Parties" in the Convention, are obligated to "hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature"[395]. A reading of the ECHR and its Protocols thus indicates that these instruments and their respective enforcement mechanisms aim to create an environment that promotes free and fair democratic processes that respect the will of the people of Europe.

As part of its broader contributions to the protection of human rights in Europe, the ECtHR has played a pivotal role in the evolution of the right to participate in the conduct of public affairs, the prohibition of discrimination in voting rights, and the standards for free and fair elections.

[385] Harris D, O'Boyle M, Bates E and Buckley C, *Law of the European Convention on Human Rights*, 4th edn (Oxford: Oxford University Press, 2014) 920.
[386] Article 1 of 'Protocol No. 1 to the European Convention on Human Rights and Fundamental Freedoms', *ETS No. 009, Adopted in Paris on 20 March 1952*.
[387] Article 2 of 'Protocol No. 1 to the European Convention on Human Rights and Fundamental Freedoms', *ETS No. 009, Adopted in Paris on 20 March 1952*.
[388] Article 3 of 'Protocol No. 1 to the European Convention on Human Rights and Fundamental Freedoms', *ETS No. 009, Adopted in Paris on 20 March 1952*.
[389] Articles 4 – 6 of 'Protocol No. 1 to the European Convention on Human Rights and Fundamental Freedoms', *ETS No. 009, Adopted in Paris on 20 March 1952*.
[390] Council of Europe Treaty Office, 'Chart of Signatures and Ratifications of Treaty 009' <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=009> [accessed 19 April 2023].
[391] Article 25 of the 'International Covenant on Civil and Political Rights'.
[392] Article 3 of 'Protocol No. 1 to the European Convention on Human Rights and Fundamental Freedoms'.
[393] William A. Schabas, *The European Convention on Human Rights: A Commentary* (Oxford: Oxford University Press, 2015).
[394] Anthea Connolly, Stephen Day, and Jo Shaw, 'The Contested Case of EU Electoral Rights', in *Making European Citizens: Civic Inclusion in a Transnational Context*, ed. by Richard Bellamy, Dario Castiglione, and Jo Shaw (New York: Palgrave Macmillan, 2006), pp. 31–55.
[395] Article 3 of 'Protocol No. 1 to the European Convention on Human Rights and Fundamental Freedoms'.

Key cases in this regard have contributed to a more nuanced understanding of these principles and have exposed areas that may warrant further attention or legal reform. One such example is the case of *Hirst v the United Kingdom* (2005), where it was claimed that the blanket ban on voting rights for prisoners, under Section 3 of the Representation of the People Act 1983[396], violated Article 3 of Protocol No. 1[397]. The ECtHR found that the blanket ban on voting rights for prisoners pursued a legitimate aim, which included preventing crime and enhancing civic responsibility and respect for the rule of law[398]. However, the Court considered the ban to be disproportionate, as it applied to all convicted prisoners, regardless of the nature of their offences or the length of their sentences, and thus violated Article 3 of Protocol No. 1[399]. This discrepancy between the UK's claim of a restricted application of the ban and the ECtHR's assessment of it as a disproportionate measure serves as a starting point for the ongoing debate on the extension of political rights to disenfranchised groups within the European region[400].

Similarly, in *Ždanoka v Latvia* (2006), the applicant challenged her disqualification from running for election, based on her past involvement in the Communist Party, prior to Latvia gaining independence[401]. She argued that this restriction violated Article 3 of Protocol No. 1[402], as well as Articles 10[403] and Article 14[404] of the Convention. The ECtHR held that while the restriction pursued legitimate aims, such as ensuring loyalty to the new democratic system and protecting Latvia's national security[405], the applicant's individual circumstances did not justify an interference with the applicant's rights[406] and thus constituted a violation of Article 3 of Protocol No.1[407]. In this case, *Ždanoka v Latvia* illustrates the challenge of balancing the protection of democratic institutions and the safeguarding of individual rights, in order to ensure the free expression of will through participation in the conduct public affairs by universal and equal suffrage.

In contrast, the landmark case of *Mathieu-Mohin and Clerfayt v Belgium* (1987). In this case, the applicants argued that the manner in which the proportional representation electoral system

[396] Section 3 of the 'Representation of the People Act', 1983 <https://www.legislation.gov.uk/ukpga/1983/2> [accessed 18 April 2023].
[397] §12 of 'Hirst v the United Kingdom', *Application No. 74025/01 (ECtHR)*, 2005.
[398] §69-70 of 'Hirst v the United Kingdom'.
[399] §82 of 'Hirst v the United Kingdom'.
[400] §77-78 of 'Hirst v the United Kingdom'.
[401] Paragraphs 6 – 9 of 'Ždanoka v Latvia', *Application No. 58278/00 (ECtHR)*, 2006.
[402] Paragraph 100 of 'Ždanoka v Latvia'.
[403] Paragraph 130 of 'Ždanoka v Latvia'.
[404] Paragraph 161 of 'Ždanoka v Latvia'.
[405] Paragraph 115 – 118 of 'Ždanoka v Latvia'.
[406] Paragraph 135 – 137 of 'Ždanoka v Latvia'.
[407] Paragraph 175 of 'Ždanoka v Latvia'.

for the Belgian Senate connected different electoral constituencies and affected the allocation of seats violated Article 3 of Protocol No. 1[408].

They argued that such a system fails to ensure the participation in elections by universal and equal suffrage[409]. The Court held that Article 3 imposes both positive obligations on states to facilitate free elections and negative obligations to refrain from interference in the electoral processes[410]. Ultimately the Court found that the Belgian electoral system did not violate Article 3, as the restrictions were proportionate and pursued a legitimate aim[411].

Furthermore, in the case of *Sejdić and Finci v Bosnia and Herzegovina* (2009), the applicants, who were of Roma and Jewish ethnicity, claimed that their country's Constitution[412] and Election Law[413], which only allowed members of the three main ethnic groups (Bosniaks, Croats, and Serbs) to run as candidates in presidential elections, violated Article 3 of Protocol No. 1[414] and Article 14[415] of the Convention. The ECtHR found that the exclusion of the applicants based on their ethnicity constituted discrimination and violated their rights under both provisions[416]. This decision reaffirmed the importance of non-discrimination in the electoral process and has since bolstered ongoing efforts to extend political rights to disenfranchised groups within the European region. These cases demonstrate the region's multifaceted approach to addressing the complexities of individual and people's rights as it pertains to maintaining democratic systems that both provide avenues for participation for all while not infringing on this right for some.

The true value of presenting cases to the ECtHR, however, rests in the extent to which judgements are able to affect real change towards better protections of human rights in the region. The Council of Europe's Committee of Ministers, tasked with monitoring the execution of judgements, employs a range of techniques to engage with member states and ensure compliance with the court's decisions[417]. These may include the initiation of infringement

[408] §29 of 'Mathieu-Mohin and Clerfayt v Belgium', *Application No. 9267/81 (ECtHR)*, 1987.
[409] Stefan Graziadei, 'Democracy v Human Rights? The Strasbourg Court and the Challenge of Power Sharing', *European Constitutional Law Review*, 12.1 (2016), 54–84 <https://doi.org/10.1017/S1574019616000043>.
[410] §47 of 'Mathieu-Mohin and Clerfayt v Belgium'.
[411] §54 of 'Mathieu-Mohin and Clerfayt v Belgium'.
[412] Parliamentary Assembly of Bosnia and Herzegovina, *Constitution of Bosnia and Herzegovina*, 1995.
[413] *Election Law of Bosnia and Herzegovina* (Bosnia and Herzegovina, 2001).
[414] Paragraphs 1 – 5 of 'Sejdić and Finci v Bosnia and Herzegovina', *Application No. 34836/06 (ECtHR)*, 2009.
[415] Paragraph 6 of 'Sejdić and Finci v Bosnia and Herzegovina'.
[416] Paragraphs 43 – 57 of 'Sejdić and Finci v Bosnia and Herzegovina'.
[417] Jonas Christoffersen and Mikael Rask Madsen, *The European Court of Human Rights between Law and Politics* (Oxford: Oxford Academic, 2011).

proceedings[418], the issuance of recommendations or resolutions[419], and the provision of technical assistance in the form of expert advice, capacity-building, or financial support[420]. In certain instances, the Committee's intervention has led to tangible legislative changes. For example, following the judgement in the *Hirst v United Kingdom* case, the UK government engaged in extensive parliamentary debates on prisoner enfranchisement and ultimately introduced the Voting Eligibility (Prisoners) Draft Bill in 2012[421], although it has yet to be fully implemented[422]. Additionally, the *Sejdić and Finci v Bosnia and Herzegovin*a case prompted amendments to the Bosnian Constitution and Election Law, aimed at addressing the identified discrimination[423].

The ECtHR's jurisprudence indirectly impacts region-wide legal systems through its influence on domestic courts, which frequently refer to the Court's body of case law when interpreting and applying human rights standards[424]. For instance, in the case of *R (on the application of Animal Defenders International) v Secretary of State for Culture, Media and Sport* (2008) UKHL 15 brought before the UK House of Lords, the Court considered the compatibility of a UK statutory ban on political advertising with the right to freedom of expression under Article 10 of the Convention[425]. The House of Lords referred to the ECtHR's jurisprudence in cases such as *VgT Verein gegen Tierfabriken v Switzerland* (2001)[426] and *Murphy v Ireland* (2003)[427], ultimately concluding that the ban was a justified interference with freedom of expression, given the legitimate aim of protecting the democratic debate from distortion by:

> "[P]reventing powerful groups from obtaining a competitive political advantage, protecting the formation of public opinion from undue commercial influence,

[418] Fiona De Londras and Kanstantsin Dzehtsiarou, 'Mission Impossible? Addressing Non-Execution through Infringement Proceedings in the European Court of Human Rights', *International and Comparative Law Quarterly*, 66.2 (2017), 467–90 <https://doi.org/10.1017/S002058931700001X>.
[419] A. Føllesdal, B. Peters, and G. Ulfstein, *Constituting Europe: The European Court of Human Rights in a National, European and Global Context (Vol. 2)* (Cambridge, UK: Cambridge University Press, 2013) 284.
[420] Irina Moroianu Zlitescu, 'Towards a Reform of the European Court of Human Rights', *Drepturile Omului*, 1 (2012), 7–12.
[421] Cormac Behan, 'Embracing and Resisting Prisoner Enfranchisement: A Comparative Analysis of the Republic of Ireland and the United Kingdom', *Irish Probation Journal*, 11 (2014), 156–76 <www.oireachtas.ie>.
[422] Section 3 of Parliament of the United Kingdom, 'Representation of the People Act'.
[423] Maja Sahadžić, 'Bosnia and Herzegovina', *The I·CONnect-Clough Center 2018 Global Review of Constitutional Law*, 2019, 28–32.
[424] Christian Djeffal, 'Dynamic and Evolutive Interpretation of the ECHR by Domestic Courts?', in *The Interpretation of International Law by Domestic Courts: Uniformity, Diversity, Convergence*, ed. by Helmut Philipp Aust and Georg Nolte (Oxford: Oxford University Press, 2016) <https://doi.org/10.1093/acprof:oso/9780198738923.001.0001>.
[425] Paragraphs 1 – 2 of 'R (on the Application of Animal Defenders International) v Secretary of State for Culture, Media and Sport', *[2008] UKHL 15 on Appeal from: [2006] EW 3069*, 2008.
[426] Paragraphs 33 – 35 of 'R (on the Application of Animal Defenders International) v Secretary of State for Culture, Media and Sport'.
[427] Paragraph 35 of 'R (on the Application of Animal Defenders International) v Secretary of State for Culture, Media and Sport'.

> bringing about a certain equality of opportunity among the different forces of society, contributing to the independence of broadcasters, and substantially influencing the democratic process of formation of opinion"[428].

Over the course of the last seven decades, the ECtHR has established a system of judicial protection for individuals in Europe and has issued landmark judgments on issues such as freedom of expression, gender equality, religious freedom, and LGBT rights. It has also been instrumental in the development of international human rights law, having established important principles such as the margin of appreciation, the margin of appreciation doctrine, and the principle of subsidiarity[429]. Despite these successes, gaps remain in the enforcement of ECtHR judgments with certain states displaying resistance to the execution of reforms[430]. One of the most notable instances of such resistance, and more specifically as it pertains to participation in the conduct of public affairs, is the UK's ongoing reluctance to amend the Representation of the People (RP) Act, as illustrated by the case of *Hirst v the United Kingdom*[431]. Highlighting the dire nature of this state party's non-execution, in the ECtHR judgment for the case of *Greens and M.T. v the United Kingdom*, the court pointed out that, at the time of the judgment, approximately 2,500 applications concerning Section 3 of the RP Act were pending before the Court. With an estimated 70,000 prisoners serving sentences in the UK, the blanket ban on prisoners' voting rights presents "a threat to the future effectiveness of the Convention system" as a whole[432].

4.3. Cyber law in the European region

The European region has arguably been at the vanguard of worldwide endeavours in the creation and refinement of nuanced legal frameworks pertaining to cyber law. Instruments such as the Budapest Convention of 2001 and its associated Additional Protocols exemplify this commitment[433]. Driven by the rapid evolution of digital technology and the correlated escalation in cyber threats, substantial transformation has transpired since the turn of the

[428] Paragraphs 73 and 76 of 'R (on the Application of Animal Defenders International) v Secretary of State for Culture, Media and Sport'.
[429] Kanstantsin Dzehtsiarou and Vassilis P. Tzevelekos, 'The Conscience of Europe That Landed in Strasbourg: A Circle of Life of the European Court of Human Rights', *European Convention on Human Rights Law Review*, 1.1 (2020), 1–6 <https://doi.org/10.1163/26663236-00101005>.
[430] Joseph Marko and Sergiu Constantin, 'Against Marginalisation', in *Human and Minority Rights Protection by Multiple Diversity Governance: History, Law, Ideology and Politics in European Perspective* (London: Routledge, 2019), pp. 340–95.
[431] 'Hirst v the United Kingdom'.
[432] Section IV(a) of 'Greens and M.T. v the United Kingdom', *Application Nos. 60041/08 and 60054/08 (ECtHR)*, 2010.
[433] Seger.

century[434]. As discussed in earlier sections, the Council of Europe's Budapest Convention transcends geographical limitations, providing a bulwark against cyber-harms not only for European nations, but also on a global scale. A testament to its significance is the ratification of the Convention[435] and its Additional Protocols[436] by many non-European nations. More recently, the European Union's General Data Protection Regulation (GDPR), which came into effect in 2018, represents another remarkable milestone[437].

The GDPR has globally reshaped the conversation around data protection, privacy, and consent. It mandates stringent data protection standards, enshrining principles like the right to be forgotten, data portability, and data minimisation, among others.[438] Article 9 of the GDPR, guards against the processing of personal data that reveals political opinions[439]. One might argue that this provision can be applied to the practice of social media content personalisation, in that such practices exercise undue influence over users which drives online behaviour[440] that, in turn, interferes with users' ability to express their true will[441] regarding matters of public affairs. Article 11 of the GDPR prescribes that data controllers are not to process personal data that no longer requires the identification of a data subject[442], which seems incompatible with social media content personalisation practices that deploy complex algorithms which frequently leverage comprehensive data profiles that the average social media user is not familiar with[443]. Article 18 further also enables users to limit the processing of their data under certain conditions[444], but given the vast amount of data produced by even simple social media use and the expanse of manners in which such data can be applied to content personalisation, this provision seems out of sync with the current realities of social media use. Similarly, the practice of content personalisation, driven by complex algorithms functioning without manual

[434] Preamble of the 'Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence'.
[435] Council of Europe, 'Chart of Signatures and Ratifications of Treaty 185', 2023 <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185> [accessed 30 May 2023].
[436] Council of Europe, 'Chart of Signatures and Ratifications of Treaty 224', 2023 <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224> [accessed 30 May 2023].
[437] Anup Kumar Das, 'European Union's General Data Protection Regulation, 2018: A Brief Overview', *Annals of Library and Information Studies*, 65 (2018), 139–40 <http://www.ifla.org/node/36104>.
[438] He Li, Lu Yu, and Wu He, 'The Impact of GDPR on Global Technology Development', *Journal of Global Information Technology Management*, 22.1 (2019), 1–6 <https://doi.org/10.1080/1097198X.2019.1569186>.
[439] Article 9(1) of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].
[440] Quinn.
[441] Article 3 of 'Protocol No. 1 to the European Convention on Human Rights and Fundamental Freedoms'.
[442] Article 11(1) of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].
[443] Westbrook et al.
[444] Article 18 of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].

human intervention, seems incompatible with Article 22 of the GDPR, which prohibits decisions using user data that are based solely on automated processing[445]. Amongst the wide range of personal data protections, Article 20 stands out as not simply a provision protecting individual rights, but how those individual rights co-exist with public interest[446] – arguably the only piece of substantive regional cyber law that addresses societal impact. With regards to enforcement, the GDPR notably also establishes robust enforcement mechanisms, such as fines of up to 4% of annual global turnover or €20 million for non-compliance[447].

Functioning in tandem with GDPR[448], another significant milestone in the EU's cyber law landscape is the Directive on Security of Network and Information Systems (NIS 2 Directive) of 2016[449]. As the first piece of EU-wide legislation on cybersecurity, the NIS 2 Directive provides legal measures aimed at boosting the overall level of cybersecurity in the EU. Its focus extends beyond data protection, aiming to ensure the security of essential services in critical sectors such as energy, transport, banking, and healthcare, as well as digital service providers like online marketplaces, cloud services, and search engines. The Directive mandates these entities to take appropriate technical and organisational measures to manage the risks posed to their network and information systems, and to report major security incidents to national authorities.[450]

Together, the GDPR and the NIS 2 Directive serve a central function in the enforcement of cyber law within the European region, granting member states' national data protection authorities (DPAs) the mandate to investigate and penalise regulatory infringements. Bolstering this enforcement framework, particularly in instances of cross-border disputes, the European Data Protection Board (EDPB), a regulatory body tasked with ensuring consistent

[445] Article 22(1) of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].
[446] Article 20(3) of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].
[447] Article 83(6) of the 'Regulation 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*, I. 199/1 (2016).
[448] Dimitra Markopoulou, Vagelis Papakonstantinou, and Paul de Hert, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation', *Computer Law and Security Review*, 35.6 (2019), 1–11 <https://doi.org/10.1016/j.clsr.2019.06.007>.
[449] Council of Europe, 'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for the High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and the Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)', *Official Journal of the European Union*, I. 333/80 (2022).
[450] Marie Theres Holzleitner and Johannes Reichl, 'European Provisions for Cyber Security in the Smart Grid – an Overview of TheNIS-Directive', *Elektrotechnik Und Informationstechnik*, 134.1 (2017), 14–18 <https://doi.org/10.1007/s00502-017-0473-7>.

application of data protection rules across the EU, is frequently summoned to adjudicate conflicts and issue binding decisions[451]. These enforcement mechanisms have proved effective, as demonstrated by the significant penalties imposed on major corporations. Notably, France's DPA imposed a €50 million fine on Google in 2019 for GDPR violations.[452] This significant penalty not only emphasises the potential financial implications of non-compliance, but also serves as a reminder of the responsibility digital enterprises bear in preserving individual rights of their users[453]. While these fines levied under GDPR provisions signal a broader message about the necessity of regulatory compliance amidst rapid technological advancement[454], the instrument is not without criticism. Its adoption has faced significant resistance from challenging small and medium enterprises, citing the high costs and complex requirements of implementation.

During the global COVID-19 pandemic, ethical concerns regarding the GDPR being fit for purpose during times of crisis arose, as well as the data privacy dilemmas that result from the use of contact tracing applications and related technologies for the purposes of public health[455]. Furthermore, the disparity in enforcement between different DPAs across the EU has raised concerns regarding both procedural and substantive fairness[456]. Personal data protection advocacy groups have also argued that high-profile fines are inconsequential for tech giants, who simply absorb these into their operational costs, in lieu of compliance[457]. In addition to the aforementioned enforcement mechanisms, the European Court of Justice (ECJ) provides crucial judicial oversight and interpretative authority over EU laws, including cyber law regulations. The ECJ's rulings are instrumental in shaping the implementation and understanding of these laws across the region.[458]

[451] Laima Jančiūtė, 'European Data Protection Board: A Nascent EU Agency or an "Intergovernmental Club"?', *International Data Privacy Law*, 10.1 (2020), 57–75.
[452] Brian Daigle and Mahnaz Khan, 'The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities', *United States International Trade Commission Journal of International Commerce and Economics*, 2020, 1–38 <https://www.usitc.gov/journals.>.
[453] Benesch.
[454] Mani Karthik Suhas Suripeddi and Pradnya Purandare, 'Blockchain and GDPR - A Study on Compatibility Issues of the Distributed Ledger Technology with GDPR Data Processing', in *Journal of Physics: Conference Series* (IOP Publishing Ltd, 2021), MCMLXIV <https://doi.org/10.1088/1742-6596/1964/4/042005>.
[455] Maria Christofidou, Nathan Lea, and Pascal Coorevits, 'A Literature Review on the GDPR, COVID-19 and the Ethical Considerations of Data Protection During a Time of Crisis', *Yearbook of Medical Informatics*, 30.1 (2021), 226–32 <https://doi.org/10.1055/s-0041-1726512>.
[456] Chander A, Abraham M, Chandy S, Fang Y, Park D and Yu I, 'Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation', *Georgetown University Law Center*, 9594 (2021), 1–42 <https://scholarship.law.georgetown.edu/facpub/2374https://ssrn.com/abstract=3827228>.
[457] Douglas Heaven, 'Taking on the Tech Giants', *New Scientist*, 242.3228 (2019), 18–19 <www.newscientist.com/insight>.
[458] Michael Blauberger and Susanne K. Schmidt, 'The European Court of Justice and Its Political Impact', *West European Politics*, 40.4 (2017), 907–18 <https://doi.org/10.1080/01402382.2017.1281652>.

Beyond data protection, the European region has also established dedicated agencies for addressing the broad-ranging issues of cybersecurity and cybercrime. The European Union Agency for Cybersecurity (ENISA), established in 2004 and strengthened by the NIS 2 Directive[459] and the EU Cybersecurity Act of 2019[460], serves as a central coordinating entity in promoting Europe's resilience against cybersecurity threats. ENISA's core mandate includes developing cybersecurity certification frameworks, supporting policy development and implementation, and coordinating responses to large-scale cross-border cybersecurity incidents.[461] In the context of regional enforcement, Europol's European Cybercrime Centre (EC3), established in 2013, functions as a central hub in combating cybercrime within the European Union[462]. The EC3 not only facilitates member states in dismantling and disrupting cybercrime networks but also nurtures a secure cyberspace through its strong commitment to awareness-raising and prevention[463]. Furthermore, it bolsters cybercrime reporting and contributes to cyber law by aiding in the preparation of impact assessments on emerging technologies and associated legislative proposals[464].

Notable case law shapes the region's cyber law landscape. In 2014, the European Court of Justice (ECJ) ruled in *Google Spain v AEPD and Mario Costeja González* that individuals have the right to request search engines to delist information about them under certain conditions, establishing the so-called "right to be forgotten". This landmark ruling stemmed from a case involving a Spanish national, Mario Costeja González, who sought to have certain web pages removed from Google's search results as they referred to an auction notice of his repossessed home, which González contended was resolved and hence irrelevant.[465] The ECJ found in favour of González, stating that under certain circumstances, the data protection rights of an

[459] Paragraph 18 of the 'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for the High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and the Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)'.
[460] Paragraph 4 of the 'Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act)', *Official Journal of the European Union*, I. 151/15 (2019).
[461] W. Gregory Voss, 'The Concept of Accountability in the Context of the Evolving Role of ENISA in Data Protection, Privacy, and Cybersecurity', in *Technocracy and the Law Accountability, Governance and Expertise*, ed. by Alessandra Arcuri and Florin Coman-Kund (London: Routledge, 2021), p. 323.
[462] Laviero Buono, 'Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and the Establishment of the European Cybercrime Centre (EC3)', *New Journal of European Criminal Law*, 3.3 (2012), 332–43.
[463] Ethem Ilbiz and Christian Kaunert, 'Europol and Cybercrime: Europol's Sharing Decryption Platform', *Journal of Contemporary European Studies*, 30.2 (2022), 270–83 <https://doi.org/10.1080/14782804.2021.1995707>.
[464] Tuesday Reitano, Troels Oerting, and Marcena Hunter, 'Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce (J-CAT)', *The European Review of Organised Crime*, 2.2 (2015), 142–54.
[465] Paragraph 14 of Google v. González, 'Judgement of the Court of Justice of 13 May 2014 on the Case of Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González' (C 131/12, p. 21, 2014).

individual can supersede the interest of internet users in having access to that information[466]. In the case of *Delfi AS v Estonia*, the European Court of Human Rights (ECtHR) considered the liability of an internet news portal for offensive comments posted by its readers[467]. In 2014, the Chamber of the ECtHR found that there had been no violation of Article 10 (freedom of expression) of the European Convention on Human Rights, thereby upholding the decision of the Estonian courts that the news portal, Delfi, was liable for the defamatory comments of its readers[468]. Delfi appealed this decision to the Grand Chamber of the ECtHR, but in 2015 the Grand Chamber affirmed the original ruling[469]. This decision has had a significant impact on the legal landscape surrounding online publishers and their responsibility for user-generated content, especially in Europe, but it has also been a subject of criticism, with concerns about its potential to infringe on the human right of freedom of expression within cyberspace[470].

The multi-level, multi-stakeholder approach to cyber law within the European region provides a critical exploration into the intersections of technology, human rights, and societal norms. The GDPR and the NIS 2 Directive mark considerable and recent progress in protecting individuals and organisations in the region from cyber-harms, but also introduce challenges related to enforcement across heterogeneous jurisdictions. While these legal frameworks strengthen personal data protection, they concurrently illuminate tensions between individual rights and broader societal freedoms, especially in the context of social media and content personalisation. Unprecedented situations, such as the global pandemic, further emphasise the need for agile legal frameworks capable of responding to rapidly shifting contexts. As the digital domain transcends regional confines, the imperative for regional collaboration becomes increasingly central to cyber law discourse. Consequently, the successes and shortcomings within the European cyber law landscape offer valuable insights, contributing significantly to the evolution of cyber law globally.

4.4. The right to participate in the conduct of public affairs in the Americas

The Organization of American States (OAS) is a regional organisation with a history dating back to the First International Conference of American States, held in Washington, D.C., from

[466] Paragraph 4 of Google v. González.
[467] L. Brunner, 'The Liability of an Online Intermediary for Third Party Content: The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia ', *Human Rights Law Review*, 16.1 (2016), 163–74.
[468] 'Delfi AS v Estonia', *Application No. 64569/09 (ECtHR)*, 2013.
[469] 'Grand Chamber Case of Delfi AS v Estonia', *Application No. 64569/09 (ECtHR)*, 2015.
[470] Robert Alexy, ' The Responsibility of Internet Portal Providers for Readers' Comments. Argumentation and Balancing in the Case of Delfi AS v. Estonia', in *The Rule of Law in Europe: Recent Challenges and Judicial Responses*, ed. by M. Elósegui, A. Miron, and I. Motoc (Cham: Springer, 2021), pp. 199–213.

October 1889 to April 1890. This conference led to the establishment of the International Union of American Republics, which later evolved into the OAS as it is known today. Officially established in 1948, the OAS aims to promote democracy, human rights, security, and development in the Americas[471]. The OAS is comprised of 35 member states[472] and is founded on the Charter of the Organization of American States, which was signed in Bogotá, Colombia, in April 1948[473]. The Charter sets out the objectives[474] of the organisation and establishes its main bodies. The General Assembly, the Meeting of Consultation of Ministers of Foreign Affairs, and the Permanent Council are among these main bodies, which address the various aspects of the OAS mandate, including human rights[475]. Within the OAS framework, the Inter-American System for the protection of human rights consists of the Inter-American Commission on Human Rights (IACHR)[476] and the Inter-American Court of Human Rights (IACtHR)[477].

The IACHR was initially created in 1959 by a resolution of the Fifth Meeting of Consultation of Ministers of Foreign Affairs and later incorporated into the OAS Charter[478]; its functions and mandate were further defined and expanded by the American Convention on Human Rights (ACHR)[479], which also established the IACtHR[480]. The mandate of the IACHR is to receive, investigate[481], and analyse individual complaints alleging human rights violations[482], as well as to monitor and provide reports regarding human rights conditions among OAS member states[483]. The IACtHR, in turn, is a judicial body that commenced operation in 1979 following the adoption of the ACHR in 1969, responsible for adjudicating cases involving alleged violations of the ACHR[484]. The ACHR, also known as the Pact of San José, remains the primary legal instrument used to promote and protect human rights in the Americas today. However, unlike the Council of Europe, where ratification of the ECHR is a condition of membership,

[471] David Sheinin, *The Organization of American States* (New Brunswick: Transaction Publishers, 1995) 84.
[472] 'OAS Member States' <https://www.oas.org/en/member_states/default.asp> [accessed 25 April 2023].
[473] Josef L. Kunz, 'The Bogota Charter of the Organization of American States', *American Journal of International Law*, 42.3 (1948), 568–89.
[474] Chapter 1 of the 'Charter of the Organization of American States', *No. 1609*, 1948.
[475] Article 53 of the 'Charter of the Organization of American States', *No. 1609*, 1948.
[476] Article 33(a) of the 'American Convention on Human Rights', *No. 17955 Vol. 1144, I-17955, Adopted on 22 November 1969*.
[477] Christina M. Cerna, 'The Inter-American System for the Protection of Human Rights', *Florida Journal of International Law*, 16.1 (2004), 195–212.
[478] Pan American Union General Secretariat of the Organization of American States, 'Fifth Meeting of Consultation of Ministers of Foreign Affairs Santiago, Chile', 1959.
[479] Preamble of the 'American Convention on Human Rights'.
[480] Article 33(b) of the 'American Convention on Human Rights'.
[481] Article 44 of the 'American Convention on Human Rights'.
[482] Article 45 of the 'American Convention on Human Rights'.
[483] Article 42 of the 'American Convention on Human Rights'.
[484] Article 51 of the 'American Convention on Human Rights'.

the OAS does not require ratification of the ACHR for its member states[485]. This difference is particularly noteworthy considering that the United States and Canada, both influential actors within the OAS and major economies in the region, have signed but not ratified the ACHR[486].

Under Article 62 of the ACHR, state parties to the Convention may recognise the Court's jurisdiction to hear cases concerning alleged human rights violations either on a case-by-case basis or as a matter of general jurisdiction[487]. Under Article 61, individuals and groups cannot directly submit complaints to the IACtHR; rather, cases must be referred directly by a state party or by the IACHR[488]. Furthermore, under Article 46(a) complaints to the IACtHR may also only be lodged if it can be demonstrated that domestic remedies have been exhausted[489]. As such, the IACHR plays a central role in facilitating access to human rights protections by investigating individual complaints and deciding whether to refer these to the Court. In instances where the IACtHR determines a violation of the ACHR, it issues binding judgments, adherence and implement of which the IACHR must monitor and report on[490]. Additionally, the OAS General Assembly[491] and the Permanent Council[492] may also contribute to the enforcement of IACtHR judgements within the region. While not directly involved in the adjudication process, these bodies can exert political pressure on member states to uphold their human rights commitments and implement necessary measures to rectify identified issues.

The drafting process of the ACHR began in the 1960s, after the adoption of the UDHR by the UN in 1948[493] and the ECHR by the Council of Europe in 1950[494], during the time when the ICCPR was being developed and finalised[495]. The ACHR was adopted in 1969 and entered into force in 1978[496]. During the drafting process, experts and representatives from OAS member

[485] Rodolfo Piza, 'Coordination of the Mechanisms for the Protection of Human Rights in the American Convention with Those Established by the United Nations', *The American University Law Review*, 30.1 (1980), 167.
[486] Alvaro Paul, 'Controversial Conceptions: The Unborn and the American Convention on Human Rights Recommended Citation', *Loyola University Chicago International Law Review*, 9.2 (2012), 209–47 <http://lawecommons.luc.edu/lucilr/vol9/iss2/2>.
[487] Article 62 of the 'American Convention on Human Rights'.
[488] Article 61 of the 'American Convention on Human Rights'.
[489] Article 46(a) of the 'American Convention on Human Rights'.
[490] Ariel Dulitzky, 'Too Little, Too Late: The Pace of Adjudication of the Inter-American Commission on Human Rights American Commission on Human Right', *Loyola of Los Angeles International and Comparative Law Review*, 35.2 (2013), 131–208.
[491] Cecilia M Bailliet, 'Measuring Compliance with the Inter-American Court of Human Rights: The Ongoing Challenge of Judicial Independence in Latin America', *Nordic Journal of Human Rights*, 31.4 (2013), 477–95 <www.latinobarometro.org/latino/>.
[492] Antônio Augusto Cançado Trindade, 'Compliance with Judgments and Decisions: The Experience of the Inter-American Court of Human Rights: A Reassessment', in *Nigerian Yearbook of International Law*, ed. by Chile Eboe-Osuji and Engobo Emeseh (The Hague: Springer, 2018), pp. 3–16 <http://www.springer.com/series/14355>.
[493] Preamble of the 'Universal Declaration of Human Rights', *217 A (III), Adopted 10 December 1948*.
[494] Preamble of the 'European Convention on Human Rights'.
[495] Preamble of the 'International Covenant on Civil and Political Rights'.
[496] Preamble of the 'American Convention on Human Rights'.

states who were involved in the development of the ACHR drew on various sources, including the UDHR, ECHR, and the draft text of the ICCPR[497]. The influence of these instruments can be seen in the ACHR's text, structure, and scope. In particular, with regard to the right to participate in the conduct of public affairs, the language of Article 23(1)[498] of the ACHR mirrors the provisions of Article 25[499] of the ICCPR exactly. These provisions encompass the following rights:

> "a. To take part in the conduct of public affairs, directly or through freely chosen representatives;
> b. To vote and to be elected in genuine periodic elections, which shall be by universal and equal suffrage and by secret ballot that guarantees the free expression of the will of the voters; and
> c. To have access, under general conditions of equality, to the public service of his country."

Under Article 23 of the ACHR, states have both positive and negative obligations related to the right to participate in the conduct of public affairs[500]. Article 23(1)(a) specifically requires states to facilitate participation in public affairs, either "directly or through freely chosen representatives"[501], which arguably primarily imposes a positive obligation to create the conditions necessary for active participation. Article 23(1)(b) mandates that elections are "genuine, periodic, and conducted through universal and equal suffrage with a secret ballot that guarantees the free expression of the voters' will"[502], from which one might infer both positive and negative obligations. While the positive obligation here would be to ensure proper electoral processes, the negative obligation one might infer is that states must refrain from interfering with these electoral processes, manipulating electoral outcomes, or restricting access to voting for eligible citizens. Furthermore, Article 23(1)(c) imposes the positive obligation upon states to provide access to public services for all citizens, from which one may also infer the negative obligation to refrain from unjustly or arbitrarily excluding certain individuals or groups from accessing public services[503]. Similar to Article 3 of Protocol No. 1 of the ECHR, Article 23 of the ACHR also does not mandate a specific electoral system, but upholds the principles of free will and universal suffrage[504], emphasising the importance of ensuring equal and non-

[497] J. M. Pasqualucci, *The Practice and Procedure of the Inter-American Court of Human Rights* (Cambridge: Cambridge University Press, 2003) <https://doi.org/10.1017/CBO9780511494055.004>.
[498] Article 23(1) of the 'American Convention on Human Rights'.
[499] Article 25 of the 'International Covenant on Civil and Political Rights'.
[500] Laurens Lavrysen, 'Positive Obligations in the Jurisprudence of the Inter-American Court of Human Rights', *Inter-American and European Human Rights Journal*, 7 (2004), 94–115.
[501] Article 23(1)(a) of the 'American Convention on Human Rights'.
[502] Article 23(1)(b) of the 'American Convention on Human Rights'.
[503] Article 23(1)(c) of the 'American Convention on Human Rights'.
[504] Article 23(1)(b) of the 'American Convention on Human Rights'.

discriminatory access to the electoral process for all citizens, regardless of the particular system adopted by the state party.

The IACtHR has significantly contributed to the development and interpretation of the right to participate in the conduct of public affairs in the Americas by addressing critical issues such as the protection of political pluralism[505], transparency in electoral processes[506], and the expansion of voter rights[507]. Through a number of landmark cases, the Court has clarified the scope and content of Article 23 of the ACHR, established standards for free and fair elections, and underscored the importance of ensuring inclusive and meaningful political participation[508]. These jurisprudential advancements have, in turn, provided guidance for OAS member states to align their national legal frameworks with the ACHR, fostering a deeper commitment to democratic principles and human rights across the region[509]. Evidence from case law illustrates these contributions. In the case of *YATAMA v Nicaragua* (2005), the IACtHR's ruling set a landmark legal precedent, guaranteeing the right to political participation for indigenous communities[510]. In this case, the Court held that the exclusion of the indigenous party YATAMA from the 2000 regional elections in Nicaragua violated Article 23 of the ACHR[511], as it restricted the rights of the party's members to participate in public affairs[512]. The Court's decision established that electoral laws and regulations must not unfairly hinder or discriminate against minority or indigenous political groups[513], thereby reinforcing the importance of inclusiveness and pluralism in democratic systems[514]. Similarly, in *Apitz-Barbera et al. ("First Court of Administrative Disputes") v Venezuela* (2008), the IACtHR heard a case involving political discrimination and a violation of the right to political participation *and* freedom of expression[515]. Three Venezuelan public servants had their government employment contracts

[505] Alejandro Fuentes, 'Judicial Interpretation and Indigenous Peoples' Rights to Lands, Participation and Consultation. The Inter-American Court of Human Rights' Approach', *International Journal on Minority and Group Rights*, 23.1 (2016), 39–79 <https://doi.org/10.1163/15718115-02202006>.
[506] Helio Bicudo, 'The Inter-American Commission on Human Rights and the The Inter-American Commission on Human Rights and the Process of Democratization in Peru', *Human Rights Brief*, 9.2 (2002), 18–20 <https://digitalcommons.wcl.american.edu/hrbrief>.
[507] Beth Lyon, 'The Inter-American Court of Human Rights Defines Unauthorized Migrant Workers' Rights for the Hemisphere: A Comment on Advisory Opinion 18', *New YorkUniversity Review of Law & Social Change*, 28.4 (2004), 547–96 <http://www.corteidh.or.cr/Serie_a_ 18_ing.doc>.
[508] Jorge Contesse, 'Contestation and Deference in the Inter-American Human Rights System', *Law and Contemporary Problems*, 79.2 (2016), 123–45.
[509] Lavrysen.
[510] Paragraph 218 of 'YATAMA v Nicaragua', *Serie C No. 127 (IACtHR)*, 2005.
[511] Paragraphs 194 and 202 of 'YATAMA v Nicaragua'.
[512] Paragraphs 216 – 217 of 'YATAMA v Nicaragua'.
[513] Paragraph 225 of 'YATAMA v Nicaragua'.
[514] Paragraphs 211 and 224 of 'YATAMA v Nicaragua'.
[515] Paragraphs 3 – 4 of 'Apitz Barbera et Al. ("First Court of Administrative Disputes") v Venezuela', *Series C No. 182 (IACtHR)*, 2008.

terminated after their names were published in a list of persons who had signed a petition calling for a recall election of then-President of Venezuela, Hugo Chavez[516]. The Court held that the Venezuelan government had abused its power[517], and the dismissal of the public servants constituted retaliation against them for exercising their rights by signing the petition[518]. This constituted a prohibited form of political discrimination[519] and a violation of the public servants' rights to freedom of expression and political participation[520]. Furthermore, in *Castañeda Gutman v Mexico* (2008), the IACtHR examined claims of a violation of Article 23 as a result of Mexico's electoral laws required candidates for presidential elections to be nominated by political parties[521], effectively barring independent candidates from participating in the election[522]. The IACtHR found that Mexico had violated the applicant's political rights under Article 23 by not providing an adequate legal framework guaranteeing the right to participate in government as an independent candidate[523], and ordered major electoral reform in the country[524]. These rulings demonstrate the IACtHR's continued contribution to the evolution of democratic processes in the region and reinforce the importance of states meeting their positive obligations to create the conditions necessary for active political participation and their positive obligations to refrain from unjust or arbitrary interference with such participation.

A central function of the IACtHR is to harmonise domestic law[525]. Therefore, by design, the IACtHR's decisions not only directly affect the parties involved in the cases but also serve as persuasive authority for domestic courts in the region, thereby contributing to the harmonisation and strengthening of human rights protections across the Americas[526]. For example, following the IACtHR's landmark ruling in *Castañeda Gutman v. Mexico* (2008), which ordered Mexico to amend its legislation to allow for independent candidacies, the Mexican Congress approved constitutional amendments in 2011, granting independent

[516] Paragraphs 87 – 88 of 'Apitz Barbera et Al. ("First Court of Administrative Disputes") v Venezuela'.
[517] Paragraph 165 of 'Apitz Barbera et Al. ("First Court of Administrative Disputes") v Venezuela'.
[518] Paragraphs 166 of 'Apitz Barbera et Al. ("First Court of Administrative Disputes") v Venezuela'.
[519] Paragraphs 131 of 'Apitz Barbera et Al. ("First Court of Administrative Disputes") v Venezuela'.
[520] Paragraphs 132 – 280 of 'Apitz Barbera et Al. ("First Court of Administrative Disputes") v Venezuela'.
[521] Paragraph 114 of 'Castañeda Gutman v México', *Serie C No. 184 (IACtHR)*, 2008.
[522] Paragraph 117 – 118 of 'Castañeda Gutman v México'.
[523] Paragraph 172 – 173 of 'Castañeda Gutman v México'.
[524] Paragraph 202 – 218 of 'Castañeda Gutman v México'.
[525] Diego García-Sayán, 'The Inter-American Court and Constitutionalism in Latin America', *Texas Law Review*, 89 (2011), 1835–62 <http://corteidh.or.cr/historia.cfm>.
[526] Azul A. Aguiar-Aguilar, 'Harmonizing National Law with Inter-American Human Rights Law: Evidence from Mexico', *Journal of Human Rights*, 15.4 (2016), 477–95.

candidates the right to run for public office[527]. These changes in domestic law directly stemmed from the IACtHR's decision and have had a lasting impact on the Mexican political landscape[528]. Another example of jurisprudential influence in the region is that of the Peruvian Constitutional Court's 2007 judgment on *Callao Bar Association v Congress of the Republic*. In this case, the Callao Bar Association filed a motion of unconstitutionality against Law No. 28,642, which deemed actions for the protection of constitutional rights inadmissible when challenging decisions of the National Electoral Board. Drawing on the IACtHR's 2005 ruling in *YATAMA v Nicaragua*, among others, the Peruvian Constitutional Court declared the application admissible and emphasised that, as reaffirmed by the IACtHR ruling, no circumstances should allow the disregard of an individual's right to recourse to constitutional procedures when faced with a violation of fundamental rights recognised by the state's Constitution[529]. In addition to civil and criminal cases, the influence of IACtHR jurisprudence in the region can also be seen in legislative consultations and decision-making processes. Recently, in Costa Rica, during consultation regarding proposed amendments to Article 14 of the Municipal Code, Law No. 7794 of 1998, which aimed to limit the indefinite re-election of local authorities, both Article 23 of the ACHR and the IACtHR's ruling in *YATAMA v Nicaragua* was extensively cited. Here, the consultation proceedings did not identify procedural defects in the bill, and a majority decision declared the findings on substantive defects to be non-justiciable. As a result, the Constitutional Chamber of Costa Rica's current ruling is that the constitutionality of the proposed bill remains unresolved[530]. This example of legal reform from Costa Rica further demonstrates the function and contributions of the IACtHR in developing the rule of law in the region and harmonising domestic legal frameworks.

Like its European counterpart, for decades, the IACtHR has played a vital role in the development of the human rights protection system in the Americas, offering rulings on complex issues related to political participation[531], indigenous rights[532], and freedom of expression[533]. The Court has contributed to shaping standards for free and fair elections in the

[527] Víctor Manuel Collí Ek, 'Improving Human Rights in Mexico: Constitutional Reforms, International Standards, and New Requirements for Judges International Standards, and New Requirements for Judges', *Human Rights Brief*, 20.2 (2012), 7–14 <https://digitalcommons.wcl.american.edu/hrbrief>.
[528] Pasqualucci.
[529] García-Sayán.
[530] 'Ruling No. 2022-006119 of the Constitutional Chamber', *File No. 22-001848-0007-CO (Supreme Court of Costa Rica)*, 2022 <https://vlex.co.cr/libraries/jurisprudencia-425> [accessed 25 April 2023].
[531] Collí Ek.
[532] Paragraph 218 of 'YATAMA v Nicaragua'.
[533] Paragraphs 132 and 280 of 'Apitz Barbera et Al. ("First Court of Administrative Disputes") v Venezuela'.

region, emphasising the importance of inclusiveness and pluralism in democratic systems[534]. However, significant challenges persist in the pursuit of the IACtHR, IACHR, and ACHR's vision for human rights in the region. Similar to the execution challenges faced by the ECtHR, certain member states in the region display persistence in their unwillingness to adhere to IACtHR rulings by implementing necessary reforms[535]. Recognising the gravity of state party non-compliance, the IACtHR has enlisted the support of the various bodies within the OAS structure to exert political pressure on member states to uphold their human rights commitments, emphasising the importance of inclusive political processes for all communities[536]. As numerous groups across the region continue to face obstacles in exercising their right to freely express one's will through participation in the conduct of public affairs by equal and universal suffrage[537], the effective enforcement of IACtHR rulings remains critical to safeguard the legitimacy and impact of the Inter-American system as a whole, ultimately fostering the protection of democracy in the region[538].

4.5. Cyber law in the American region

One of the first major steps towards the establishment of a legal framework for cybercrime in the American region was the adoption of the OAS Comprehensive Inter-American Cybersecurity Strategy in 2004. Prompted by rapidly increasing cyber threats, the Strategy was developed to promote a holistic cybersecurity environment among American states[539]. While not legally binding, the Strategy laid the foundation for the development of national cyber law frameworks[540]. In contrast, OAS has the Inter-American Portal on Cybercrime and a related working group, which were developed as part of the process of Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA). The portal's main purpose is to facilitate cooperation and information exchange among government experts from OAS member states with responsibilities in the area of cybercrime or in international cooperation

[534] Fuentes.
[535] Cançado Trindade.
[536] Bailliet.
[537] Cristóbal Rovira Kaltwasser, 'Explaining the Emergence of Populism in Europe and the Americas', in *The Promise and Perils of Populism: Global Perspectives*, ed. by Carlos de la Torre (Lexington: University Press of Kentucky, 2015), pp. 189–227.
[538] Natalia Torres Zuñiga, 'The Image of the Inter-American Court of Human Rights as an Agent of Democratic Transformation: A Tool of Self-Validation', *Araucaria: Revista Iberoamericana de Filosofía, Política, Humanidades y Relaciones Internacionales*, 23.46 (2021), 483–504 <https://doi.org/10.12795/ARAUCARIA.2021.I46.24>.
[539] OAS General Assembly, 'Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity', *AG/RES. 2004 (XXXIV-O/04), Adopted in Washington D.C. on 8 June 2004*.
[540] OAS General Assembly, 'Appendix A: A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity', *AG/RES. 2004 (XXXIV-O/04), Adopted in Washington D.C. on 8 June 2004*.

for its investigation and prosecution[541]. The working group, in turn, promotes the adoption and updating of legislation and procedural measures necessary for the effective prosecution and adjudication of cybercrime among OAS member states[542]. As a hemispheric forum under OAS, REMJA's is to improve justice system efficiency among member states[543] and, in addition to the portal and working group, has been instrumental in the standardisation and enhancement of cyber law practices across the American region[544]. As the primary legislative body, REMJA forms part of the OAS's three-pillar regional cybersecurity framework, along with the Inter-American Committee Against Terrorism (CICTE), and the Inter-American Telecommunication Commission (CITEL)[545].

The CICTE was established in 1999, with the mandate to prevent, combat, and eliminate terrorism through the promotion of multilateral cooperation among member states and the enhancement of institutional capabilities[546]. In 2006 it expanded its mandate into cyberspace with the implementation of its Cybersecurity Program. This program works to strengthen cybersecurity capabilities within the OAS member states through information sharing, developing and disseminating best practices, and promoting capacity-building initiatives in cybersecurity practices and legislation.[547] These developments nearly two decades ago, signal the OAS's proactive commitment to cybersecurity and a cohesive legal and operational response[548]. CITEL, as the development pillar of the regional framework, was established by the OAS in 1994 to promote and develop information and communication technologies (ICTs) throughout the Americas[549]. Nearly three decades later its mission remains to facilitate and coordinate the region's efforts to integrate telecommunications and ICTs into its socio-economic development goals[550]. CITEL accomplishes this by fostering cooperation among the member states, promoting the development of modern, efficient, and universal

[541] Inter-American Portal on Cybercrime, 'Home Portal', 2023 <http://www.oas.org/en/sla/dlc/cyber-en/homePortal.asp> [accessed 18 June 2023].
[542] Inter-American Portal on Cybercrime, 'Working Group', 2023 <http://www.oas.org/en/sla/dlc/cyber-en/grupo-trabajo.asp> [accessed 18 June 2023].
[543] Meeting of Ministers of Justice or Other Ministers or Attorney General of the Americas, 'Document on the REMJA Process (Document of Washington)', *REMJA-VII/Doc.6/08 Rev.4, Adopted in Washington D.C. on 19 May 2021*.
[544] L. Purdon and F. Vera, 'Regional Cybersecurity Approaches in Africa and Latin America', in *Routledge Handbook of International Cybersecurity*, ed. by E. Tikk and M. Kerttunen (London: Routledge, 2020), pp. 234–46.
[545] Belisario Contreras, *OAS Cybersecurity Capacity Building Efforts* (Washington D.C., 2016).
[546] 'Resolution Creating the Inter-American Committee against Terrorism (CICTE)', *AG/RES. 1650 (XXIX-O/99), Adopted in Guatemala City on 7 June 1999* <https://2001-2009.state.gov/p/wha/rls/fs/2006/64283.htm> [accessed 18 June 2023].
[547] Inter-American Committee against Terrorism, *OAS Cybersecurity Program* (Bogotá, 24 March 2006) <www.oas.org/cyber/>.
[548] Contreras.
[549] OAS General Assembly, 'Resolution Establishing the Inter-American Telecommunication Commission (CITEL)', *AG/RES. 1259 (XXIV-O/94), Adopted in Belém on 10 June1994*.
[550] D. Kekić and D. Subošić, 'Inter-American Telecommunication Commission', *Međunarodna Politika*, 63.1148 (2012), 115–28 <http://www.>.

telecommunications infrastructure, and encouraging the adoption of policies and regulations that facilitate digital inclusion and a robust digital economy[551].

In line with the multidimensional and multidisciplinary approach of the Comprehensive Inter-American Cybersecurity Strategy[552], the OAS, in partnership with the Global Cyber Security Capacity Centre of the University of Oxford, and the Inter-American Development Bank (IDB), launched the Cybersecurity Capacity Maturity Model for Nations (CMM) in 2015[553]. This tool sought to assist nations in gauging their preparedness for cybersecurity threats and developing appropriate responses. The CMM offers an invaluable framework to evaluate the maturity of national cyber policies, pinpoint areas of improvement, and identify best practices.[554] Since its launch, the CMM has seen over 120 reviews globally, including contributions from partner organisations such as the World Bank, the ITU, the Commonwealth Telecommunications Organisation, the Oceania Cyber Security Centre (OCSC), and the Cybersecurity Capacity Centre for Southern Africa (C3SA)[555]. Similar to the trajectory of the Budapest Convention, a regional initiative that subsequently gained international recognition and acceptance, the CMM represents a comparable paradigm of global cybersecurity cooperation[556].

As discussed in preceding sections, the Budapest Convention on Cybercrime extends beyond the European region, including several American nations as its signatories. Among OAS member states, Argentina, Brazil, Canada, Chile, Colombia, Costa Rica, Dominican Republic, Panama, Paraguay, Peru, and the United States of America have adopted the convention[557]. Additionally, Ecuador, Guatemala, Mexico, and Trinidad and Tobago are signatories and have been invited to accede to the convention[558]. The OAS itself is an Observer Organisation to the Cybercrime Convention Committee, which oversees the Budapest Convention[559]. In 2013, at

[551] A.C. de Brito, C. Kauffmann, and J. Pelkmans, 'The Contribution of Mutual Recognition to International Regulatory Co-Operation', *OECD Regulatory Policy Working Papers*, 2016.
[552] OAS General Assembly, 'Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity'.
[553] Shigeo Mori and Atsuhiro Goto, 'Reviewing National Cybersecurity Strategies', *Journal of Disaster Research*, 13.5 (2018), 957–66 <https://doi.org/10.20965/jdr.2018.p0957>.
[554] Global Cyber Security Capacity Centre, *Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition* (Oxford, 31 March 2016).
[555] Global Cyber Security Capacity Centre, *Cybersecurity Capacity Maturity Model for Nations (CMM)* (Oxford, March 2021).
[556] L Pace and P. Cornish, 'Cybersecurity Capacity Building', in *The Oxford Handbook of Cyber Security*, ed. by The Oxford Handbook of Cyber Security (Oxford: Oxford University Press, 2021), pp. 463–78.
[557] Council of Europe, 'Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY', *Parties to the Budapest Convention*, 2023 <https://www.coe.int/en/web/cybercrime/parties-observers> [accessed 19 June 2023].
[558] Council of Europe, 'The Budapest Convention (ETS No. 185) and Its Protocols', 2023 <https://www.coe.int/en/web/cybercrime/the-budapest-convention> [accessed 19 June 2023].
[559] Council of Europe, 'Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY'.

their 9th meeting, the Ministers of Justice or other Ministers or Attorney Generals of the Americas (REMJA IX) acknowledged the need for legislative harmonisation and capacity-building in cybercrime and cybersecurity issues[560]. In a declaration adopted during their 11th meeting in 2021 (REMJA XI), the OAS recommended its member states to consider acceding to the Budapest Convention and adopt the necessary legal and other measures for its implementation[561].

Other recent developments in the region's cyber law landscape include the OAS General Assembly passing a resolution on Advancing Hemispheric Security in 2019, emphasising the growing concern over cybercrime threats[562]. This resolution affirmed the OAS's continued commitment among member states to enhance cooperation on cyber matters, laying a solid groundwork for further legal harmonisation in the region[563]. Here, the OAS CICTE has been instrumental in bolstering cybersecurity defences across the Americas[564]. With over 15 years of experience, this committee has emerged as a regional leader in supporting OAS member states in building both technical and policy-level cybersecurity capacities. This has involved initiatives to develop national cybersecurity strategies, establish national Computer Security Incident Response Teams (CSIRTs), and provide tailored technical assistance and training.[565] CSIRTs therefore function as a regional network of entities focussed on the enforcement of national cyber law among OAS member states[566]. Their work also contributes to the development and refinement of cyber law frameworks, based on frontline experience[567]. Furthermore, 2021 saw the establishment of a significant collaborative initiative between the OAS and the Global Forum on Cyber Expertise (GFCE), in the form of the GFCE-OAS Regional Hub[568]. This partnership between the OAS and the Global Forum on Cyber Expertise

[560] Section V(6) of 'Conclusions and Recommendations of REMJA IX', *REMJA-IX//Doc.2/12 Rev. 1, Adopted in Quinto, on 29 November 2012*.
[561] Section B(3) of 'Conclusions and Recommendations to REMJA XI', *REMJA-IX/DOC.2/21 Rev. 1, Held Virtually on 19 May 2021*.
[562] OAS General Assembly, 'Resolution Advancing Hemispheric Security: A Multidimensional Approach', *AG/RES. 2945 (XLIX-O/19), Adopted in Washington D.C. on 28 June 2019*.
[563] B. Contreras and K.A. Barrett, 'Challenges in Building Regional Capacities in Cybersecurity: A Regional Organizational Reflection', in *Routledge Handbook of International Cybersecurity*, ed. by E. Tikk and M. Kerttunen (London: Routledge, 2020), pp. 214–17.
[564] Louise Marie Hurel, 'Beyond the Great Powers: Challenges for Understanding Cyber Operations in Latin America', *Global Security Review*, 2.1 (2022), 21–31 <https://doi.org/10.25148/gsr.2.009786>.
[565] CSIRTAmericas, 'Protecting the Americas in Cyberspace', 2023 <https://csirtamericas.org/es> [accessed 19 June 2023].
[566] K.P. Newmeyer, 'Elements of National Cybersecurity Strategy for Developing Nations', *National Cybersecurity Institute Journal*, 1.3 (2015), 9–19.
[567] Carlos Solar, 'Cybersecurity and Cyber Defence in the Emerging Democracies', *Journal of Cyber Policy*, 5.3 (2020), 392–412 <https://doi.org/10.1080/23738871.2020.1820546>.
[568] GFCE, 'GFCE Latin America and Caribbean (LAC) Meetings 2021', *GFCE-OAS Capacity Building Meeting*, 2021 <https://thegfce.org/events/gfce-latin-america-and-caribbean-lac-meetings-2021/> [accessed 19 June 2023].

(GFCE) reinforces regional collaboration[569], strengthens cyber defence mechanisms[570], and advances cyber law within the region[571].

The intersection of cyber law and human rights law is evident in a significant body of IACtHR case law that deals with matters within the cyber domain. One such case is that of *Escher et al. v Brazil* (2009). This case was heard by the IACtHR, and had a significant impact on laws on surveillance as it pertains to the right to privacy in the region, among others[572]. The applicants alleged violations of Articles 8(1), 11, 16, and 25 of the ACHR[573], due to wiretaps of digital communications of members of rural workers' organisations by the Paraná State Police[574]. The court did not find sufficient evidence for a violation of the right to free trial or right to judicial protection, but found that while the interference with the applicants' right to privacy was not arbitrary[575], the state did not meet the requirement of judicial authorisation[576]. The Court's ruling on this case set an important precedent in the region for cases related to privacy rights in the context of digital communications[577]. More recently, in 2017, *Ríos et al. v Venezuela*, a case involving the right to freedom of expression on the internet, also came before the IACtHR. The case pertained to the actions of Venezuelan government officials following digital broadcasting content produced by Radio Caracas Televisión (RCTV), a private television service in Venezuela. The applicants claimed that between 2001 and 2005, they suffered harassment, persecution, and both physical and verbal attacks for exercising their freedom of thought and expression[578]. In their application, they alleged that government officials committed acts of intimidation and assault against them, and prevented them from covering public demonstrations at the time[579]. The court found that the individual government officials violated the applicants' rights to personal integrity and freedom of thought and expression

[569] Contreras and Barrett.
[570] S. Amazouz, 'Cyber Capacity-Building and International Security', in *Routledge Handbook of International Cybersecurity*, ed. by E. Tikk and M. Kerttunen (London: Routledge, 2020), pp. 201–13.
[571] Digital Development Partnership, *Integrating Cyber Capacity into the Digital Development Agenda* (The Hague, November 2021) <www.digitaldevelopmentpartnership.org.>.
[572] Dahlmann A, Venturini J, Dickow M and Maciel M, *Privacy and Surveillance in the Digital Age: A Comparative Study of the Brazilian and German Legal Frameworks* (Rio de Janeiro, 2015).
[573] Paragraph 3 of 'Escher et Al. v Brazil', *Serie C No. 200 (IACtHR)*, 2009.
[574] Paragraph 2 of 'Escher et Al. v Brazil'.
[575] Article 11(2) of the 'American Convention on Human Rights', *No. 17955 Vol. 1144, I-17955, Adopted on 22 November 1969*.
[576] Paragraph 174 of 'Escher et Al. v Brazil'.
[577] 'Case of Escher and Others v. Brazil: Global Perspective', *Global Freedom of Expression Columbia University*, 2023 <https://globalfreedomofexpression.columbia.edu/cases/case-of-escher-and-others-v-brasil/> [accessed 19 June 2023].
[578] Paragraph 2 of 'Ríos v Venezuela', *Serie C No. 194 (IACtHR)*, 2009 <https://globalfreedomofexpression.columbia.edu/cases/rios-v-venezuela/#:~:text=The>.
[579] Paragraph 66 of 'Ríos v Venezuela'.

under Articles 5[580] and 13[581] of the ACHR. The court also found that the State failed to meet its obligation to guarantee these rights through an effective investigation of the aggressions and statements made by public officials[582]. The court ruled that the State had failed to implement measures to prevent, investigate, and punish the guilty parties and to make appropriate reparations to the applicants[583]. In terms of regional jurisprudence, while the IACtHR and the ECtHR) are structurally and functionally similar for their respective regions, their roles in interpreting and enforcing human rights conventions vary significantly[584]. Among these differences, the IACtHR has developed a relatively limited set of legal precedents, partly due to the ACHR's inception during a period of political upheaval, violence, and economic unrest in the region. Resultantly, the IACtHR's case log consists primarily of applicants alleging first-generation human rights violations by member states.[585]

A review of contemporary sources reveals that developments in cyber law within the American region is a noticeably collaborative undertaking, with a focus on enforcement and cybersecurity, with stakeholders including inter-governmental security committees like the OAS CICTE[586], ministerial justice meetings like REMJA[587], incident response teams like national CSIRTs[588], and collaborative initiatives like the GFCE-OAS Regional Hub[589]. While the European approach appears to be focussed on legislating cybercrime[590] and privacy rights[591], the American region's focus appears to be in cybersecurity capacity building and threat mitigation[592]. This presents an interesting juxtaposition between legalism and pragmatism as both approaches have benefits and limitations depending on which context it is being applied to. While the European region is leading cyber law development[593], and, in doing

[580] Article 5(1) of 'American Convention on Human Rights', No. 17955 Vol. 1144, I-17955, Adopted on 22 November 1969.
[581] Article 13(3) of 'American Convention on Human Rights', No. 17955 Vol. 1144, I-17955, Adopted on 22 November 1969.
[582] Paragraph 69 of 'Ríos v Venezuela'.
[583] Paragraph 416 of 'Ríos v Venezuela'.
[584] Raluca David, 'Comparative Study of Three International Human Rights Systems and Their Enforcement Mechanisms', *SSRN*, 2009 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1566495> [accessed 19 June 2023].
[585] Josiah Wolfson, 'The Expanding Scope of Human Rights in a Technological World — Using the Interamerican Court of Human Rights to Establish a Minimum Data Protection Standard Across Latin America', *University of Miami Inter-American Law Review*, 48.3 (2017), 188–232 <http://repository.law.miami.edu/umialrhttp://repository.law.miami.edu/umialr/vol48/iss3/8>.
[586] 'Resolution Creating the Inter-American Committee against Terrorism (CICTE)'.
[587] Meeting of Ministers of Justice or Other Ministers or Attorney General of the Americas, 'Document on the REMJA Process (Document of Washington)'.
[588] CSIRTAmericas.
[589] GFCE.
[590] Preamble of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[591] Article 5 of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].
[592] Contreras.
[593] Seger.

so, promoting legislative standardisation and harmonisation, a legalist approach is essentially reactive and relies heavily on adjudicative processes that are notorious for being encumbered by bureaucratic inertia[594]. The more pragmatist approach among OAS member states appears superior in its ability to prevent and deter cybercrime proactively and expeditiously[595], but lacks harmonised legal doctrine[596], including but not limited to regional cyber law jurisprudence[597]. Initiatives such as the Comprehensive Inter-American Cybersecurity Strategy and the Cybersecurity Capacity Maturity Model for Nations (CMM) highlight a commitment to understanding and addressing cybersecurity issues at both a national and regional level[598], juxtaposed against the European emphasis on enforcement across diverging national legal frameworks[599]. Similarities between the European and American regions, most notably, include an alignment between the ECtHR and the IACtHR in terms of how security measures are balanced with respect for human rights and civil liberties in the digital sphere[600]. Thus, one could argue that a critical focal point for both European and American regions should be the refinement and dynamic adaptation of their respective cyber law frameworks, necessitated by the ever-shifting contours of cyber threats and the challenge of safeguarding both individual liberties and national security. Specifically, the American region would likely benefit from the development of a unified legal doctrine, thereby ensuring consistency in the interpretation and enforcement of cyber law. Meanwhile, the European region would likely benefit from integrating more pragmatic, adaptive measures to complement its existing comprehensive legal frameworks. The European region might also benefit from an adoption of similar cross-national collaboration efforts, such as the national CSIRTs and GFCE-OAS Regional Hub of the American region.

4.6. The right to participate in the conduct of public affairs in Africa

The Organization of African Unity (OAU) was established in 1963 by 32 African states at the Summit Conference in Addis Ababa, Ethiopia[601]. The creation of the OAU was prompted by

[594] Section IV(a) of 'Greens and M.T. v the United Kingdom'.
[595] GFCE.
[596] J. de Arimatéia da Cruz and N. Godbee, 'Cybercrime Initiatives South of the Border: A Complicated Endeavor', in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, ed. by T Thomas J. Holt and Adam M. Bossler (Cham: Palgrave Macmillan, 2020), pp. 365–84.
[597] Wolfson.
[598] Global Cyber Security Capacity Centre, *Cybersecurity Capacity Maturity Model for Nations (CMM)*.
[599] Article 83(6) of the 'Regulation 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*, I. 199/1 (2016).
[600] Eliza Watt, *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law* (Cheltenham: Edward Elgar Publishing, 2021) 24.
[601] African Union, 'About the African Union' <https://au.int/en/overview> [accessed 6 May 2023].

several factors: the wave of decolonisation that swept through the continent in the mid-1900s, leading to the emergence of newly independent states[602]; the influence of Pan-Africanism, which sought to promote unity and cooperation among African countries[603]; and the need to foster socio-economic development in the face of unique regional challenges[604]. The OAU was founded on the principles of promoting unity and solidarity among African countries, safeguarding their sovereignty and territorial integrity, and accelerating the political and socio-economic integration of the continent[605]. In 2002, the OAU was replaced by the African Union (AU), which aimed to build on the OAU's achievements and incorporate human rights instruments, bodies, and enforcement mechanisms[606]. The evolution of the AU, currently comprised of 55 nations[607], resulted in the adoption of the African Charter on Human and Peoples' Rights (ACHPR)[608], the establishment of the African Commission on Human and Peoples' Rights (African Commission) and the African Court on Human and Peoples' Rights[609]. Since the adoption of the African Charter in 1982, the African Court has undergone several changes in its structure and jurisdiction[610]. In 1998, the Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights was adopted in Ouagadougou, Burkina Faso[611]. In 2003, the Protocol of the Court of Justice of the African Union was adopted in Maputo, Mozambique[612]. Subsequently, in 2004, the Protocol on the Statute of the African Court of Justice and Human Rights replaced the 1998 and 2003 protocols, merging the two courts and establishing the African Court of Justice and Human Rights (ACtJHR)[613].

[602] Victor Osaro Edo and Michael Abiodun Olanrewaju, 'An Assessment of the Transformation Of The Organization of African Unity (OAU) To The African Union (AU), 1963-2007', *Journal of the Historical Society of Nigeria*, 21 (2012), 41–69 <https://about.jstor.org/terms>.
[603] Sonu Trivedi, 'African Unity', *World Affairs: The Journal of International Issues*, 13.1 (2009), 12–30.
[604] N.J. Padelford, 'The Organization of African Unity', *International Organization*, 18.3 (1964), 521–42.
[605] Paul G Adogamhe, 'Pan-Africanism Revisited: Vision and Reality of African Unity and Development', *African Review of Integration*, 2.2 (2008), 1–34.
[606] Osaro Edo and Abiodun Olanrewaju.
[607] African Union, 'Member States', 2023 <https://au.int/en/member_states/countryprofiles2> [accessed 6 May 2023].
[608] Article 1 of the 'African Charter on Human and Peoples' Rights', *CAB/LEG/67/3, Adopted on 27 June 1982 in Banjul*, 1982 <https://doi.org/10.9783/9780812205381.713>.
[609] Article 30 of the 'African Charter on Human and Peoples' Rights', *CAB/LEG/67/3, Adopted on 27 June 1982 in Banjul*, 1982 <https://doi.org/10.9783/9780812205381.713>.
[610] Wiebusch M, Aniekwe CC, Oette L and Vandeginste S, 'The African Charter on Democracy, Elections and Governance: Past, Present and Future', *Journal of African Law*, 63.S1 (2019), 9–38 <https://doi.org/10.1017/S002185531900007X>.
[611] Assembly of the African Union, 'Protocol to the African Charter on Human And Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights', *Treaty 0019, Adopted on 10 June 1998 in Maputo*, 1998.
[612] Article 2 of the 'Protocol of the Court of Justice of the African Union', *Treaty 0026, Adopted on 1 July 2003 in Maputo*, 2003.
[613] Chapter 1 of the 'Protocol on the Statute of the African Court of Justice and Human Rights', *Adopted on 1 July 2008 in Sharm El-Sheikh*, 2004.

Both the African Commission and the ACtJHR have the mandate to address violations of the right to participate in the conduct of public affairs under Article 13(1) of the African Charter[614]. Under Article 30 of the Protocol on the Statute of the African Court of Justice and Human Rights:

> "[E]ntities shall also be entitled to submit cases to the Court on any violation of a right guaranteed by the African Charter, by the Charter on the Rights and Welfare of the Child, the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa, or any other legal instrument relevant to human rights ratified by the States Parties"[615].

While the African Commission investigates complaints and issues recommendations[616], the ACtJHR has binding authority to make judgments on human rights cases, provided that the state in question has ratified the relevant protocols and accepted the Court's jurisdiction[617]. The ACtJHR can address cases submitted by state parties, the Assembly or staff members of the AU[618], as well as cases referred by the African Commission, cases referred by the African Committee of Experts on the Rights and Welfare of the Child, African inter-governmental organisations, national African human rights organisations, and individuals within the jurisdiction of the AU[619].

The right to participate in the conduct of public affairs is primarily protected under Article 13(1) of the ACHPR, which guarantees "the right to participate freely in the government of his country, either directly or through freely chosen representatives"[620]. Additionally, and in contrast to the European and American regions, the AU has adopted two distinct legal instruments dedicated entirely to the principles and mechanisms of maintaining democracy, namely the Declaration on the Principles Governing Democratic Elections in Africa (2002) and the African Charter on Democracy, Elections and Governance (2007). The 2002 Declaration establishes a comprehensive set of guidelines for conducting democratic elections in Africa,

[614] M. Ssenyonjo, 'Responding to Human Rights Violations in Africa: Assessing the Role of the African Commission and Court on Human and Peoples' Rights (1987–2018)', *International Human Rights Law Review*, 7.1 (2018), 1–42.
[615] Article 30 of the 'Protocol on the Statute of the African Court of Justice and Human Rights'.
[616] Article 45 of the 'African Charter on Human and Peoples' Rights', *CAB/LEG/67/3, Adopted on 27 June 1982 in Banjul*, 1982 <https://doi.org/10.9783/9780812205381.713>.
[617] Article 2 of the 'Protocol on the Statute of the African Court of Justice and Human Rights'.
[618] Article 29 of the 'Protocol on the Statute of the African Court of Justice and Human Rights'.
[619] Article 30 of the 'Protocol on the Statute of the African Court of Justice and Human Rights'.
[620] Article 13(1) of the 'African Charter on Human and Peoples' Rights', *CAB/LEG/67/3, Adopted on 27 June 1982 in Banjul*, 1982 <https://doi.org/10.9783/9780812205381.713>.

emphasising the importance of regular, transparent, free, and fair elections[621]. It highlights key principles such as respect for human rights[622], political pluralism [623], and equal access to public media [624]. The African Charter on Democracy, Elections and Governance of 2007, in turn, elaborates on these democratic principles, and requires state parties to hold regular, transparent, and credible elections through universal suffrage[625], to create conditions that are conducive to the promotion of citizen participation in the democratic process[626], and to respect freedom of expression[627] as essential elements of a democratic society.

The enforcement of human rights protections in the African region, including the right to participate in the conduct of public affairs, is primarily overseen by the African Commission and the ACtJHR[628]. Under Article 45 of the ACHPR, the African Commission is responsible for promoting and protecting human rights, interpreting the provisions of the Charter, and investigating human rights violations. The Commission receives communications from individuals and organisations alleging violations of human rights, conducts examinations, and issues recommendations to the concerned state [629]. However, these recommendations are non-binding and rely on the state's commitment to adhere to them[630]. Conversely, the ACtJHR has the authority to issue binding judgments on cases relating to the violation of human rights under the ACHPR and other relevant legal instruments ratified by the state parties[631]. Judgements of the African Court are final[632], and state parties are obligated to comply within the specified time[633]. In instances of failure to comply with judgments, the ACtJHR may refer the matter to

[621] Section II(4) of the 'OAU/AU Declaration on the Principles Governing Democratic Elections in Africa', *AHG Decl. 1 (XXXVIII), Adopted on 8 July 2002 in Durban* , 2002.
[622] Section I of the 'OAU/AU Declaration on the Principles Governing Democratic Elections in Africa', *AHG Decl. 1 (XXXVIII), Adopted on 8 July 2002 in Durban* , 2002.
[623] Section IV(5) of the 'OAU/AU Declaration on the Principles Governing Democratic Elections in Africa', *AHG Decl. 1 (XXXVIII), Adopted on 8 July 2002 in Durban* , 2002.
[624] Section III(d) of the 'OAU/AU Declaration on the Principles Governing Democratic Elections in Africa', *AHG Decl. 1 (XXXVIII), Adopted on 8 July 2002 in Durban* , 2002.
[625] Article 4(2) of the 'African Charter on Democracy, Elections and Governance', *Assembly/AU/Dec. 147(VIII), Adopted on 30 January 2007 in Addis Ababa*, 2007.
[626] Article 20 of the 'African Charter on Democracy, Elections and Governance', *Assembly/AU/Dec. 147(VIII), Adopted on 30 January 2007 in Addis Ababa*, 2007.
[627] Article 27 of the 'African Charter on Democracy, Elections and Governance', *Assembly/AU/Dec. 147(VIII), Adopted on 30 January 2007 in Addis Ababa*, 2007.
[628] Ssenyonjo.
[629] Article 45 of the 'African Charter on Human and Peoples' Rights', *CAB/LEG/67/3, Adopted on 27 June 1982 in Banjul*, 1982 <https://doi.org/10.9783/9780812205381.713>.
[630] G.M. Wachira and A. Ayinla, 'Twenty Years of Elusive Enforcement of the Recommendations of the African Commission on Human and Peoples' Rights: A Possible Remedy', *African Human Rights Law Journal*, 6.2 (2006), 465–92.
[631] Article 46(1) of the 'Protocol on the Statute of the African Court of Justice and Human Rights'.
[632] Article 46(2) of the 'Protocol on the Statute of the African Court of Justice and Human Rights'.
[633] Article 46(3) of the 'Protocol on the Statute of the African Court of Justice and Human Rights'.

the AU Assembly for a decision on the appropriate measures to be taken to give effect to judgments[634], which may include sanctions against the state party[635].

While the African human rights system has made significant strides in promoting and protecting the right to participate in the conduct of public affairs, its enforcement mechanisms face enduring challenges. Much like its European and American counterparts, the ACtJHR is also susceptible to patterns of resistance that can undermine its authority and impact[636]. Such patterns of resistance can be seen as an apparent trend among states to withdraw their declaration, accepting the competence of the ACtJHR[637], which severely limits its jurisdiction to receive cases directly from individuals and NGOs[638]. Additional challenges include insufficient resources[639] for operating the African Commission and Court, as well as the absence of an appeal mechanism, and weak institutional shields[640].

In addition to these challenges, the ACtJHR, similar to the European and American human rights systems, has contributed to the development and interpretation of the right to participate in the conduct of public affairs through its jurisprudence[641]. One of the cases illustrating the ACtJHR's role in protecting this right is *Tanganyika Law Society & The Legal and Human Rights v the United Republic of Tanzania* (2011). The applicants contended that the Tanzanian government violated Article 13(1) of the Charter by requiring candidates for elections to belong to political parties[642]. The Court found that this requirement limited citizens' ability to participate freely in the government and held that Tanzania violated the right to participate freely in the conduct of public affairs[643]. Another example is *Kouassi Kouame Patrice and Baba Sylla v Republic of Côte d'Ivoire* (2021), where the applicants alleged that material irregularities occurred during the 2021 parliamentary election, including the lack of

[634] Article 46(4) of the 'Protocol on the Statute of the African Court of Justice and Human Rights'.
[635] Article 46(5) of the 'Protocol on the Statute of the African Court of Justice and Human Rights'.
[636] Tom Gerald Daly and Micha Wiebusch, 'The African Court on Human and Peoples' Rights: Mapping Resistance against a Young Court', *International Journal of Law in Context*, 14.2 (2018), 294–313 <https://doi.org/10.1017/S1744552318000083>.
[637] Article 34(6) of the 'Protocol to the African Charter on Human And Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights'.
[638] Sègnonna Horace Adjolohoun, 'A Crisis of Design and Judicial Practice? Curbing State Disengagement from the African Court on Human and Peoples' Rights', *African Human Rights Law Journal*, 20.1 (2020), 1–40 <https://doi.org/10.17159/1996-2096/2020/v20n1a1>.
[639] Chairman Okoloise, 'Circumventing Obstacles to the Implementation of Recommendations by the African Commission on Human and Peoples' Rights', *African Human Rights Law Journal*, 18.1 (2018), 28–57 <https://doi.org/10.17159/1996-2096/2018/v18n1a2>.
[640] Adjolohoun.
[641] Kariuki Muigua, 'African Court of Justice and Human Rights: Emerging Jurisprudence', *Kariuki Muigua and Company Advocates*, 2020, 1–9 <https://en.african-court.org/>.
[642] Paragraph 91 of 'Tanganyika Law Society & the Legal and Human Rights v the United Republic of Tanzania', *Application No. 009/2011 (ACJHR)*, 2011.
[643] Paragraph 111 of 'Tanganyika Law Society & the Legal and Human Rights v the United Republic of Tanzania'.

transparency in vote counting, unequal access to state-owned media, and the arbitrary disqualification of candidates[644]. The applicants claimed that these irregularities amounted to violations of domestic electoral laws and their fundamental human rights[645]. In its judgement, the Court emphasised that the right to participate freely in the conduct of public affairs includes the right to free, fair, and transparent elections, and that these irregularities and violations of electoral laws undermined this right. The Court held that the lack of transparency in the electoral process, as well as the unequal access to state-owned media and the arbitrary disqualification of candidates, violated the applicants' rights under Article 13(1) of the Charter.[646]

Most recently, the case of *Ibrahim Ben Mohamed Ben Ibrahim Belguit v Republic of Tunisia* (2021) followed President Kais Saied's self-coup on 25 July 2021, which expanded his control over everything from the legislature to the media[647]. The applicant argued that the Tunisian government violated his right to participate in the conduct of public affairs under Article 13(1) of the Charter, following the President's decision to suspend the Tunisian Parliament, dismiss the Prime Minister, and concentrate power in the hands of the President. The applicant claimed that this action effectively abrogated the Constitution, halted the democratic process, and undermined the rule of law in Tunisia.[648] In its judgement, the Court emphasised the importance of the separation of powers and the rule of law as fundamental principles underpinning the right to participate in the conduct of public affairs. The Court found that the Tunisian government's actions had violated these principles and, in turn, the applicant's rights under Article 13(1) of the Charter[649]. The Court also noted that the concentration of power in the hands of the President and the suspension of the Parliament restricted citizen's ability to participate in the conduct of public affairs and ordered a return to a constitutional democracy within two years, including reinstating the Parliament and ensuring the independence of the judiciary [650].

Like its European and American counterparts, the ACtJHR's jurisprudence has influenced not only the parties directly involved but also the broader interpretation and application of human

[644] Paragraph 3 of 'Kouassi Kouame Patrice and Baba Sylla v Republic of Côte D'Ivoire', *Application No. 015/2021 (ACJHR)*, 2021.
[645] Paragraph 6(ii) of 'Kouassi Kouame Patrice and Baba Sylla v Republic of Côte D'Ivoire'.
[646] Paragraph 116 of 'Kouassi Kouame Patrice and Baba Sylla v Republic of Côte D'Ivoire'.
[647] Sarah Yerkes and Maha Alhomoud, 'One Year Later, Tunisia's President Has Reversed Nearly a Decade of Democratic Gains', *Carnegie Endowment for International Peace*, 2022.
[648] Paragraph 3 of 'Ibrahim Ben Mohamed Ben Ibrahim Belguith v Republic of Tunisia', *Application No. 017/2021 (ACJHR)*, 2021.
[649] Paragraph 147(iv) of 'Ibrahim Ben Mohamed Ben Ibrahim Belguith v Republic of Tunisia'.
[650] Paragraph 147(viii) of 'Ibrahim Ben Mohamed Ben Ibrahim Belguith v Republic of Tunisia'.

rights norms across the continent[651]. This influence is evident in domestic courts, national human rights institutions, and regional bodies, which often look to the ACtJHR's decisions for guidance on human rights issues.[652] Among this influence, transparent and independent judiciaries appear to be a dominant theme[653]. In particular, the ACtJHR has been instrumental in promoting the right to fair trial across Africa. In cases where individuals have alleged violations of their right to a fair trial, the African Court has emphasised the importance of an independent and impartial judiciary, the right to legal representation, and the right to a public hearing. These principles have since been incorporated into the jurisprudence of domestic courts and the work of national human rights institutions.[654] Mechanisms for the protection of human rights for specific vulnerable groups such as women and children also distinguish the African region from its European and American counterparts. This focus on the protection of vulnerable groups is apparent from the Protocol to the African Charter on the Rights of Women in Africa, which addresses specific human rights challenges faced by women in Africa, including the right to non-discrimination[655], dignity[656], and equal protection before the law[657], as well as protection from harmful traditional practices[658] and access to reproductive health services[659]. Since its adoption in 2003, the Protocol to the African Charter on the Rights of Women has had a significant impact on legal frameworks, domestic legislation and judicial enforcement in the region[660]. Moreover, the African Charter on the Rights and Welfare of the Child imposes a range of both positive and negative obligations on state parties to ensure the comprehensive protection of children's rights[661]. Positive obligations include provisions such as the right to education[662], the right to specialised healthcare[663], and the administration of

[651] Lilian Chenwi, 'Exhaustion of Local Remedies Rule in the Jurisprudence of the African Court on Human and Peoples' Rights', *Human Rights Quarterly*, 41.2 (2019), 374–98 <https://heinonline.org/HOL/License>.
[652] Muigua.
[653] Trésor Muhindo Makunya, 'Decisions of the African Court on Human and Peoples' Rights during 2020: Trends and Lessons', *African Human Rights Law Journal*, 21.2 (2021), 1230–64 <https://doi.org/10.17159/1996-2096/2021/v21n2a49>.
[654] M.A. Plagis, 'The Makings of Remedies: The (R)Evolution of the African Court on Human and Peoples' Rights' Remedies Regime in Fair Trial Cases', *African Journal of International and Comparative Law*, 28 (2020), 45–71.
[655] Article 2 of the 'Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa', *AHG/Res.240 (XXXI), Adopted on 11 July 2003*.
[656] Article 3 of the 'Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa', *AHG/Res.240 (XXXI), Adopted on 11 July 2003*.
[657] Article 8 of the 'Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa', *AHG/Res.240 (XXXI), Adopted on 11 July 2003*.
[658] Article 5 of the 'Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa', *AHG/Res.240 (XXXI), Adopted on 11 July 2003*.
[659] Article 14 of the 'Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa', *AHG/Res.240 (XXXI), Adopted on 11 July 2003*.
[660] Somé KA, Forkum PN, Tanoh A, echane MG, Nabaneh S, Nyarko MG, *The Impact of the African Charter and the Maputo Protocol in Selected African States* (Pretoria: PULP, 2016).
[661] Article 4 of the 'African Charter on the Rights and Welfare of the Child', *CAB/LEG/24.9/49, Adopted on 11 July 1990*.
[662] Article 11 of the 'African Charter on the Rights and Welfare of the Child', *CAB/LEG/24.9/49, Adopted on 11 July 1990*.
[663] Article 14 of the 'African Charter on the Rights and Welfare of the Child', *CAB/LEG/24.9/49, Adopted on 11 July 1990*.

juvenile justice systems[664], while negative obligations address issues such as child labour[665], child abuse[666], and protections against harmful cultural practices[667]. While several challenges to the protection of the human rights of children in the African region remain, especially that of child marriages and adolescent pregnancies[668], the Charter has served as a unified framework for policy development and monitoring and reporting on the welfare of children in Africa[669].

Though the African Commission and the ACtJHR have a more recent emergence compared to their European and American counterparts[670], their impact on the development and application of standards for the protection of human rights in the region has been both profound and indisputable[671]. In fact, while the ECtHR[672] and the IACtHR[673] remain under consistent scrutiny for the slow pace in adjudicating cases, decisions on cases such as *Ibrahim Ben Mohamed Ben Ibrahim Belguith v Republic of Tunisia* (2021)[674] and *Kouassi Kouame Patrice and Baba Sylla v Republic of Côte D'Ivoire* (2021)[675] suggest that the African system may be more adept at resolving cases in a timely manner. Conversely, the ECtHR itself acknowledges that the frequent non-execution of its judgments by member states poses a substantial threat to the efficacy of the region's entire human rights protection system[676]. Moreover, what sets the African system apart from other regional systems is its focus on addressing context-specific challenges linked to historical and socio-political factors[677], and improved regional harmonisation of human rights norms within the region[678]. Despite these advances in human

[664] Article 17 of the 'African Charter on the Rights and Welfare of the Child', *CAB/LEG/24.9/49, Adopted on 11 July 1990.*
[665] Article 15 of the 'African Charter on the Rights and Welfare of the Child', *CAB/LEG/24.9/49, Adopted on 11 July 1990.*
[666] Article 16 of the 'African Charter on the Rights and Welfare of the Child', *CAB/LEG/24.9/49, Adopted on 11 July 1990.*
[667] Article 21 of the 'African Charter on the Rights and Welfare of the Child', *CAB/LEG/24.9/49, Adopted on 11 July 1990.*
[668] Maswikwa B,Richter L, Kaufman J and Nandi A, 'Minimum Marriage Age Laws and the Prevalence of Child Marriage and Adolescent Birth: Evidence from Sub-Saharan Africa', *International Perspectives on Sexual and Reproductive Health*, 41.2 (2015), 58–68 <https://doi.org/10.1363/4105815>.
[669] W. Vandenhole, G.E. Türkelli, and S. Lembrechts, *Children's Rights: A Commentary on the Convention on the Rights of the Child and Its Protocols* (Cheltenham: Edward Elgar Publishing, 2019).
[670] E.K. Quashigah, 'The African Court of Human Rights: Prospects, in Comparison with the European Court of Human Rights and the Inter-American Court of Human Rights', *Annual Conference - African Society of International and Comparative Law*, 1998, 59–69.
[671] Ssenyonjo.
[672] De Londras and Dzehtsiarou.
[673] Bailliet.
[674] 'Ibrahim Ben Mohamed Ben Ibrahim Belguith v Republic of Tunisia'.
[675] 'Kouassi Kouame Patrice and Baba Sylla v Republic of Côte D'Ivoire'.
[676] Section IV(a) of 'Greens and M.T. v the United Kingdom'.
[677] Maria A. Sanchez, 'The African Court on Human and Peoples' Rights: Forging a Jurisdictional Frontier in Post-Colonial Human Rights', *International Journal of Law in Context*, 2023, 1–15 <https://doi.org/10.1017/s1744552323000046>.
[678] Babatunde Fagbayibo, 'A Normative Appraisal of the African Union's Membership Admission Rules', *Verfassung in Recht Und Übersee*, 50.2 (2017), 156–74 <https://doi.org/10.5771/0506-7286-2017-2-156>.

rights protections in the African region, challenges in both administration[679] and enforcement[680] remain. As the free expression of one's will through fair democratic processes remains a dominant theme in the human rights discourse[681], it seems critical that the African Union and its member states bolster their commitment to the ACtJHR and the African Commission[682], enabling these institutions to continue to effectively promote and protect the human right to participate in the conduct of public affairs by equal and universal suffrage.

4.7. Cyber law in the African region

The evolution of cyber law in the African region is a testament to burgeoning progress, marked by the development of legal instruments[683], regulatory bodies[684], and enforcement mechanisms[685]. This progress, however, has not been uniform across the continent, with significant variations in the adoption, monitoring and enforcement between Regional Economic Communities (RECs) and individual AU member states.[686] Article 25 of the African Economic Community Treaty, also referred to as the Abuja Treaty, includes a provision establishing seven specialised technical committees (STCs) on various specialised fields that might impact economic activity in the region[687]. Under Article 14 of the AU's Constitutive Act of 2000, the General Assembly is empowered to restructure STCs to better align with changing socio-economic developments in the region[688], and there are currently 13 STCs, one of which is the STC on Communication and Information Communications Technology (STC-CICT)[689]. Subsequently, Cyber Security has also been included as a Flagship project of Agenda 2063[690]. One might therefore argue that the driver behind efforts towards a harmonised cyber law framework in Africa has been growing concerns among AU decision-makers that the absence

[679] D. Ntanda Nsereko and M. Ventura, 'Perspectives on the International Criminal Jurisdiction of the African Court of Justice and Human Rights Pursuant to the Malabo Protocol', in The *African Court of Justice and Human and Peoples' Rights in Context: Development and Challenges*, ed. by J.K. Clarke and V. Nmehielle (Cambridge: Cambridge University Press, 2019), pp. 257–84.
[680] Daly and Wiebusch.
[681] Rubinstein A, Roznai Y, Yaniv R and Roznai Y, *The Right to a Genuine Electoral Democracy Recommended Citation Symposium Article The Right to a Genuine Electoral Democracy, Genuine Electoral Democracy*, 2018, XXVII <https://scholarship.law.umn.edu/mjilhttps://scholarship.law.umn.edu/mjil/266>.
[682] Fagbayibo.
[683] ALT Advisory, *The Malabo Roadmap: Approaches to Promote Data Protection and Data Governance in Africa* (Johannesburg, September 2022).
[684] Alexandra Gaillard, 'Cybersecurity Challenges and Governance Issues in the Cyberspace "When Stronger Passwords Are Not Enough: Governing Cyberspace in Contemporary African Nations" Case Study: Can South Africa and Nigeria Secure Cyberspace without a Lock?', *SSRN*, 2021, 3877526 <https://ssrn.com/abstract=3877526>.
[685] Etienne Vallée and Yu Chang Hsu, 'Protecting Students: Data Privacy in the African Union', *TechTrends*, 67 (2023), 203–6 <https://doi.org/10.1007/s11528-023-00834-0>.
[686] Graham Greenleaf and Bertil Cottier, 'Comparing African Data Privacy Laws: International, African and Regional Commitments', *University of New South Wales Law Research Series*, 2020 <https://au.int/memberstates>.
[687] Article 25 of the 'Treaty Establishing the African Economic Community (Abuja Treaty)', 1991.
[688] Article 14(2) of the 'Constitutive Act of the African Union', *CAB/LEG/23.15, Adopted in Lomé, on 11 July 2000*.
[689] African Union, 'Specialised Technical Committees', 2023 <https://au.int/en/stc> [accessed 22 June 2023].
[690] Section G of the 'Agenda 2063 Progress Report', *Eco/STC/MAEPI(IV)/EXP/8, Adopted on 11 March 2020*.

of a comprehensive cybersecurity plan poses a material threat to socio-economic development initiatives within the region[691]. A rapid succession of new initiatives, demonstrates the AU's intensified concerns regarding cybersecurity and digital transformation. In 2017, the AU's Internet Infrastructure Security Guidelines for Africa was launched[692]. 2018 saw the establishment of the Africa Cyber Security Collaboration and Coordination Committee (ACS3C) and the AU Cybersecurity Expert Group (AUCSEG)[693], and in 2020 the AU adopted a Digital Transformation Strategy, aiming for an 'integrated and inclusive' digital society by 2030[694]. Most recently, the AU Convention on Cyber Security and Personal Data Protection, also known as the Malabo Convention, came into force in June of 2023[695], nearly a decade after its regional adoption in 2014[696].

The AU Commission (AUC), as an official organ of the Union under the AU Constitutive Act of 2000, is the key administrative arm of the African Union[697] and is central to the development, implementation and monitoring of cyber law-related initiatives among AU member states[698]. The Commission consists of the Chairperson, the Deputy Chairperson, and eight Commissioners, whom are elected by the Assembly of Heads of State and Government for a four-year term[699]. The eight Commissioners are responsible for different portfolios, including economic affairs and science and technology, and plays a crucial role in driving the AU's agenda and executing its programmes[700]. Both the ACS3C and the AUCSEG fall within the mandate of the AUC. The ACS3C is a multi-stakeholder group that advises policymakers of the AUC on regional strategies and capacity building, while also facilitating information

[691] Vedaste Ndizera and Hannah Muzee, 'A Critical Review of Agenda 2063: Business as Usual?', *African Journal of Political Science and International Relations*, 12.8 (2018), 142–54 <https://doi.org/10.5897/ajpsir2018.1114>.
[692] AU Commission and Internet Society, *Internet Infrastructure Security Guidelines for Africa: A Joint Initiative of the Internet Society and the Commission of the African Union* (Addis Ababa, 30 May 2017).
[693] AU Executive Council, 'Decisions of the Thirty-Second Ordinary Session', *EX.CL/Dec.986-1007(XXXII), Adopted in Addis Ababa on 26 January 2018*.
[694] AU Commission, *The Digital Transformation Strategy for Africa (2020-2030)* (Addis Ababa, 9 February 2020) <https://futurium.ec.europa.eu/en/Digital4Development/library/digital-transformation-strategy-africa-2020-2030> [accessed 23 June 2023].
[695] Yohannes Eneyew Ayalew, 'The African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force Nearly after a Decade: What Does It Mean for Data Privacy in Africa or Beyond?', *Blog of the European Journal of International Law*, 15 June 2023 <https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-doe>.
[696] AU General Assembly, 'African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)', *EX.CL/846(XXV), Adopted in Malabo on 27 June 2014*.
[697] Article 5 of the 'Constitutive Act of the African Union'.
[698] Nnenna Ifeanyi-Ajufo, 'Cybersecurity for Inclusive Digital Transformation in Africa', *Observer Research Foundation*, 2022 <https://www.orfonline.org/expert-speak/cybersecurity-for-inclusive-digital-transformation-in-africa/> [accessed 23 June 2023].
[699] Article 20 of the 'Constitutive Act of the African Union'.
[700] African Union, 'The Structure and Portfolios of The Senior Leadership of The AU Commission', 2020 <https://au.int/en/announcements/20200707/structure-and-portfolios-senior-leadership-au-commission> [accessed 23 June 2023].

sharing across the region. This Committee serves as a key vehicle for the AUC to receive advice on cybersecurity matters, enabling the Commission to formulate effective strategies that can be adopted and implemented by member states.[701] The AUCSEG, in turn, supports the AUC by facilitating coordination and information sharing among African countries and regions. This group identifies areas where resources are needed and advises on national, regional, and continental strategies that should be prioritised.[702] The AUCSEG, therefore, aids the AUC in understanding the cybersecurity landscape, identifies critical areas of intervention, and enables focused resource allocation within the region[703].

The AUC is also the custodian of the Digital Transformation Strategy for Africa (2020-2030), adopted in 2020, which includes recommendations and actions to support the development of a Digital Single Market (DSM) for Africa[704]. This strategy is expected to build on existing initiatives such as the Policy and Regulatory Initiative for Digital Africa (PRIDA), the Programme for Infrastructure Development in Africa (PIDA), and the African Union Financial Institutions (AUFIs)[705]. The strategy highlights the interconnectedness of the region's economic development goals with its cybersecurity priorities, and demonstrates the necessity of a harmonised regional regulatory framework for supporting growth while maintaining safety and security in the modern socio-economic landscape. It is towards such growth that the AUC have collaborated with the Internet Society (ISOC) to produce the AU's Internet Infrastructure Security Guidelines for Africa, which introduces four essential principles of Internet infrastructure security, namely awareness, responsibility, cooperation, and adherence to fundamental rights and internet properties[706]. The AUC has promoted these principles to be the bedrock upon which stakeholders can build their contributions to improve internet infrastructure, security, and law[707]. Of such legal instruments, the Malabo Convention is generally regarded as a significant policy step forward and pivotal milestone in Africa's

[701] Tomslin Samme-Nlar, 'Cyberspace Security in Africa – Where Do We Stand?', *African Academic Network on Internet Policy* , 2020 <https://aanoip.org/cyberspace-security-in-africa-where-do-we-stand/> [accessed 23 June 2023].
[702] Halefom H Abraha, 'Government Access to Digital Evidence Across Borders: Some Lessons for Africa', in *The Internet and Policy Responses in Ethiopia: New Beginnings and Uncertainties*, ed. by K.M. Yilma (Addis Ababa: Addis Ababa University Press, 2020), pp. 11–49 <https://bit.ly/2Irp0jq>.
[703] Oladotun E. Awosusi, 'The Imperative of Cyber Diplomacy and Cybersecurity in Africa: A New Means to a "Borderless" Regional End?', *Journal of African Foreign Affairs*, 9.3 (2022), 57–81 <https://doi.org/10.31920/2056-5658/2022/v9n3a3>.
[704] Chloe Teevan and Lidet Tadesse Shiferaw, *Briefing Note No. 150: Digital Geopolitics in Africa: Moving from Strategy to Action* (Maastricht, October 2022).
[705] AU Commission, *Annexure 2 of the Draft Digital Transformation Strategy for Africa (2020-2030)* (Addis Ababa, 2 September 2020) <www.au.int>.
[706] Ifeanyi-Ajufo.
[707] M.J.Z. de Barros and H. Lazarek, 'A Conceptual Model for the Development of Cybersecurity Capacity in Mozambique', in *European Conference on Cyber Warfare and Security* (Coimbra: Academic Conferences International Limited, 2019), pp. 623–XIII.

campaign to address contemporary commerce issues[708]. The Convention, which has been ratified by 15 AU member states, provides a comprehensive legal structure for data protection, cybercrime, and cybersecurity[709]. While the Convention does offer a holistic continent-wide framework to harmonise data protection policies in Africa, it is not without scrutiny. Points of concern include that the Convention lacks important detail, and does not provide for mechanisms to support its enforcement[710]. Much like Europe's GDPR, the Malabo Convention seeks to create a unified framework of data protection across its member states[711]. However, unlike the GDPR which clearly outlines enforcement responsibilities to the EDPB and national DPAs[712], the enforcement mechanisms in the Malabo Convention are less defined. It emphasises the need for establishing data protection authorities in each member state, but lacks clarity on the implementation process.[713] This contributes to a gap between the ambitious legal frameworks and the actual enforcement capability.

The gap between the Malabo Convention's objectives and its enforcement is exacerbated by the absence of designated Data Protection Authorities (DPAs) in many AU member states[714]. An independent DPA is a central feature of the effective implementation of the Convention's principles[715]. As such, the absence of such authorities and the inability of several member states to guarantee their DPA's independence currently undermines the efficacy of the Convention[716]. A gap also currently exists between the Malabo Convention's holistic approach to cyber law and the implementation capacity of member states that are still in the process of developing their digital infrastructure and capacities[717]. Yet, with the incorporation of cybersecurity as a flagship project under Agenda 2063[718], and the AU's Digital Transformation Strategy for Africa[719], in conjunction with initiatives like the Policy and Regulatory Initiative for Digital

[708] Bitange Ndemo and Ben Mkalama, *The Context Digitalization and Financial Data Governance in Africa: Challenges and Opportunities* (Nairobi, June 2022).
[709] ALT Advisory, 'Africa: AU's Malabo Convention Set to Enter Force after Nine Years', *Data Protection Africa*, 2023 <https://dataprotection.africa/malabo-convention-set-to-enter-force/#:~:text=The latest status list on,force by 8 June 2023.&text=This marks a significant milestone,of cybersecurity and data protection.> [accessed 23 June 2023].
[710] ALT Advisory, *The Malabo Roadmap: Approaches to Promote Data Protection and Data Governance in Africa*.
[711] Preamble to 'African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)'.
[712] Jančiūtė.
[713] Tomiwa Ilori, 'Data Protection in Africa and the COVID-19 Pandemic: Old Problems, New Challenges and Multistakeholder Solutions', *Association for Progressive Communications*, 2020.
[714] Ilori.
[715] Article 11(1)(b) of the 'African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)'.
[716] Lukman Adebisi Abdulrauf, 'Giving "Teeth" to the African Union towards Advancing Compliance with Data Privacy Norms', *Information & Communications Technology Law*, 30.2 (2021), 87–107 <https://www.tau.ac.il/law/minerva2/Birnhack.pdf>.
[717] Kinfe Yilma, 'African Union's Data Policy Framework and Data Protection in Africa', *Journal of Data Protection and Privacy*, 5.3 (2022), 1–7 <https://ssrn.com/abstract=4253828>.
[718] STC-MAEPI.
[719] Teevan and Shiferaw.

Africa (PRIDA), the Programme for Infrastructure Development in Africa (PIDA), and the African Union Financial Institutions (AUFIs), represents regional attempts to bridge this divide towards socio-economic development[720]. Compared to the European approach, where the European Commission spearheads the development of cybersecurity strategies and regulatory frameworks[721], the AU relies on a multi-stakeholder group such as ACS3C and AUCSEG for the same[722]. It could be argued that these groups play a similar role to Europe's ENISA in facilitating information sharing, advising on strategies, and prioritising resource allocation for cybersecurity within their respective regions. However, the AU's approach seems distinctly more consultative, involving stakeholders from a wider spectrum, which includes not only governmental and intergovernmental entities but also non-governmental organisations and the private sector. Furthermore, in contrast to regions like Europe and the Americas, where evidence of enforcement can be found in established case law and well-defined enforcement mechanisms, the African region is yet to show such concrete evidence of enforcement at the regional level[723].

Preceding and informing the Malabo Convention's overarching framework, Regional Economic Communities (RECs) like the East African Community (EAC) and the Economic Community of West African States (ECOWAS) have taken active steps to address the aforementioned gaps. As early as 2009, the EAC became the first region within the larger African region to adopt a harmonised regional cyber law framework. The framework was proposed and developed to meet the needs expressed by the Council of Ministers of the East African Community in 2006, as part of their support for the regional e-government and e-commerce integration process.[724] To date, however, this progressive framework has remained the guiding principles and has not been legally binding until translated into domestic laws, which has been limited to Kenya, Uganda and Rwanda[725]. ECOWAS, in turn, has introduced legal instruments binding Community member states to reinforce cybersecurity in the region. These include the Supplementary Act on Personal Data Protection in 2010[726] and the Directive

[720] ALT Advisory, *The Malabo Roadmap: Approaches to Promote Data Protection and Data Governance in Africa*.
[721] Elaine Fahey, 'Developing EU Cybercrime and Cybersecurity On Legal Challenges of EU Institutionalisation of Cyber Law-Making', in *The Routledge Handbook of European Integrations*, ed. by T. Hoerber, G. Weber, and I. Cabras (Abingdon, UK: Routledge, 2022), pp. 270–84.
[722] AU Commission, *The Digital Transformation Strategy for Africa (2020-2030)*.
[723] Alex B. Makulilo, 'The Long Arm of GDPR in Africa: Reflection on Data Privacy Law Reform and Practice in Mauritius', *International Journal of Human Rights*, 25.1 (2020), 117–46 <https://doi.org/10.1080/13642987.2020.1783532>.
[724] UNCTAD, *Harmonizing Cyberlaws and Regulations: The Experience of the East African Community* (Geneva, 2012).
[725] Olumide Babalola, *Data Protection Legal Regime and Data Governance in Africa: An Overview* (Nairobi, February 2023).
[726] ECOWAS, 'Supplementary on Personal Data Protection within ECOWAS', *Act A/SA.1/01/10, Adopted in Abuja on 16 February 2010*.

on Fighting Cybercrime in 2011[727], to reinforce cybersecurity in the region. The Supplementary Act on Personal Data Protection standardises data protection legislation through guiding principles such as legitimacy, fairness, proportionality, and security, as well as rules on cross-border data transfers[728]. The Act highlights the importance of consent in data processing and outlines individuals' rights to be informed, access, rectify, and object to their data being processed[729]. The Act also stipulates that each ECOWAS member state must establish an independent authority to oversee and enforce data protection regulations[730]. The Directive on Fighting Cybercrime, in turn, provides a legal framework for the prevention, investigation, and prosecution of cybercrimes within the ECOWAS region[731]. The Directive covers a wide range of cybercrimes including illegal access to computer systems[732], data interference[733], system interference[734], misuse of devices[735], computer-related forgery and fraud[736], offences related to child pornography[737], and violations of network security[738]. The Directive also introduces procedural laws that allow competent authorities to collect electronic evidence, conduct surveillance, and seek international cooperation in cybercrime investigations[739]. Furthermore, it imposes obligations on ECOWAS member states to enact the necessary legislation and develop capacity-building measures to combat cybercrime at a domestic level[740]. Much like the EU's NIS 2 Directive, which seeks to achieve a high common level of network and information systems security across the Union[741], the ECOWAS Directive on Fighting Cybercrime is an attempt at harmonising cybercrime laws in the West African region [742]. While the NIS 2 Directive includes guidelines on cooperation between member states and the role of national cybersecurity centres[743], the ECOWAS Directive also introduces procedural laws for the collection of electronic evidence, conduct surveillance, and international cooperation in

[727] ECOWAS, 'Directive on Fighting Cyber Crime within ECOWAS', *C/DIR.1/08/11, Adopted in Abuja on 19 August 2011*.
[728] INTERPOL and ECOWAS, *WAPIS Guide: Best Practice on Personal Data Protection* (Lyon, June 2020).
[729] Article 23 of the 'Supplementary on Personal Data Protection within ECOWAS'.
[730] Article 14(1) of the 'Supplementary on Personal Data Protection within ECOWAS'.
[731] Article 2 of the 'Directive on Fighting Cyber Crime within ECOWAS'.
[732] Article 4 of the 'Directive on Fighting Cyber Crime within ECOWAS'.
[733] Article 9 of the 'Directive on Fighting Cyber Crime within ECOWAS'.
[734] Article 6 of the 'Directive on Fighting Cyber Crime within ECOWAS'.
[735] Article 14 of the 'Directive on Fighting Cyber Crime within ECOWAS'.
[736] Article 13 of the 'Directive on Fighting Cyber Crime within ECOWAS'.
[737] Article 16-19 of the 'Directive on Fighting Cyber Crime within ECOWAS'.
[738] Article 21 of the 'Directive on Fighting Cyber Crime within ECOWAS'.
[739] Chapter V of the 'Directive on Fighting Cyber Crime within ECOWAS'.
[740] Article 35(1) of the 'Directive on Fighting Cyber Crime within ECOWAS'.
[741] Holzleitner and Reichl.
[742] Preamble of the 'Directive on Fighting Cyber Crime within ECOWAS'.
[743] Para. 20 of the 'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for the High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and the Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)', *Official Journal of the European Union*, I. 333/80 (2022).

cybercrime investigations, demonstrating a similar commitment to collaborative efforts against cybercrime[744].

In parallel with the AU's development of legal and regulatory structures for cyberspace, an essential role is played by the African Network Information Centre (AFRINIC), the region's Regional Internet Registry[745]. As the steward of Internet Protocol (IP) resources within Africa, AFRINIC is tasked with managing the distribution and registration of these resources[746]. It carries out this responsibility while adhering to international guidelines and its own policies, the formulation of which carries profound legal implications[747]. The AFRINIC Government Working Group (AFGWG) also plays a significant role in the development of regional cyber law by serving as a conduit for consultation and dialogue between AFRINIC, African governments, law enforcement agencies, and other stakeholders[748]. The AFGWG allows for the diffusion of best practices, fosters collaborative decision-making and, importantly, serves as a catalyst for the harmonisation of cyber law across the continent[749]. Furthermore, AfricaCERT, the official forum of CSIRTs, rely on the guidance and regional definitions as outlined by AFRINIC[750]. AfricaCERT follows the CSIRT model used by the OAS's CICTE in the Americas, and has been instrumental in building both technical and policy-level cybersecurity capacities in Africa[751]. The regional cooperation, facilitated by AfricaCERT, has played a significant role in the enforcement of national cyber laws among its member states, and as such has contributed to the development and refinement of cyber law frameworks[752]. However, unlike the American region where the OAS and the Global Forum on Cyber Expertise (GFCE) have established a significant collaborative initiative, a similar stable and robust partnership are yet to be established in the African region[753].

[744] Chapter V of the 'Directive on Fighting Cyber Crime within ECOWAS'.
[745] AFRINIC, 'About Us', *African Network Information Centre: Internet Numbers Registry for Africa*, 2023 <https://afrinic.net/about> [accessed 26 June 2023].
[746] AFRINIC, 'IPv6 Resources from AFRINIC', *African Network Information Centre: Internet Numbers Registry for Africa*, 2023 <https://afrinic.net/resources/ipv6> [accessed 26 June 2023].
[747] AFRINIC, 'Governance', *African Network Information Centre: Internet Numbers Registry for Africa*, 2023 <https://afrinic.net/governance> [accessed 26 June 2023].
[748] AFRINIC, 'AFRINIC Government Working Group (AFGWG)', *African Network Information Centre: Internet Numbers Registry for Africa*, 2023 <https://afrinic.net/committees/afgwg> [accessed 26 June 2023].
[749] T. Nyirenda-Jere and T. Biru, 'Internet Development and Internet Governance in Africa', *Internet Society*, 2015, 1–44.
[750] Cybil Portal, 'AfricaCERT', 2023 <https://cybilportal.org/actors/africacert/> [accessed 26 June 2023].
[751] P. Pawlak and P. N. Barmpaliou, 'Politics of Cybersecurity Capacity Building: Conundrum and Opportunity', *Journal of Cyber Policy*, 2.1 (2017), 123–44.
[752] Rene Nkongho Eno-Akpa, *The Case for an African Solution to Cybercrime: A Critical Assessment of the African Union Convention on Security in Cyberspace and Personal Data Protection* (Nkozi, 2016) <https://www.newshosting.com/blog/internet-security-defending->.
[753] Amazouz.

4.8. Analysis at regional level

Scrutinising the intersection of human rights and cyber law across the European, American, and African regions brings to light fundamental disparities in the maturity and breadth of these legal domains. Human rights law, rooted in longstanding international[754] and regional conventions[755], presents a multidimensionality that encompasses the spectrum of substantive rights[756], procedural guarantees[757], mechanisms of enforcement[758], and an established jurisprudence[759]. This provides a well-defined and robust foundation for the enforcement and safeguarding of rights, including the protection of Article 25(b) of the ICCPR. Cyber law, in contrast, while growing rapidly in response to technological advancement, reveals a relative dearth of sophistication across these same areas[760]. Its substantive provisions are often narrower[761], procedural aspects more sporadic[762], and the mechanisms of enforcement less universal[763] and harmonised[764], revealing an infant field of legal specialisation navigating an intricate digital landscape. Article 25(b) of the ICCPR ensures the right of every citizen "to vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors"[765]. This article implies the necessity of an unbiased and undistorted information landscape, a condition which appears to be at odds with the content personalisation practices of social media corporations, that have the express purpose of extracting value from the 'Attention Economy' through the promotion of certain content at the expense of other content[766] – practices which have been demonstrate to result in "filter bubbles"[767], "echo chambers"[768], and even "stochastic terrorism"[769], that distort political discourse[770]. As discussed in the preceding sections, content personalisation practices, through the lens of evolutionary

[754] Preamble of the 'International Covenant on Civil and Political Rights', *2200A(XXI), Adopted 23 March 1976*.
[755] Preamble of the 'European Convention on Human Rights', *ETS No. 005 Adopted in Rome on 4 November 1950*.
[756] Article 23(1) of the 'American Convention on Human Rights'.
[757] García-Sayán.
[758] Section 2 of the 'European Convention on Human Rights', *CoE Treaty Series 005, Adopted on 4 November 1950* <https://doi.org/10.1017/S0008197300013908>.
[759] Djeffal.
[760] Monika Zalnieriute, 'Reinvigorating Human Rights in Internet Governance: The UDRP Procedure through the Lens of International Human Rights Principles', *Columbia Journal of Law & Arts*, 43 (2020), 197–235 <https://heinonline.org/HOL/Page?handle=hein.journals/cjla43&id=205&div=11&collection=usjournals>.
[761] Article 2 of the 'Supplementary on Personal Data Protection within ECOWAS'.
[762] Chapter V of the 'Directive on Fighting Cyber Crime within ECOWAS'.
[763] Contreras and Barrett.
[764] Babalola.
[765] Article 25(b) of the International Covenant on Civil and Political Rights.
[766] Myllylahti.
[767] Grossetti, Mouza, and Travers.
[768] Orlowski.
[769] Amman and Meloy.
[770] Grossetti, Mouza, and Travers.

psychology, exploit humans' inherent tribal tendencies[771] and thus would arguably inevitably result in social fragmentation, political polarisation, and the rise of populist ideologies in the absence of direct regulatory measures. The question here is, given that social fragmentation and political polarisation have a societal level impact, how would that manifest as a violation of individual rights? Significantly, Article 20 of GDPR stands as a rare provision that not only protects individual rights, but also acknowledges their co-existence with public interest[772]. This is arguably the only piece of substantive regional cyber law that addresses societal impact, thereby hinting at a potential pathway for addressing the societal consequences of social media content personalisation

The analysis presented in this section reveals a significant commitment within the European region's legal frameworks for preserving human rights in the cyber space. The GDPR's principles like the right to be forgotten[773], data portability[774], and data minimisation[775] have globally reshaped the conversation around data protection and privacy. In particular, Article 9 of the GDPR safeguards against processing of personal data revealing political opinions, which can potentially be linked to practices of social media content personalisation[776]. Also, Article 11 prescribes limits to personal data processing[777], a provision that appears to be in conflict with pervasive content personalisation practices. However, this does not necessarily prevent the potential manipulation of public opinion through algorithmic bias, as the GDPR focuses more on personal data privacy and control rather than addressing the wider societal consequences of data usage. The NIS 2 Directive, in turn, while primarily targeting cybersecurity, mandates entities to manage the risks posed to their network and information systems[778]. The scope of this legislation could be interpreted to include the mitigation of societal risks like those posed by manipulative content personalisation. However, the

[771] Molenberghs.
[772] Article 20(3) of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].
[773] Paragraph 14 of Google v. González.
[774] Article 20(3) of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].
[775] Article 5(1)(c) of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].
[776] Article 9(1) of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].
[777] Article 11(1) of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].
[778] Para. 3 of the 'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for the High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and the Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)'.

Directive's primary focus on securing essential services[779] implies a limited application to the concerns of Article 25(b) of the ICCPR. Developments in regional jurisprudence, such as that seen in the cases of *Google Spain v AEPD and Mario Costeja González* and *Delfi AS v Estonia* signal progress towards the socially responsible use of personal data by third parties[780]. However, these cases mainly emphasise individual data privacy and control, while the broader societal effects of content personalisation remain a largely unaddressed issue in jurisprudence; which begs the question, how does one prove social fragmentation or political polarisation at an individual rights level? Currently, it seems the onus of navigating the complex terrain of digital manipulation is largely placed on individuals, who are expected to actively opt out of content personalisation should they desire to do so. The shift of responsibility to individual users arguably represents a failure in regional mechanisms to enable European states to fulfil their positive obligations for protecting the human right to participate in the conduct of public affairs "by universal and equal suffrage" and in a manner that "[guarantees] the free expression of the will of the electors"[781]. Indeed, how does one prove a distortion of public discourse, and how does one prove that it violated individual rights? Therefore, the existing legal frameworks in the European region, while advanced and comprehensive in many aspects, do not sufficiently address the risks posed by social media content personalisation in the context of potential violations of Article 25(b) of the ICCPR. The substantive provisions, procedural guarantees, and mechanisms of enforcement of cyber law must therefore evolve further to adequately address these challenges and align more closely with the multidimensional protections offered by human rights law.

In the American region, OAS member states have also demonstrated notable strides in establishing cyber law frameworks aimed at cybersecurity capacity building, threat mitigation, and the promoting of international cooperation[782]. This distinctly more pragmatic approach, however, leaves questions unanswered when assessing the effectiveness of preventing social media content personalisation practices from violating Article 25(b) of the ICCPR. The American region's proactive stance on cybersecurity, as manifested in the Comprehensive

[779] Para. 2 of the 'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for the High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and the Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)'.
[780] Agnes Callamard, 'Are Courts Re---Inventing Internet Regulation?', *International Review of Law, Computers & Technology*, 31.3 (2017), 323–39 <http://www.asef.org/images/stories/publications/documents/ASEF->.
[781] Article 25(b) of the International Covenant on Civil and Political Rights.
[782] Inter-American Portal on Cybercrime, 'Home Portal'.

Inter-American Cybersecurity Strategy[783], CMMs[784], and the GFCE-OAS Regional Hub[785], represents robust responses to cyber threats. However, while these initiatives have set standards for cybersecurity, their focus is predominantly on the technical aspects of cybersecurity and threat mitigation[786], rather than addressing potential human rights implications, including possible violations of Article 25(b).

While regional networks such as national CSIRTs[787] and REMJA[788] have shown promise in terms of information sharing and enforcement of national cyber law, their effectiveness is contingent on consistent interpretation and application of these laws across diverse national jurisdictions[789]. Furthermore, while exceedingly pragmatic and proactive compared to the European region, the American region lacks a harmonised legal doctrine[790] to effectively adjudicate matters related to human rights in cyberspace, which arguably presents limitations to which OAS member states are able to meet their positive obligation to protect the human right to participate in the conduct of public affairs "by universal and equal suffrage" and in a manner that "[guarantees] the free expression of the will of the electors"[791]. Indeed, American nations' adherence to the Budapest Convention[792], and judicial precedents set by IACtHR rulings in cases such as *Escher et al. v Brazil* and *Rios et al. v Venezuela*, signal an acknowledgement of the need to protect fundamental human rights such as the right to privacy[793] and freedom of thought and expression[794] in the digital age; yet, there remains a notable gap in regional mechanisms that would enable OAS member states to address the intricate and nuanced risks social media content personalisation practices pose to Article 25(b) of the ICCPR.

Cyber law in Africa has seen robust initiatives from the AU and a variety of sub-regional organisations such as the EAC and ECOWAS. However, akin to trends in Europe and America,

[783] OAS General Assembly, 'Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity'.
[784] Mori and Goto.
[785] GFCE.
[786] OAS General Assembly, 'Resolution Advancing Hemispheric Security: A Multidimensional Approach'.
[787] CSIRTAmericas.
[788] Meeting of Ministers of Justice or Other Ministers or Attorney General of the Americas, 'Document on the REMJA Process (Document of Washington)'.
[789] Section V(6) of 'Conclusions and Recommendations of REMJA IX', *REMJA-IX//Doc.2/12 Rev. 1, Adopted in Quinto, on 29 November 2012*, 2012.
[790] de Arimatéia da Cruz and Godbee.
[791] Article 25(b) of the International Covenant on Civil and Political Rights.
[792] Section B(3) of 'Conclusions and Recommendations to REMJA XI', *REMJA-IX/DOC.2/21 Rev. 1, Held Virtually on 19 May 2021*.
[793] Dahlmann et al.
[794] Paragraph 69 of 'Ríos v Venezuela'.

cyber law protections in Africa remain in the emergent stages of legal practice and scholarship[795]. These stages are characterised by significant limitations, and more specifically as it pertains to this mini-thesis, insufficient mechanisms for preventing human rights violations in cyberspace[796]. The evolution of cyber law in Africa can be distinguished from other regions by an apparent focus on economic development[797]. Notable examples of this focus include the AU's dedicated STC for Communication and Information Communications Technology[798], the EAC's regional cyber law framework supporting an e-commerce integration process[799], and ECOWAS's Directive on Fighting Cybercrime[800]. While distinct in its apparent emphasis on supporting economic development, the cyber law landscape in Africa does share some characteristics with the European and American regions. For example, the AU has adopted the Malabo Convention on Cyber Security and Personal Data Protection[801], a step that parallels the European legalistic approach, exemplified by the Budapest Convention[802], its various protocols[803], and the GDPR[804]. Like the more legalistic approach in Europe, exemplified by the Budapest Convention[805] and GDPR[806]. Furthermore, evidence of a more pragmatic emphasis on collaborative cybercrime prevention is present among OAS states[807], the AUC has also established bodies like the ACS3C and the AUCSEG to facilitate the implementation of the Malabo Convention[808].

With regards to social media content personalisation specifically, the AU's Internet Infrastructure Security Guidelines[809] and the Malabo Convention's provisions on personal data protection[810] could theoretically provide some safeguards. Such claims, however, would require that applicants are able to provide evidence of a direct link between content personalisation activities on their social media account and their ability to "participate freely

[795] ALT Advisory, 'Africa: AU's Malabo Convention Set to Enter Force after Nine Years'.
[796] Anja Mihr, *Cyber Justice: Human Rights and Good Governance for the Internet* (Cham, Switzerland: Springer, 2017).
[797] Ndizera and Muzee.
[798] African Union, 'Specialised Technical Committees'.
[799] UNCTAD.
[800] ECOWAS, 'Directive on Fighting Cyber Crime within ECOWAS'.
[801] Ayalew.
[802] Preamble of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[803] Seger.
[804] Das.
[805] Seger.
[806] Das.
[807] OAS General Assembly, 'Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity'.
[808] Tomáš Minárik and Audrey Garcia, 'Internet Infrastructure Security Guidelines for Africa Unveiled by the African Union', *CCDCOE*, 2017 <https://ccdcoe.org/incyder-articles/internet-infrastructure-security-guidelines-for-africa-unveiled-by-the-african-union/> [accessed 19 July 2023].
[809] AU Commission and Internet Society.
[810] Chapter II of the 'African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)'.

in the government of his country" as protected by Article 13(1) of the ACHPR[811], again placing the onus of navigating the complex terrain of digital manipulation on the individual. In the African context specifically, such a burden shift is exceedingly problematic given current regional capability to enforce these frameworks. The Malabo Convention, though ambitious and comprehensive, lacks mechanisms for enforcement[812]. Additionally, a gap exists between the adoption of the legal framework and the practical enforcement capacity among AU member states, a situation further compounded by the absence of DPAs in many of these nations[813].

Juxtaposing the right to participate in the conduct of public affairs with developments in cyber law across the European, American and African regions reveals important similarities and differences. Each region displays an effort to navigate the legal complexities of a rapidly evolving digital age, albeit with varied approaches and distinct challenges. The divergences represent the relative infancy of cyber law, whose provisions have not yet achieved the breadth, sophistication, and universal applicability of established human rights law across all three regions. This is a critical point in view of the proliferation of social media and the associated risks content personalisation practices pose to Article 25(b) of the ICCPR. A shared shortcoming lies in the fact that none of these regions' legal frameworks adequately address the complex threats posed by social media content personalisation practices to the right to participate freely in public affairs. There is no provisioning of substantive legal protections that address the wider societal impact of social media content personalisation as human rights that pertain to participation in public affairs are codified as individual rights, as opposed to people's rights, in Article 3 of Protocol No. 1 to the ECHR[814], Article 23(1) of the ACHR[815] or Article 13(1) of the ACHPR[816]. Substantive rights regarding personal data in reginal instruments also lack sufficient nuance that would allow for such substantial law to be applied this very specific human rights context. It is also unclear how the procedural laws of human rights and cyber law instruments might be applied to claims of such violations. Finally, enforcement presents a challenge, especially for the American and African region. Both the OAS and AU have significant incongruencies in the adoption of regional cyber law frameworks which, given the borderless nature of social media, places severe restrictions on the extent to which they can be

[811] Article 13(1) of the Organization of African Unity.
[812] Vallée and Hsu.
[813] Ilori.
[814] Article 3 of 'Protocol No. 1 to the European Convention on Human Rights and Fundamental Freedoms', *ETS No. 009, Adopted in Paris on 20 March 1952*.
[815] Article 23(1) of the 'American Convention on Human Rights'.
[816] Article 13(1) of the Organization of African Unity.

enforced. In sum, it appears that regional mechanisms currently do not enable states to reconcile their dual obligations effectively. States have a positive obligation to ensure free and fair political participation, juxtaposed against a negative obligation to refrain from arbitrary interference with an individual's rights to autonomy, the free exercise of will, and freedom of thought and expression. Balancing these obligations is of paramount importance to prevent social media content personalisation practices from violating Article 25(b) of the ICCPR.

CHAPTER 5: DOMESTIC FRAMEWORK

5.1. Introduction

This chapter explores the harmonisation of international and regional social media regulation at a domestic level, with a specific focus on the UK, the US, and South Africa. The chapter starts with an examination of the UK's approach to regulating social media, particularly in light of the societal impacts of content personalisation. The chapter examines the foundational legal frameworks underpinning developments in human rights and cyber law in the UK, to the more recent Online Harms White Paper and Online Safety Bill. The chapter then presents an overview of the US's commitment to its First Amendment freedoms, alongside the distinct legal and political landscape shaping its approach to social media regulation. The chapter assesses the US's efforts to address the challenges posed by social media algorithms and their potential impact on public discourse and democratic processes. The chapter then moves on to South Africa, and presents an exploration of the country's unique journey from an Apartheid regime to a champion for human rights, tracing how this historic transition influences the country's contemporary approach to cyber law. The chapter traces notable legislative developments and challenges in South Africa, including the implementation of the POPI Act and amendments to the Film and Publications Act. The chapter concludes with a comparative analysis at the domestic level across the UK, US, and South Africa.

5.2. International and regional harmonisation of social media regulation in the United Kingdom

Public discourse in the UK has not been immune to the collateral damage caused by social media content personalisation[817]. Given the prevalence of social media use in the country, at an approximate 84% of the total population[818], this wider societal impact presents a significant legal problem. Signalling the country's acknowledgement of this problem, and a need to reform domestic cyber law's governance of social media, the UK government's Online Harms White Paper of 2019, and subsequent Draft Online Safety Bill of 2021, advocates for a new "duty of care" for companies that permit the sharing of user-generated content or engage with users

[817] Laura Alonso-Muñoz and Andreu Casero-Ripollés, 'Populism against Europe in Social Media: The Eurosceptic Discourse on Twitter in Spain, Italy, France, and United Kingdom during the Campaign of the 2019 European Parliament Election', *Frontiers in Communication*, 5.54 (2020), 1–12 <https://doi.org/10.3389/fcomm.2020.00054>.
[818] Simon Kemp, 'Digital 2023: The United Kingdom', 2023 <https://datareportal.com/reports/digital-2023-united-kingdom#:~:text=The UK was home to,percent of the total population.> [accessed 19 July 2023].

online[819]. The proposed consequences for non-compliance include fine structures[820], similar to the GDPR[821], and other forms of government sanctions[822]. Before examining the current state of social media regulation in the UK, however, it is important to consider the foundational landscape of human rights and cyber law from which this regulation emerges.

The UK has been a party to the UDHR since its adoption by the UN General Assembly in 1948[823]. The UDHR's principles, such as the provisions of Article 21 regarding the right to take part in the government of one's country, serve as the foundation for many of the UK's domestic laws[824]. The UK is also became a signatory to the ECHR in 1953[825], Protocol No. 1 to the ECHR in the following year [826], and the ICCPR in 1976[827], offering international and regional hard law reinforcement of the soft law principles contained in the UDHR. Reflecting the ICCPR's provisions for the right to freedom of thought[828], freedom of expression[829], and the right to participate in the conduct of public affairs[830], as well as Protocol No. 1 to the ECHR's protection of free and fair elections[831], is the Representation of the People Act of 1983, the Human Rights Act of 1998, and their subsequent amendments[832]. The Representation of the People Act provides a comprehensive statutory framework for the right to vote and run for office in elections. The Human Rights Act, in turn, closely mirrors the ECHR and its Optional Protocols, protecting freedom of thought[833], freedom of expression[834], and the right to participate in free elections[835].

[819] L. Woods, 'The Duty of Care in the Online Harms White Paper', *Journal of Media Law*, 11.1 (2019), 6–17.
[820] Para. 6.4 of the 'Online Harms White Paper (CP 57)', *HM Government*, 2019 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf> [accessed 20 July 2023].
[821] Article 83 of the 'General Data Protection Regulation'.
[822] Para. 6.3 of the 'Online Harms White Paper (CP 57)', *HM Government*, 2019 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf> [accessed 20 July 2023].
[823] United Nations, 'Member States', *Universal Declaration of Human Rights* <https://www.un.org/en/about-us/member-states#gotoU> [accessed 22 July 2023].
[824] Tom Obokata and Rory O'Connell, 'The Universal Declaration of Human Rights and the United Kingdom: Developing a Human Rights Culture', in *60 Years of the Universal Declaration of Human Rights in Europe*, ed. by M. Suksi and V. Jaichand (Antwerp: Intersentia, 2009).
[825] Council of Europe, '46 Member States'.
[826] Council of Europe Treaty Office, 'Chart of Signatures and Ratifications of Treaty 009' <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=009> [accessed 19 April 2023].
[827] United Nations, 'Parties to the International Covenant on Civil and Political Rights'.
[828] Article 18(1) of the 'International Covenant on Civil and Political Rights'.
[829] Article 19(2) of the 'International Covenant on Civil and Political Rights'.
[830] Article 25 of the 'International Covenant on Civil and Political Rights'.
[831] Article 3 of the 'Protocol No. 1 to the European Convention on Human Rights and Fundamental Freedoms'.
[832] Tom Lewis, '"Diffcult and Slippery Terrain": Hansard, Human Rights and Hirst v UK', *Public Law*, 2006, 209–18.
[833] Article 9(1) of the *Human Rights Act* (United Kingdom, 1998).
[834] Article 10(1) of the *Human Rights Act* (United Kingdom, 1998).
[835] Protocol 1, Article of the *Human Rights Act* (United Kingdom, 1998).

With regards to cyber law, the UK has been a party to the Budapest Convention since 2011[836] and the GDPR since 2018[837]. However, given the UK's withdrawal from the EU, the NIS 2 Directive did not come into force on 23 January of 2023[838]. Resultantly, the Budapest Convention and the GDPR are primarily reflected in the Computer Misuse Act of 1990, and its subsequent amendments, the Data Protection Act of 2018, and the post-Brexit' UK GDPR'. The Computer Misuse Act of 1990, a seminal piece of legislation in the UK, was pivotal in criminalising unauthorised access to computer material[839]. Yet, it's been criticised for its narrow purview and inability to deal with contemporary cyber threats like ransomware attacks and distributed denial-of-service attacks[840]. More so, it appears to lack the granular detail present in Budapest Convention Article 14[841] concerning the intentional and without right damaging, deletion, deterioration, alteration or suppression of computer data. Efforts to evolve the Act to address these and other criticisms most notably include amendments by the Police and Justice Act of 2006, which expanded the Act's scope by introducing a new offence of making, supplying or obtaining articles for use in computer misuse offences[842], and amendments by the Serious Crime Act of 2015 that criminalised cyber-attacks that result in severe damage to the economy, environment, national security, or human welfare[843].

More recently, the Data Protection Act of 2018 was amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, as part of the UK's Brexit process[844]. This amendment ensured the domestication of the principles of the GDPR into UK law, resulting in a subtly transformed 'UK GDPR' after the country's exit from the EU on 31 January 2020[845], in accordance with the European Union (Withdrawal) Act 2018[846]. There does, however, appear to be some incompatibility with this post-Brexit cyber law landscape and the human rights of freedom of thought, freedom of expression, and the right

[836] Council of Europe, 'Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY'.
[837] Das.
[838] Marija Nonkovic, 'Government Confirms Proposals to Reform the NIS Regulations in Order to Strengthen UK Cyber Resilience', *Lexology*, 2023 <https://www.lexology.com/library/detail.aspx?g=2309c1d3-7bec-4b2e-b7e1-a8824fe74777> [accessed 22 July 2023].
[839] A. Charlesworth, 'Legislating against Computer Misuse: The Trials and Tribulations of the UK Computer Misuse Act 1990', *Journal of Law, Information and Science*, 4.1 (1993), 80–93.
[840] Neil MacEwan, 'The Computer Misuse Act 1990: Lessons from Its Past and Predictions for Its Future', *Criminal Law Review*, 12.1 (2008), 955–67.
[841] Article 14 of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[842] Section 35 - 38 of the *Police and Justice Act* (United Kingdom, 2006).
[843] Section 41 – 44 of the *Serious Crime Act* (United Kingdom, 2015).
[844] Regulation 4 of the '*The Data Protection, Privacy and Electronic Communications (Amendments Etc) (EU Exit) Regulations* (United Kingdom, 2019)'. <https://www.legislation.gov.uk/ukdsi/2019/9780111177594/contents> [accessed 21 July 2023].
[845] Para. 2 of the '*Exiting the European Union Data Protection Electronic Communications Draft Statutory Instruments*' (United Kingdom, 2019).
[846] Section 2(1) of the '*European Union (Withdrawal) Act*' (United Kingdom, 2018).

to participate in free elections. A central theme among these apparent incompatibilities arises from the inherent risk of misuse of personal data. The freedom of expression to hold opinions and to receive and impart information and ideas without interference by a public authority[847], for example, can potentially be undermined by the wide-ranging sanctions against non-compliance embedded within the UK's domestic data protection laws[848]. It can be argued that, while these laws aim to prevent online harms and protect user data, they could inadvertently restrict online discourse and penalise users for expressing their thoughts, thereby discouraging democratic participation. Furthermore, the Protocol No. 1 to the ECHR mandates free and fair elections[849], closely intertwined with the right to freedom of thought[850] and expression[851]. The expansive data collection and processing powers granted by cyber law[852], however, can potentially manipulate public opinion or exploit electoral processes, infringing upon this fundamental democratic right.

With regards to social media more specifically, the current landscape in the UK is heavily debated and significant decisions are currently being made to protect consumers from the way in which private companies leverage, monetise, and possibly abuse massive amounts of user behavioural, purchasing, and demographic data[853]. Mounting concerns regarding the wider societal impact of social media have prompted the UK government's release of its Online Harms White Paper in 2019[854]. The UK has embraced internet censorship before, such as its (now-abandoned) plan to require an 'internet driver's license' to view online pornography, but it is argued that the level of censorship currently proposed is unmatched by any other Western democracy[855]. This white paper sets out an ambitious plan for the regulation of the internet to protect citizens from harm that might arise from the consumption of online content. The white paper proposes establishing a new "duty of care" towards users, to be upheld by tech companies and enforced by an independent regulator. The white paper covers a broad array of online

[847] Article 10(1) of the *Human Rights Act* (United Kingdom, 1998).
[848] Schedule 15 of the '*Data Act Protection*' (United Kingdom, 2018).
[849] Article 3 of the 'Protocol No. 1 to the European Convention on Human Rights and Fundamental Freedoms'.
[850] Article 9 of the *Human Rights Act* (United Kingdom, 1998).
[851] Article 10 of the *Human Rights Act* (United Kingdom, 1998).
[852] Schedule 15 of the '*Data Act Protection*' (United Kingdom, 2018).
[853] Myojung Chung and John Wihbey, 'Social Media Regulation, Third-Person Effect, and Public Views: A Comparative Study of the United States, the United Kingdom, South Korea, and Mexico', *New Media and Society*, 00.0 (2022), 1–20 <https://doi.org/10.1177/14614448221122996>.
[854] Woods.
[855] Eric Goldman, 'The UK Online Harms White Paper and the Internet's Cable-Ized Future', *Ohio State Technology Law Journal*, 16.2 (2020), 351–62 <https://www.bbc.com/news/technology-50073102>.

harms, including but not limited to cyberbullying[856], dissemination of terrorist and extremist content[857], child sexual exploitation[858], and the promotion of self-harm and suicide[859]. Interestingly, in contrast to other cyber law instruments that address individual rights across contexts, the Online Harms White Paper addresses very specific, societal impacts of the internet, such as "[the] Electoral Commission's oversight of the activity of political parties, and other campaigners, including activity on social media" as a significant shortcoming of the current regulatory landscape[860], the need for an independent regulator with the "power to inspect algorithms in situ, to understand their use of personal data and whether this leads to bias or other detriment"[861], and a need for mechanisms that require social media companies "to ensure that algorithms selecting content do not skew towards extreme and unreliable material in the pursuit of sustained user engagement"[862].

The cyber law reform proposed by this white paper, however, is not without its critique. Most notably, criticism represents fears that the proposed regulatory changes could inadvertently harm free speech and even tilt towards authoritarian tendencies, particularly in its approach to "harms which may be legal but harmful[863]"[864]. Such concerns represent the potential for incompatibility freedom of thought, conscience, and religion, and the freedom of expression and information, under the provisions of Articles 18 and 19 of the UDHR, Articles 1(3) and 2(3)(a) of the ICCPR, and Article 34 of the ECHR. Critics also call into question potential

[856] Para. 7.43 - 7.47 of the 'Online Harms White Paper (CP 57)', *HM Government*, 2019 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf> [accessed 20 July 2023].
[857] Para. 3.10 - 3.12 of the 'Online Harms White Paper (CP 57)', *HM Government*, 2019 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf> [accessed 20 July 2023].
[858] Para. 1.6 - 1.7 of the 'Online Harms White Paper (CP 57)', *HM Government*, 2019 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf> [accessed 20 July 2023].
[859] Para. 7.32 - 7.35 of the 'Online Harms White Paper (CP 57)', *HM Government*, 2019 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf> [accessed 20 July 2023].
[860] Para. 2.5 of the 'Online Harms White Paper (CP 57)', *HM Government*, 2019 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf> [accessed 20 July 2023].
[861] Para. 2.4 of the 'Online Harms White Paper (CP 57)', *HM Government*, 2019 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf> [accessed 20 July 2023].
[862] Para. 7.30 of the 'Online Harms White Paper (CP 57)', *HM Government*, 2019 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf> [accessed 20 July 2023].
[863] Para. 3.5 of the 'Online Harms White Paper (CP 57)', *HM Government*, 2019 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf> [accessed 20 July 2023].
[864] Peter Pomerantsev, 'A Cycle of Censorship: The UK White Paper on Online Harms and the Dangers of Regulating Disinformation', *Transatlantic Working Group on Content Moderation Online and Freedom of Expression*, 2019 <www.annenbergpublicpolicycenter.org/twg>.

impacts on political discourse and electoral processes that represent an expression free will[865], that are protected under Article 21 of the UDHR, Article 25(b) of the ICCPR, and Article 3 of Protocol No. 1 to ECHR. The potential for regulatory uncertainty, high compliance costs, and the blurring of boundaries between "illegal" and "harmful" content, coupled with threats to freedom of expression, feature prominently among criticisms[866]. Critics also call into question the ambiguity of the keystone concept of a "duty of care" and the necessity of a two-tier regulatory system differentiating definite harms from those that might be more ambiguous[867]. Here, the expansive approach of the regulatory reform proposed by the white paper may not be compatible with the Budapest Convention's specific provisions under Articles 14 to 18, despite its attempts to respond to newer forms of cybercrime. However, the proposed regulation that addresses user-generated content and its algorithmic manipulation may, however, complement the GDPR's provisions on data protection – specifically Articles 9(1), 11(1), 18, 20, and 22. The proposed powers of enforcement are also argued to go beyond what is permitted in the offline world, with calls for a clearer distinction between "harmful content" and "illegal harmful content"[868]. While its aims have been ostensibly noble, the Online Harms White Paper's proposed regulatory framework has been argued to lack a proportionate approach, with calls for the primacy of freedom of expression and participatory rights, reflected in Articles 1 and 2 of the UDHR, in any social media regulation[869].

Following the Online Harms White Paper, the UK's Draft Online Safety Bill (CP 405) of 2021 seeks to articulate a framework that regulates social media[870] and addresses the societal impacts arising from content personalisation[871]. The foundational principle of a duty of care is comprehensively extrapolated from the Online Harms White Paper into this draft bill[872]. All

[865] Frederick Mostert, '"Digital Due Process": A Need for Online Justice', *Journal of Intellectual Property Law & Practice*, 2020 <https://doi.org/10.1093/jiplp/jpaa024>.
[866] Damian Tambini, 'The Differentiated Duty of Care: A Response to the Online Harms White Paper', *Journal of Media Law*, 11.1 (2019), 28–40 <https://doi.org/10.1080/17577632.2019.1666488>.
[867] Stefan Theil, 'The Online Harms White Paper: Comparing the UK and German Approaches to Regulation', *Journal of Media Law*, 11.1 (2019), 41–51 <http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=E23D493>.
[868] Harbinja E, Leiser MR, Barker K, Mangan D, Romero-Moreno F and Dushi D, *Online Harms White Paper: Consultation Response [BILETA Response to the UK Government Consultation 'Online Harms White Paper']*, 2019 <http://www.europarl.europa.eu/charter/pdf/text_en.pdf.>.
[869] Kim Barker and Olga Jurasz, 'Online Harms White Paper Consultation Response', *Stirling Law School & The Open University Law School*, 2019.
[870] Section 1(1) of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].
[871] Section 13 of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].
[872] Trengove M, Kazim E, Almeida D, Hilliard A, Zannone S and Lomas E, 'A Critical Review of the Online Safety Bill', *Patterns*, 3.8 (2022), 100544 <https://doi.org/10.1016/j.patter.2022.100544>.

providers of user-to-user services[873] and search services[874] have an obligation to prevent user exposure to harmful content. To operationalise these principles, the draft bill specifically designates OFCOM, the UK's communications regulator, as the enforcing authority for this legislation[875]. The bill also lays out clear obligations for the providers, to conduct risk assessments[876] and outlines reporting responsibilities[877]. The draft bill introduces very specific "duties to protect content of democratic importance", which creates an obligation for social media companies to understand the risks associated with their platforms and mitigate them appropriately, the level of compliance to which OFCOM has the power to demand information[878].

The imposition of a duty of care on user-generated online platform providers marks a significant departure from the reactive moderation approach generally adopted by internet services[879]. Concurrently, however, the wording of the draft bill echoes many of the criticisms of proposed regulatory change contained in the Online Harms White Paper regarding the risks of excessive censorship stifling freedom of thought and expression[880]. The bill contains a specific provision for social media companies "to operate a service using systems and processes designed to ensure that the importance of the free expression of content of democratic importance"[881]. This distinctly proactive approach demonstrates how domestic cyber law can

[873] Section 5 of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].
[874] Section 17 of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].
[875] Section 1(1) of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].
[876] Section 7 of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].
[877] Section 15 of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].
[878] Section 75 - 77 of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].
[879] Irfan Chaudhry and Anatoliy Gruzd, 'Expressing and Challenging Racist Discourse on Facebook: How Social Media Weaken the "Spiral of Silence" Theory', *Policy and Internet*, 9999.9999 (2019), 1–21 <https://doi.org/10.1002/poi3.197>.
[880] Pomerantsev, 'A Cycle of Censorship: The UK White Paper on Online Harms and the Dangers of Regulating Disinformation'.
[881] Section 13(2) of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].

be used as a mechanism for ensuring that the protection of democratic processes[882] does not come at the expense of social liberties such as freedom of thought[883] and expression[884].

While the letter of the law in this draft bill does acknowledge the risk of regulating online content infringing on the freedom of thought and expression[885], some critics maintain that inherent risks are presented by the practical application of the bill's statutory duties. The penalty regime allows for fines of up to £18 million[886] or 10%[887] of a company's global turnover. It is argued that such severe penalties could lead to over-compliance and excessive caution on the part of social media companies, which risks material constraints on users' freedom of thought and expression[888], as well as users' privacy rights[889]. In contrast, the first version of the draft bill's response to commentary on ambiguity regarding the concepts of "illegal" versus "legal but harmful" sets out clear guidelines for determining if content can be considered "legal but harmful" through a risk assessment process[890]. In the more recent amended bill, announced on 28 November 2022, revisions have notably excised provisions related to the regulation of "legal but harmful" content, resulting in a profound shift in the legislation's initial stance. While the revised bill, which is currently under review in the House of Lords[891], incorporates mechanisms to shield users from specified harmful materials and criminalises certain digital transgressions, critics assert that this regulatory transformation may dilute the fight against pervasive online harms and limit the flexibility of social media companies to counter emerging online freedom of speech issues.[892] With regards to the specific question posed by this mini-thesis, both the draft and revised version of the Online Safety Bill

[882] Article 21 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948*.
[883] Article 18(1) of the 'International Covenant on Civil and Political Rights'.
[884] Article 10 of the 'European Convention on Human Rights', *CoE Treaty Series 005, adopted on 4 November 1950.*
[885] Section 13(2) of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].
[886] Section 85(4)(a) of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].
[887] Section 85(4)(b) of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].
[888] Trengove et al.
[889] Article 9(1) of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].
[890] Section 7(10) of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].
[891] House of Lords, 'Online Safety Bill', *Parliamentary Bills*, 2023 <https://bills.parliament.uk/bills/3137>.
[892] M. MacCarthy, *U.K. Government Purges Legal but Harmful Provisions from Its Revised Online Safety Bill* (Washington D.C., 2022).

still do not sufficiently address the 'black box problem'[893] of how social media algorithms function, with the closest reference to this niche issue being Section 235(4)(a):

> "References to harm presented by content, and any other references to harm in relation to content, include references to cumulative harm arising or that may arise in the following circumstances—
>
> (a) where content, or content of a particular kind, is repeatedly encountered by an individual (including, but not limited to, where content, or a kind of content, is sent to an individual by one user or by different users or encountered as a result of algorithms used by, or functionalities of, a service);"

This reference to cumulative harm and the role of algorithms could potentially be seen as an attempt to align domestic legislation with Article 22 of the GDPR, which speaks to the right to not be subject to decisions based solely on automated processing[894]. However, the lack of specific regulation around the functioning of algorithms could also be seen as a gap in achieving full compliance with this GDPR provision. While the revised Online Safety Bill is a significant step towards comprehensive social media regulation, ongoing critique and debate reveal the challenge of regulating cyberspace while preserving essential human rights and democratic values.

5.3. International and regional harmonisation of social media regulation in the United States

The rise of populism and the noticeable shift towards right-wing nationalism in recent years are defining characteristics of the contemporary political landscape in the United States[895]. Social media platforms, significantly influencing public discourse, appear to be at the epicentre of these seismic shifts[896]. As discussed in previous sections, social algorithms that indiscriminately tailor content to individual user profiles in order to maximise platform engagement, reinforcing existing biases and a lack of understanding of different perspectives

[893] U. Reviglio and C. Agosti, 'Thinking Outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media', *Social Media+ Society*, 6.2 (2020), 2056305120915613.
[894] Article 22 of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].
[895] Bart Bonikowski, 'Three Lessons of Contemporary Populism in Europe and the United States Populism in the Twenty-First Century', *Brown Journal of World Affairs*, 23.1 (2016), 9–24.
[896] Zeynep Tufekci, 'How Social Media Took Us from Tahrir Square to Donald Trump', *MIT Technology Review*, 14.18 (2018), 1–12;
Peter Pomerantsev, 'To Unreality—and Beyond', *Journal of Design and Science*, 6.1 (2019) <https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html>.

that have been shown to have a detrimental effect on public discourse and democracy[897]. A sobering example of these effects was the shocking attack on the US Capitol by its own citizens. On the eve of the 2020 US presidential election, the hashtag #StoptheSteal emerged on Twitter and, along with videos regarding voter fraud now proven to have been misleading, soon went viral[898]. The hashtag quickly started trending on Facebook as well, culminating in the armed attack on the US Capitol on 6 January 2021[899]. Arguably, it was not the online sharing of alleged voter fraud alone that resulted in these acts of domestic terrorism, but rather, the years of exposure to non-critical, imbalanced public discourse within the online echo chambers and filter bubbles that arise from content personalisation[900]. As such, social media regulation in the US sits within a dynamic confluence of human rights and cyber law, continuously attempting to harmonise First Amendment freedoms[901], the threats posed by rapid technological advancement[902], and national security concerns[903].

The US, in line with its historical emphasis on individual freedoms and liberties, has a rich tapestry of human rights laws and principles woven into its federal and state legal systems[904]. The US Declaration of Independence of 1776 is widely acknowledged as the first civic document, globally, to meet contemporary definitions of human rights[905]. Subsequently drafted in 1787 to establish the structure of a democratic government, the US Constitution, although not expressly delineated as a human rights charter at the time, encapsulates principles that align with modern human rights ideals: forbidding bills of attainder or ex post facto laws[906] embodying the right to effective legal remedy[907]; mandating jury trials in federal criminal cases[908], resonating with the right to a fair hearing [909]; and instituting a 'Privileges and

[897] Jeff Orlowski, *The Social Dilemma* (United States: Netflix, 2020) <netflix.com/title/81254224>.
[898] Marianna Spring, '"Stop the Steal": The Deep Roots of Trump's "voter Fraud" Strategy', *BBC News* (London, 23 November 2020) <https://www.bbc.com/news/blogs-trending-55009950> [accessed 25 July 2023].
[899] Kirsten Martin, 'Recommending an Insurrection: Facebook and Recommendation Algorithms', in *Ethics of Data and Analytics: Concepts and Cases*, ed. by Kirsten Martin (Oxon: CRC Press, 2022), pp. 225–39.
[900] Jay W. Jackson and Verlin B. Hinsz, 'Group Dynamics and the U.S. Capitol Insurrection: An Introduction to the Special Issue', *Group Dynamics*, 26.3 (2022), 169–77 <https://doi.org/10.1037/gdn0000193>.
[901] Conrad Wilton, 'Sony, Cyber Security, and Free Speech: Preserving the First Amendment in the Modern World', *Pace Intellectual Property, Sports & Entertainment Law Forum*, 7.1 (2017), 1–43 <https://heinonline.org/HOL/License>.
[902] Asih Handayanti, 'The Role of Cyber Law in The Use of Technology in Mass Media', *Legal Brief*, 11.5 (2022), 2722–4643 <https://doi.org/10.35335/legal>.
[903] Robert Chesney and Danielle Keats Citron, '21st Century-Style Truth Decay: Deep Fakes and the Challenge for Privacy, Free Expression, and National Security', *Maryland Law Review*, 78.4 (2019), 882–91 <https://www.washingtontimes.com/news/2019/jan/29/dan-coats-gina->.
[904] David Sloss, 'How International Human Rights Transformed the U.S. Constitution', *Human Rights Quarterly*, 38.2 (2016), 426–49 <http://digitalcommons.law.scu.edu/facpubs>.
[905] Carol Devine, Carol R. Hansen, and Ralph Wilde, *Human Rights: The Essential Reference* (New York: Bloomsbury Academic, 1999).
[906] Article I, Section 9 of the *Constitution of the United States* (1787).
[907] Article 8 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948.*
[908] Article III, Section 2 of the *Constitution of the United States* (1787).
[909] Article 10 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948.*

Immunities' clause promoting cross-state equality[910], presaging the contemporary right to equal protection under law [911]. On 15 December 1791 Congress ratified the Bill of Rights, containing the first 10 Amendments to the US constitution, adding substantive human rights to the existing procedural rights[912]. The Bill of Rights established, among others, key human rights such as freedom of speech, religion, and the press, as well as the right to a fair trial and due process[913]. Of these foundational instruments, the First Amendment of the US Constitution is often invoked in debates regarding social media regulation[914].

One and a half centuries later, like the UK, the US was a key stakeholder in the drafting and adoption of the UDHR in 1948. However, it is worth noting that unlike the UK's unconditional ratification of several subsequent human rights treaties, the US ratified certain treaties with a number of reservations, understandings, and declarations (RUDs), including that of the ICCPR[915]. Specifically, the US has ratified the ICCPR under the RUDs listed in Table 1. Of particular concern for this mini-thesis is the reservation to the effect that the US does not accept any obligation to guarantee the right to participate in the conduct of public affairs under Article 25(b) of the ICCPR. In the most recent UPR of the US, the Special Rapporteur on Extreme Poverty noted covert disenfranchisement, concluding that certain groups were being systematically deprived of their right to participate in public affairs[916]. As per UPR protocol, UN member states have the opportunity to offer commentary and recommendations to the human rights issues identified by the UNHRC. Regarding the findings of the Special Rapporteur on Extreme Poverty, Germany recommended the US "Ensure the exercise of the right to vote, including by demanding that states refrain from using voter identification requirements that can have a discriminatory impact on voters[917]", while Greece recommended the US "Ensure the right to vote without discrimination by increasing access to every method of voting allowed in each state or jurisdiction[918]". Subsequently, in its views on conclusions

[910] Article IV, Section 2 of the *Constitution of the United States* (1787).
[911] Article 7 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948*.
[912] Michael J Douma, 'How the First Ten Amendments Became the Bill of Rights', *The Georgetown Journal of Law & Public Policy*, 15 (2017), 593–614.
[913] Amendment I of the *Bill of Rights* (United States, 1791).
[914] Jack M Balkin, 'How to Regulate (and Not Regulate) Social Media', *Journal of Free Speech Law*, 1.1 (2021), 71–96.
[915] Eric Chung, 'The Judicial Enforceability and Legal Effects of Treaty Reservations, Understandings, and Declarations', *The Yale Law Journal*, 126 (2016), 170–241.
[916] Para. 37 of the Working Group on the Universal Periodic Review, 'Report of the Office of the United Nations High Commissioner for
Human Rights: Compilation on the United States of America', *A/HRC/WG.6/36/USA/2, Adopted on 11 March 2020*.
[917] Recommendation 26.275 of the 'Report of the Working Group on the Universal Periodic Review: United States of America', *A/HRC/46/15, Adopted on 15 December 2020* <http://webtv.un.org/search/.>.
[918] Recommendation 26.276 of the 'Report of the Working Group on the Universal Periodic Review: United States of America', *A/HRC/46/15, Adopted on 15 December 2020* <http://webtv.un.org/search/.>.

and/or recommendations, voluntary commitments and replies, the US stated that it supports the recommendations from Germany and Greece only in part[919], as some recommendations require the achievement of an ideal rather than a specific goal [920], and also assert that such a partial support for recommendations does not imply acceptance of a legal requirement [921]. Furthermore, at a regional level, should the US seek to ratify the ACHR in future, its reservations regarding Article 25(b) of the ICCPR are also in conflict with Article 23 of the ACHR[922], and would present a significant obstacle. This reserved approach, particularly towards international obligations concerning participation in public affairs, not only highlights the unique challenges in transposing international human rights norms to domestic laws but also offers a contextual framing of the interplay between these domestic norms and regional legal frameworks that shape social media regulation in the US.

Table 1: US RUDs to provisions of the ICCPR

ICCPR Article	Provision	RUD
Article 6(5)	Sentence of death shall not be imposed for crimes committed by persons below eighteen years of age and shall not be carried out on pregnant women.	Reservation to the effect that the United States retains the right to execute people under the age of 18.
Article 5(1)	Nothing in the present Covenant may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms recognised herein or at their limitation to a greater extent than is provided for in the present Covenant.	Reservation to nullify certain provisions in the ICCPR.
Article 14(1)	All persons shall be equal before the courts and tribunals. In the determination of any criminal charge against him, or of his rights and obligations in a suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law.	Reservation to the effect that the United States does not accept any obligation under the ICCPR to grant individuals access to the court.

[919] Para. 7 of the 'Report of the Working Group on the Universal Periodic Review: United States of America', *A/HRC/46/15/Add.1, Adopted on 4 March 2021*.
[920] Para. 2 of the 'Report of the Working Group on the Universal Periodic Review: United States of America', *A/HRC/46/15/Add.1, Adopted on 4 March 2021*.
[921] Para. 3 of the 'Report of the Working Group on the Universal Periodic Review: United States of America', *A/HRC/46/15/Add.1, Adopted on 4 March 2021*.
[922] Article 23 of the 'American Convention on Human Rights'.

Article 19(2)	Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice	Reservation to the effect that the United States does not accept any obligation under the ICCPR to restrict speech.
Article 21	The right of peaceful assembly shall be recognised. No restrictions may be placed on the exercise of this right other than those imposed in conformity with the law.	Reservation to the effect that the United States does not accept any obligation under the ICCPR to restrict the right to peaceful assembly.
Article 22(1)	Everyone shall have the right to freedom of association with others, including the right to form and join trade unions for the protection of his interests.	Reservation to the effect that the United States does not accept any obligation under the ICCPR to restrict the right to freedom of association.
Article 25(b)	To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors;	Reservation to the effect that the United States does not accept any obligation under the ICCPR to guarantee the right to vote.
Article 26	All persons are equal before the law and are entitled without any discrimination to the equal protection of the law.	Reservation to the effect that the United States does not accept any obligation under the ICCPR to guarantee the right to equal protection of the law.

Source: Hill (2015)[923]

A decade prior to the conditional ratification of the ICCPR, however, the US enacted the Civil Rights Act in 1964 at federal level. This Act represented a milestone in the fight against discrimination, prohibiting unequal application of voter registration requirements and racial segregation in schools, employment, and public accommodations.[924] Its legacy can be seen in the ongoing debates about voting rights and access, particularly in the context of digital participation and the role of social media platforms in political discourse[925]. At the state level, human rights law varies significantly, with different states introducing legislation to address particular issues pertinent to their jurisdictions. For example, addressing growing concerns

[923] Daniel W Hill, 'Avoiding Obligation: Reservations to Human Rights Treaties', *Journal of Conflict Resolution*, 60.6 (2016), 1129–58.
[924] Juliet R Aiken, Elizabeth D Salmon, and Paul J Hanges, 'The Origins and Legacy of the Civil Rights Act of 1964', *Journal of Business and Psychology*, 28.4 (2013), 383–99 <https://doi.org/10.1007/s>.
[925] Fredrick C. Harris, 'The Next Civil Rights Movement?', *Dissent*, 62.3 (2015), 34–40.

about data protection and personal privacy in the digital age, the state of California created the California Consumer Privacy Act in 2018, reflecting a European-style privacy regime[926].

Regarding cyber law, the US has been a signatory to the Budapest Convention since its inception in 2001[927]. In doing so the US has committed to criminalising offences such as illegal access to computer systems[928], data interception[929], system interference[930], and cyber fraud[931]. Indeed, the Computer Fraud and Abuse Act (CFAA) of 1986, initially lacking specific provisions against many cyber offences[932], was later aligned with Article 2 of the Budapest Convention's goals through key amendments[933]. These amendments included, among others, the USA PATRIOT Act of 2001 broadening the CFAA's scope to include protected computers involved in interstate or foreign communication[934], and the Identity Theft Enforcement and Restitution Act of 2008 removing the financial damage threshold for cybercrimes, reinforcing its deterrent effect[935]. The USA PATRIOT Act and amendments to existing laws it affected, however, have been heavily critiqued for its impact on privacy rights[936]; a problem which is compounded by the fact that, as a signatory to the Budapest Conventions, the US actively collaborates with other signatory nations on cross-border cybercrime investigations, shares critical intelligence, and extradites cybercriminals[937].

In 2004, the US endorsed the Comprehensive Inter-American Cybersecurity Strategy, signalling its commitment to collaboration on matters of cybersecurity in the American region[938]. The Strategy's call for strengthening legal frameworks to ensure regional cybersecurity arguably contributed to the US adopting several key legislative pieces, such as

[926] Stuart L Pardau, 'The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States?', *Journal of Technology Law & Policy*, 23.1 (2018), 68–114.
[927] Council of Europe, 'Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY', *Parties to the Budapest Convention*, 2023 <https://www.coe.int/en/web/cybercrime/parties-observers> [accessed 19 June 2023].
[928] Article 2 of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[929] Article 3 of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[930] Article 5 of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[931] Article 8 of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[932] Dodd S Griffith, 'The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem', *Vanderbilt Law Review*, 43.2 (1990), 453–90.
[933] Catalina Goanta and Apostolis Zarras, *Ransomware: Notes on the US Computer Fraud and Abuse Act and the CoE International Convention on Cybercrime* (Stanford - Vienna, 2021) <http://ttlf.stanford.edu>.
[934] Section 217(1) of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act* (United States, 2001).
[935] Section 204(a) of the *Identity Theft Enforcement and Restitution Act* (United States, 2008).
[936] Kellie Delaney, 'The USA PATRIOT Act and Privacy: A New Frontier of Mass Surveillance', *GPSolo*, 37.5 (2020), 34–37.
[937] Article 14 of the 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*.
[938] K.P. Newmeyer, 'Elements of National Cybersecurity Strategy for Developing Nations', *National Cybersecurity Institute Journal*, 1.3 (2015), 9–19.

the Cybersecurity Enhancement Act of 2014[939]. Furthermore, the OAS Inter-American Portal on Cybercrime[940] and related working group[941] has been providing a platform for information exchange on cybercrime legislation since 2011, allowing the US to stay abreast with evolving regional norms and standards[942]. For example, discussions within the working group influenced the drafting of the Cybersecurity Information Sharing Act of 2015[943], which promotes the sharing cybersecurity threat information between the government and the private sector[944]. The influence of REMJA and its emphasis on international cooperation[945] is also apparent in this Act[946]. Similarly, the influence of CICTE's anti-cyberterrorism strategies is evident from certain procedural provisions in non-cyber law instruments such as the USA PATRIOT Act[947]. However, unlike the EU's NIS 2 Directive that came into effect in January of 2023[948], the US has not adopted a comparable nationwide network and information security framework, with cybersecurity largely managed through sector-specific regulations[949]. Additionally, unlike the GDPR, the US has not adopted a comprehensive federal law on data protection[950], instead preferring a sectoral approach that entails a patchwork of federal and state laws, such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996[951] and the Children's Online Privacy Protection Act (COPPA) of 1998[952], complemented by a variety of regulatory guidelines and self-regulatory regimes[953].

[939] Terry Benzel, 'A Strategic Plan for Cybersecurity Research and Development', *IEEE Security & Privacy*, 13.4 (2015), 3–5 <http://ec.europa.eu>.
[940] Inter-American Portal on Cybercrime, 'Home Portal', 2023 <http://www.oas.org/en/sla/dlc/cyber-en/homePortal.asp> [accessed 18 June 2023].
[941] Inter-American Portal on Cybercrime, 'Working Group', 2023 <http://www.oas.org/en/sla/dlc/cyber-en/grupo-trabajo.asp> [accessed 18 June 2023].
[942] Matheus M Hoscheidt and Elisa Felber Eichner, 'Legal and Political Measures to Address Cybercrime', *World Summit on the Information Society Forum*, 2 (2014), 445–77.
[943] A. Pala and J. Zhuang, ' Information Sharing in Cybersecurity: A Review', *Decision Analysis*, 16.3 (2019), 172–96.
[944] Section 10(a) of the *Cybersecurity Information Sharing Act* (United States of America, 2015).
[945] Part II of the 'Conclusions and Recommendations to REMJA XI', *REMJA-IX/DOC.2/21 Rev. 1, Held Virtually on 19 May 2021*.
[946] Section 109(b)(1) of the *Cybersecurity Information Sharing Act* (United States of America, 2015).
[947] Title II of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act* (United States, 2001).
[948] Council of Europe, 'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for the High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and the Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)', *Official Journal of the European Union*, I. 333/80 (2022).
[949] A. Manniez, 'Cyberdefense and Cybersecurity Regulations in the United States: From the Failure of the "Comprehensive Policy" to the Success of the Sectoral Approach', *Conflicts, Crimes and Regulations in Cyberspace*, 2 (2021), 177–97.
[950] Shawn Marie Boyne, 'Data Protection in the United States', *American Journal of Comparative Law*, 66 (2018), 299–343 <https://doi.org/10.1093/ajcl/avy016>.
[951] Wilnellys Moore and Sarah Frye, 'Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules', *Journal of Nuclear Medicine Technology*, 47.4 (2019), 269–72 <https://doi.org/10.2967/JNMT.119.227819>.
[952] Stacey B Steinberg, 'Sharenting: Children's Privacy in the Age of Social Media', *Emory Law Journal*, 66.4 (2017), 839.
[953] R. Medzini, 'Enhanced Self-Regulation: The Case of Facebook's Content Governance', *New Media & Society*, 24.10 (2022), 2227–51.

With regard to social media regulation, there are important regulatory changes presently under discussion aimed at safeguarding consumers from potential exploitation by private companies[954]. Dominant themes within this discourse include the problematic nature of the attention economy, which capitalises on- and potentially misuses extensive quantities of user behavioural, purchasing, and demographic data[955], and escalating concerns about the wider societal impact of social media[956]. This has culminated in numerous legislative proposals, such as the Social Media Nudging Users to Drive Good Experiences on Social Media (NUDGE) Bill, the Protecting Americans from Dangerous Algorithms Bill, and the Biased Algorithm Deterrence Bill. The Social Media NUDGE Bill, introduced to the US Senate by Senator Amy Klobuchar on 2 September 2022, seeks to address primarily issues of social media addiction[957], and the dissemination of harmful content[958]. While protecting consumers of social media *and* respecting constitutional freedoms[959] presents a challenge for US legislators, the Social Media NUDGE Bill serves as an exemplar of domestic cyber law harmonising with international human rights norms. Its focus on user control over their own data[960] aligns with Article 17 of the ICCPR[961], and possibly with Article 11 of the ACHR[962], if the US opts for ratification. Yet, the convergence of cyber law and human rights reform presents a paradox. As highlighted by the preceding discussion on stochastic terrorism[963], the state's pursuit of its negative obligation not to interfere with freedom of thought, conscience, and religion[964] for one group may inadvertently create cyberspace conditions that obstruct its positive obligation to ensure another group's right to liberty and security[965].

954 Philip M. Napoli, 'Back from the Dead (Again): The Specter of the Fairness Doctrine and Its Lesson for Social Media Regulation', *Policy and Internet*, 13.2 (2021), 300–314 <https://doi.org/10.1002/poi3.253>.
955 Vikram R. Bhargava and Manuel Velasquez, 'Ethics of the Attention Economy: The Problem of Social Media Addiction', *Business Ethics Quarterly*, 31.3 (2021), 321–59 <https://doi.org/10.1017/beq.2020.32>.
956 S. Mo Jones-Jang and Myojung Chung, 'Can We Blame Social Media for Polarization? Counter-Evidence against Filter Bubble Claims during the COVID-19 Pandemic', *New Media and Society*, 00.0 (2022), 1–20 <https://doi.org/10.1177/14614448221099591>.
957 Section 2(1) of the *Nudging Users to Drive Good Experiences on Social Media (NUDGE) Act* (United States, 2022) <https://www.congress.gov/bill/117th-congress/senate-bill/3608/text?r=4&s=1> [accessed 31 July 2023].
958 Section 2(2) of the *Nudging Users to Drive Good Experiences on Social Media (NUDGE) Act* (United States, 2022) <https://www.congress.gov/bill/117th-congress/senate-bill/3608/text?r=4&s=1> [accessed 31 July 2023].
959 Amendment I of the *Bill of Rights* (United States, 1791).
960 Section 4(b)(1) of the *Nudging Users to Drive Good Experiences on Social Media (NUDGE) Act* (United States, 2022) <https://www.congress.gov/bill/117th-congress/senate-bill/3608/text?r=4&s=1> [accessed 31 July 2023].
961 Article 17, UN General Assembly, 'International Covenant on Civil and Political Rights', *2200A(XXI), Adopted 23 March 1976.*
962 Article 11 of the 'American Convention on Human Rights'.
963 Christopher Wiggins, 'Attacks on the LGBTQ+ Community Amount to Stochastic Terrorism', *Advocate*, 16 August 2022 <https://www.advocate.com/politics/2022/8/16/attacks-lgbtq-community-amount-stochastic-terrorism>.
964 Article 18(1) of the 'International Covenant on Civil and Political Rights'.
965 Article 9(1) of the 'International Covenant on Civil and Political Rights'.

In contrast, the proposal for the Protecting Americans from Dangerous Algorithms Act, focuses less on content and more on the mechanisms that produce, organise and disseminate social media content[966]. Specifically, the Bill seeks to hold large social media companies accountable for their algorithmic systems that amplify or promote content that leads to real-world violence. The Bill aims to do so by amending Section 230 of the Communications Decency Act, which largely exempts online platforms from liability for content posted by their users[967]. Proposing a similar amendment to Section 230 of the Communications Decency Act, the Biased Algorithm Deterrence Bill seeks to impose criminal penalties on online platforms that deploy biased algorithms for processing user-generated content[968]. Here, a greater emphasis is placed on the owners of algorithms and their responsibility for its impact on society – intended or otherwise[969]. While holding companies accountable for the wider social impact of their algorithms could promote transparency and fairness in content dissemination, this approach raises concerns about compatibility with Article 19 of the ICCPR on the freedom of expression, depending on how "biased algorithms" are defined once the Act is adopted[970]. These proposed regulatory changes echo the UK's "duty of care" found in the recently revised Online Safety Bill[971], and calls for heightened transparency and accountability on the part of social media corporations while essentially leaving individual liberties intact. However, organisations such as the Regulatory Transparency Project warn that an apparent "avalanche of algorithmic fairness regulations" in the US risks a decrease in the computational capabilities of the US economy, a weakening of the US's ability to compete globally for AI technology, and the forfeiture of the country's lead in technological innovation[972].

The aforementioned discussion illustrates, that the evolution of social media regulation in the US is uniquely contextualised by the country's intertwined commitments to cyber law, human rights, and domestic constitutional norms. The breadth and complexity of these commitments are evident from the variety of responses to the societal challenges posed by social media,

[966] T. A. Lipinski and K.A. Henderson, 'Fake Science: Legal Implications in the Creation and Use of Fake Scientific Data Published as Grey Literature and Disseminated through Social Media', *The Grey Journal*, 17.3 (2021).
[967] Section 2 of the *Protecting Americans from Dangerous Algorithms Act* (United States, 2021) <https://www.congress.gov/bill/117th-congress/house-bill/2154/text> [accessed 31 July 2023].
[968] Christopher Bates, *A Review of Proposals to Reform Section 230* (Washington DC, May 2021).
[969] Peter J Pizzi, 'Social Media Immunity in 2021 and Beyond: Will Platforms Continue to Avoid Litigation Exposure Faced by Off Line Counterparts', *Defense Counsel Journal*, 88.3 (2021), 1–13 <https://www.>.
[970] Article 19, UN General Assembly, 'International Covenant on Civil and Political Rights', *2200A(XXI), Adopted 23 March 1976*.
[971] House of Lords, 'Online Safety Bill', *Parliamentary Bills*, 2023 <https://bills.parliament.uk/bills/3137>.
[972] Neil Chilson and Adam Thierer, *The Coming Onslaught of 'Algorithmic Fairness' Regulations, AIES 2018 - Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society* (Association for Computing Machinery, Inc, 2 November 2022) <https://doi.org/10.1145/3278721.3278731>.

particularly those related to the proliferation of disinformation, and increasing political polarisation. Interestingly, the so-called "coming onslaught of 'algorithmic fairness' regulations"[973] in the US betrays its nuanced understanding of free speech and its historical wariness of international obligations, alongside an enduring sectoral approach to cyber law. The country's historical, cultural and social foundations in individual liberties do, however, appear to be contending with emerging concerns regarding the potential for harm and negative societal impact of unchecked online discourse. Notably, the manner in which the US appears to be navigating these challenges and tensions carries broader implications not only for its domestic landscape but also for regional and international discourse on the governance of cyberspace.

5.4. International and regional harmonisation of social media regulation in South Africa

In 1948, as the UK and US were instrumental in formulating and adopting the UDHR South Africa, then a constituent country of the British Empire and a founding member of the UN[974], paradoxically instituted Apartheid, a regime infamous for its systemic violation of human rights. This period of extreme racial segregation and discrimination dominated the country's legal and social framework[975], explicitly contradicting the principles of equality, human dignity[976], and non-discrimination[977] encapsulated in the UDHR. Although not formally expelled from the UN, in 1974, the UN General Assembly suspended South Africa's participation due to its Apartheid public policies[978]. It was only after the end of Apartheid in 1994, with the election of Nelson Mandela as President, that South Africa fully regained its participation rights in the UN[979]. Similar to the UK and US, South Africa is also a signatory to various international and regional human rights instruments, the commitments to which are reflected in the country's contemporary domestic legal frameworks[980]. At the time of its adoption by the UN in 1948, South Africa abstained from voting on the UDHR[981], but since

[973] Chilson and Thierer.
[974] Eric Engle, 'Universal Human Rights: A Generational History', *Annual Survey of International & Comparative Law*, 12 (2006), 219–61.
[975] J. Allen, *Apartheid South Africa: An Insider's Overview of the Origin and Effects of Separate Development* (Lincoln: iUniverse Books, 2005).
[976] Article 1 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948.*
[977] Article 7 of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948.*
[978] Abbott A, 'The General Assembly, 29th Session: The Decredentialization of South Africa', *Harvard International Law Journal*, 16.3 (1975), 576–88 <https://heinonline.org/HOL/License>.
[979] Anthony Mango and Edmund Jan Osmanczyk, *Encyclopedia of the United Nations and International Agreements* (London: Routledge, 2002).
[980] Mawere J, 'The Legality of Expropriating Land without Compensation in South Africa: A Regional and International Law Perspective', *African Journal of Development Studies*, 1 (2021), 243–64 <https://doi.org/10.31920/2634-3649/2021/sin1a13>.
[981] Politico. *United Nations adopts Universal Declaration of Human Rights, Dec. 10, 1948. Available at: https://www.politico.com/story/2015/12/united-nations-adopts-universal-declaration-of-human-rights-dec-10-1948-216489*

the fall of Apartheid the country has ratified cornerstone international human rights treaties such as the ICCPR in 1998[982] and the ICESCR in 2015[983]. At the regional level, South Africa became a state party to the African Charter on Human and Peoples' Rights (ACHPR) in 1994 - the same year as the birth of its new democracy[984]. South Africa also ratified the Protocol on the Statute of the African Court of Justice and Human Rights replacing earlier protocols[985], and thus recognises the regional jurisdiction of the African Court of Justice and Human Rights (ACtJHR)[986].

Domestically, while efforts persist to systematically dismantle the enduring legacy of Apartheid[987], the construction of a new post-Apartheid South Africa has been laid on the cornerstone of a transformative constitution enacted in 1996[988]. The Constitution of the Republic of South Africa is globally recognised as one of the most progressive constitutions, affirming the democratic values of human dignity, equality, and freedom[989]. The Bill of Rights, contained in Chapter 2 of the Constitution, entrenches a broad range of socio-economic and political rights, including the right to privacy[990], freedom of religion, belief and opinion[991], freedom of expression[992], and freedom and security of the person[993]. Given the country's chequered past regarding human rights, comprehensive legal and policy frameworks have since been implemented to effectively operationalise the provisions of its Constitution. One notable mechanism is the South African Human Rights Commission (SAHRC), which was established by the South African Constitution to support democratic governance and promote respect for human rights[994]. The SAHRC is empowered to monitor, both proactively and by way of

(Accessed on 3 May 2022).

[982] United Nations, 'Parties to the International Covenant on Civil and Political Rights', *Available at: Https://Treaties.Un.Org/Pages/ViewDetails.Aspx?Src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en (Accessed on 11 June 2022)*.

[983] United Nations, 'Parties to the International Covenant on Economic, Social and Cultural Rights', *Available at: Https://Treaties.Un.Org/Pages/ViewDetails.Aspx?Src=IND&mtdsg_no=IV-3&chapter=4 (Accessed on 11 June 2022)*.

[984] African Commission on Human Rights, 'State Parties to the African Charter', *Available at: Https://Www.Achpr.Org/Statepartiestotheafricancharter (Accessed on 15 October 2022)*.

[985] Chapter 1 of the 'Protocol on the Statute of the African Court of Justice and Human Rights', *Adopted on 1 July 2008 in Sharm El-Sheikh*, 2004.

[986] F.A. Agwu, 'The African Court of Justice and Human Rights: The Future of International Criminal Justice in Africa', *Africa Review*, 6.1 (2014), 30–43.

[987] J A Dreyer, S Viviers, and N Mans-Kemp, 'Reflecting on Compliance with Broad-Based Black Economic Empowerment Codes of Good Practice: Trends and Suggestions', *South African Journal of Business Management*, 52.1 (2021), 1963 <https://doi.org/10.4102/sajbm>.

[988] South African Parliament, *Constitution of the Republic of South Africa* (South Africa, 1996).

[989] S.M. Weeks, 'South African Legal Culture and Its Dis/Empowerment Paradox', in *The Oxford Handbook of Law and Anthropology*, ed. by Marie-Claire Foblets (Oxford: Oxford University Press, 2022), pp. 56–72.

[990] Section 14 of the *Constitution of the Republic of South Africa* (South Africa, 1996).

[991] Section 15 of the *Constitution of the Republic of South Africa* (South Africa, 1996).

[992] Section 16 of the *Constitution of the Republic of South Africa* (South Africa, 1996).

[993] Section 12 of the *Constitution of the Republic of South Africa* (South Africa, 1996).

[994] Tseliso Thipanyane, 'Strengthening Constitutional Democracy: Progress and Challenges of the South African Human Rights Commission and Public Protector', *New York Law School Law Review*, 22.60 (2019), 125–51.

complaints brought before it, all aspects of human rights in the country. It carries out research, provides reports on human rights issues, and can carry out litigation in the interest of human rights.[995] Furthermore, South Africa has established various tribunals such as the Labour Court[996], Labour Appeal Court[997], and the Land Claims Court[998], which play pivotal roles in adjudicating specialised and complex claims of human rights violations.

Beyond the SAHRC and specialised courts, South Africa's commitment to protecting the rights of its individuals within its jurisdiction is evident in domestic legal instruments that span the entire human life cycle. For example, the Children's Act of 2005 provides comprehensive provisions that safeguard the rights of children, encompassing aspects such as child protection[999], parental responsibilities and rights[1000], children's court[1001], child abduction[1002], and adoption procedures[1003]. As one transitions into adulthood other human rights, such as the right to work[1004], continue to be defended with legislation such as the Employment Equity Act (EEA) of 1998. The EEA actively promotes equal opportunity in the workplace[1005], effectively prohibiting unfair discrimination and ensuring equitable representation across all occupational categories and levels[1006]. Here, it is also worth noting that South Africa's Children's Act is in line with the duties imposed on state parties by the African Charter on the Rights and Welfare of the Child[1007]. Similarly, the EEA is in line with the duties imposed on state parties by the provisions of the ACHPR related to the right to work[1008]. In a more general sense, the provisions contained in the Promotion of Equality and Prevention of Unfair Discrimination Act (PEPUDA) of 2000 protect those within the jurisdiction of South Africa from unfair discrimination by both the government and private individuals and organisations[1009]. The PEPUDA also bestows upon every High Court in the country the mandate and powers of an

[995] R. Adams and F. Adeleke, 'Protecting Information Rights in South Africa: The Strategic Oversight Roles of the South African Human Rights Commission and the Information Regulator', *International Data Privacy Law*, 10.2 (2020), 146–59.
[996] B. Van Zyl, 'Jurisdiction of the Labour Court in South Africa', *HR Future*, 8.1 (2020), 44–45.
[997] V. Naidoo, T. Rasetlola, and A. Michalow, 'Arbitrary Is Still Not Equal to Discrimination as Confirmed by the Labour Appeal Court', *Without Prejudice*, 20.11 (2020), 17–18.
[998] G. N. Barrie, 'Land Claims by Indigenous Peoples–Litigation versus Settlement? Observations on the Richtersveld Litigation Route Followed in South Africa versus the Noongar Settlement Route Followed in Western Australia', *Journal of South African Law*, 2 (2018), 344–66.
[999] Chapter 7 Part 2 of the *Children's Act* (Republic of South Africa, 2005).
[1000] Chapter 3 of the *Children's Act* (Republic of South Africa, 2005).
[1001] Chapter 4 Part 2 of the *Children's Act* (Republic of South Africa, 2005).
[1002] Chapter 17 Part 2 of the *Children's Act* (Republic of South Africa, 2005).
[1003] Chapter 15 Part 2 of the *Children's Act* (Republic of South Africa, 2005).
[1004] Article 23(1) of the 'Universal declaration of human rights', *217 A (III), adopted 10 December 1948*.
[1005] Para. 5 of the *Employment Equity Act* (Republic of South Africa, 1998).
[1006] Para. 20(2)(c) of the *Employment Equity Act* (Republic of South Africa, 1998).
[1007] Article 1 of the 'African Charter on the Rights and Welfare of the Child', *CAB/LEG/24.9/49, Adopted on 11 July 1990*.
[1008] Article 15 of the 'African Charter on Human and Peoples' Rights', *CAB/LEG/67/3, Adopted on 27 June 1982 in Banjul*, 1982 <https://doi.org/10.9783/9780812205381.713>.
[1009] Article 5(1) *Promotion of Equality and Prevention of Unfair Discrimination Act* (Republic of South Africa, 2000).

Equality Court, in the area of its jurisdiction, as a mechanism of enforcement of the provisions of the Act[1010].

The Protection of Personal Information (POPI) Act of 2013, is another significant piece of human rights legislation. The adoption of this domestic instrument in South Africa highlights the urgent need to consider human rights protections in the context of cyberspace. Given the vast amounts of personal data that are created and exchanged, simply in order to navigate everyday life, privacy has become a highly complex human right to protect[1011]. This Act seeks to give effect to the constitutional right to privacy, by introducing measures to ensure that the processing of personal information is conducted in a manner that respects privacy[1012]. Influencing essentially all facets of life, including business, education, and public service, the POPI Act has significantly transformed how personal data is used in South Africa, reinforcing privacy rights and bringing about a substantial change in everyday data practices[1013]. Prior to the adoption of the POPI Act, arguably the first definitive step towards creating a domestic cyber law framework, was the adoption of the Electronic Communications and Transactions Act (ECTA) of 2002[1014]. This Act laid the foundation for the legal recognition of electronic transactions and signatures, and established principles for consumer protection within the realm of e-commerce[1015]. The Act not only facilitated digital trade but also provided for the accreditation of authentication service providers, a critical move in ensuring the integrity and reliability of electronic transactions[1016]. The ECTA also contains both substantive and procedural provisions for addressing cybercrimes such as hacking, unlawful interception of data, and fraud[1017]. More recently, the Cybercrimes Act of 2020 strengthened and expanded South Africa's legal framework for addressing cybercrimes[1018]. Coming into force in 2021, this

[1010] Article 116(1)(a) *Promotion of Equality and Prevention of Unfair Discrimination Act* (Republic of South Africa, 2000).
[1011] Radi P. Romansky and Irina S. Noninska, 'Challenges of the Digital Age for Privacy and Personal Data Protection', *Mathematical Biosciences and Engineering*, 17.5 (2020), 5288–5303 <https://doi.org/10.3934/mbe.2020286>.
[1012] Preamble to the *Protection of Personal Information Act* (Republic of South Africa, 2013).
[1013] Agbor T. Kandeh, Reinhardt A. Botha, and Lynn A. Futcher, 'Enforcement of the Protection of Personal Information (POPI) Act: Perspective of Data Management Professionals', *SA Journal of Information Management*, 20.1 (2018), 1–9 <https://doi.org/10.4102/sajim.v20i1.917>.
[1014] Sizwe Snail, 'Cyber Crime in South Africa–Hacking, Cracking, and Other Unlawful Online Activities', *Journal of Information, Law and Technology*, 1.1 (2009).
[1015] Juana Coetzee, 'The Electronic Communications and Transactions Act 25 of 2002: Facilitating Electronic Commerce', *Stellenbosch Law Review*, 15.3 (2004), 501–21 <www.itweb.co.za/sections/internet/2002/0207110700.asp>.
[1016] M.R. de Villers, *Consumer Protection under the Electronic Communications and Transactions Act 25 of 2002* (Johannesburg: University of Johannesburg, 2009).
[1017] Shumani L Gereda, 'The Electronic Communications and Transactions Act', in *Telecommunications Law in South Africa*, ed. by Lisa Thornton (Johannesburg: STE Publishers, 2006), pp. 262–94 <http://www.uncitral.org/en->.
[1018] Sizwe Snail ka Mtuze and Melody Musoni, 'An Overview of Cybercrime Law in South Africa', *International Cybersecurity Law Review*, 4.1 (2023), 299–323 <https://doi.org/10.1365/s43439-023-00089-8>.

Act criminalises a wide array of offences, including unlawful access[1019], interception[1020], and distribution of data[1021], as well as cyber forgery[1022], and extortion[1023]. It further places an obligation on electronic communications service providers and financial institutions to report cybersecurity incidents[1024]. A distinctive feature of the Cybercrimes Act, reflecting a commitment to global and regional efforts to counter cybercrime[1025], is its provisions for extra-territorial jurisdiction regarding cross-border cybercrimes[1026]. The enforcement of this jurisdiction and the associated extradition laws, however, has sparked much debate regarding factors such as the segmented nature of the internet, and incongruent domestic legal frameworks[1027]. Furthermore, as an observer to the EU's Budapest Convention[1028], and original endorsement of the AU's Malabo Convention[1029], South Africa has shown an inclination towards harmonising its cyber law with both international and regional standards[1030].

South Africa's digital terrain, much like its counterparts in the UK and US, has been the subject of increasing scrutiny and regulatory intervention[1031]. The societal implications and challenges arising from the widespread use of social media platforms have necessitated legislative intervention, particularly in light of international human rights obligations and the broader socio-political climate of the nation[1032]. Emerging from the foundation laid by the POPI Act is the pressing debate around safeguarding consumers from the undue influence of social media[1033]. Applying domestic human rights legislation, particularly privacy laws, is crucial in South Africa's unique context. Here, social media companies can exploit the legacy of

[1019] Section 2 of the *Cybercrimes Act* (Republic of South Afrcia, 2020).
[1020] Section 3 of the *Cybercrimes Act* (Republic of South Afrcia, 2020).
[1021] Section 22(2)(a) of the *Cybercrimes Act* (Republic of South Afrcia, 2020).
[1022] Section 9 of the *Cybercrimes Act* (Republic of South Afrcia, 2020).
[1023] Section 10 of the *Cybercrimes Act* (Republic of South Afrcia, 2020).
[1024] Section 54 of the *Cybercrimes Act* (Republic of South Afrcia, 2020).
[1025] Chapter 5 of the *Cybercrimes Act* (Republic of South Afrcia, 2020).
[1026] Section 24(2) of the *Cybercrimes Act* (Republic of South Afrcia, 2020).
[1027] P. Sekati, 'Assessing the Effectiveness of Extradition and the Enforcement of Extraterritorial Jurisdiction in Addressing Transnational Cybercrimes', *Comparative and International Law Journal of Southern Africa*, 55.1 (2022), 1–36.
[1028] Council of Europe, 'Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY'.
[1029] S.B. von Solms, 'A Maturity Model for Part of the African Union Convention on Cyber Security', in *Science and Information Conference (SAI)* (London: IEEE, 2015), pp. 1316–20.
[1030] Sizwe Snail ka Mtuze, 'The Convergence of Legislation on Cybercrime and Data Protection in South Africa: A Practical Approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013', *Obiter*, 43.3 (2022), 536–69 <https://doi.org/10.23962/10539/23573>.
[1031] Vincent Chenzi, 'Fake News, Social Media and Xenophobia in South Africa', *African Identities*, 19.4 (2021), 502–21 <https://doi.org/10.1080/14725843.2020.1804321>.
[1032] Rofhiwa Felicia Mukhudwana, 'The Rise of Peripheral Actors in Media Regulation in South Africa: An Entry of Social Media Mob(S)', *African Journalism Studies*, 42.4 (2021), 153–78 <https://doi.org/10.1080/23743670.2022.2032783>.
[1033] Gilad Katzav, 'Compartmentalised Data Protection in South Africa: The Right to Privacy in the Protection of Personal Information Act', *South African Law Journal*, 139.2 (2022), 432–70.

Apartheid[1034], capitalising on poor digital literacy[1035], to enhance value extraction from the Attention Economy[1036].

One notable development was the proposed amendment to the Film and Publications Act of 1996, which sought to regulate online content[1037]. This proposition, much like the UK's Online Harms White Paper and the US's NUDGE Bill, addresses the ever growing threat of harmful online content. More specifically, an amendment to the Act of 1996 was proposed to Parliament in 2015[1038] and on 1 March 2022 the Films and Publications Amendment Act of 2019 came into force[1039]. The Act's amendments take into account technological advancements, among others those associated with social media, and the subsequent increased risk of exposure to harmful content[1040]. This attempt at modernising existing legislation, however, has not been without critique. It has been suggested that the Films and Publications Act, as amended by Act 11 of 2019, is not a suitable mechanism for determining whether politically-themed content can be considered harmful. Furthermore, critics anticipate that the amendments to the Film and Publications Act might face constitutional challenges[1041] due to potential conflicts with the domestically[1042], regionally[1043], and internationally[1044] protected freedoms of thought, opinion, and expression. Most recently, in 2022, the SAHRC took a significant step towards regulating online activities by issuing a social media charter[1045]. This charter aims to address the growing concerns around harmful online content, hate speech, and the spread of misinformation on social media platforms. The charter outlines guidelines for responsible social media use and sets expectations for both users and platform providers.[1046]

[1034] Caroline Pade-Khene, 'Embedding Knowledge Transfer in Digital Citizen Engagement in South Africa: Developing Digital Literacy', *Reading & Writing*, 9.1 (2018), 1–9 <https://doi.org/10.4102/rw.v9i1.193>.
[1035] Lena Nyahodza and Richard Higgs, 'Towards Bridging the Digital Divide in Post-Apartheid South Africa: A Case of a Historically Disadvantaged University in Cape Town', *South African Journal of Libraries and Information Science*, 83.1 (2017), 39–48 <https://doi.org/10.7553/83-1-1645>.
[1036] Alex Beattie, 'The Manufacture of Disconnection' (Victoria of of University of Wellington, 2020).
[1037] Section 4.1 of the 'Statement on Cabinet Meeting of 12 August 2015', 2015 <https://www.gcis.gov.za/newsroom/media-releases/statement-cabinet-meeting-12-august-2015> [accessed 17 August 2023].
[1038] Ellipsis, 'The Film & Publication Board and Online Content Regulation', 2023 <https://www.ellipsis.co.za/the-film-publication-board-and-online-content-regulation/#:~:text=The Bill amends the Films,platforms (physical and online).> [accessed 17 August 2023].
[1039] Proclamation Notice 52, *Government Gazette* (Republic of South Africa, 2022).
[1040] Government Gazette, *Films and Publications Amendment Act* (Republic of South Africa, 2019).
[1041] J.P. Ongeso, 'South Africa: Films and Publications Amendment Act Comes into Operation', *Bowmans*, 2022 <https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/#:~:text=These amendments have been viewed,group characteristics%2C and that constitutes> [accessed 17 August 2023].
[1042] Section 15 and 16 of the *Constitution of the Republic of South Africa* (South Africa, 1996).
[1043] Article 9(2) of the 'African Charter on Human and Peoples' Rights', *CAB/LEG/67/3, Adopted on 27 June 1982 in Banjul*, 1982 <https://doi.org/10.9783/9780812205381.713>.
[1044] Article 18(1) and 19 of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979*.
[1045] Section A of the *Social Media Charter, adopted on 15 March 2023 by the SAHRC* (Republic of South Africa, 2023).
[1046] Section B of the *Social Media Charter, adopted on 15 March 2023 by the SAHRC* (Republic of South Africa, 2023).

South Africa, therefore, has taken active steps in developing the country's cyber law framework, with specialised laws such as ECTA and the Cybercrimes Act, human rights law that can be applied to activities in cyberspace such as the POPI Act, and modernising existing legislation to maintain relevance in a digital era, as seen in the Films and Publications Amendment Act. However, South Africa has yet to propose or pass legislation directly targeting the use of algorithms, akin to the US's Protecting Americans from Dangerous Algorithms Act[1047].

In the broader landscape of digital regulation, South Africa's membership to the AU introduces an additional level of complexity. The AU's Malabo Convention, bearing South Africa's endorsement, promotes a cohesive digital policy framework across African nations[1048]. While such unity holds promise, it also presents potential challenges to alignment with broader continental directives without compromising its unique needs for human rights protections in cyberspace[1049]. South Africa's distinct historical and socio-political context warrants the development of domestic frameworks that provide substantive and procedural standards to ensure socio-economic advancement in a digital age, while maintaining efforts to address enduring inequalities that threaten said prosperity in and out of cyberspace. As South Africa continues to build a more comprehensive domestic cyber law framework, it will invariably be anchored in the constitutional principles the nation has become known for. Yet, for all of South Africa's uniqueness, herein lies the common challenge faced by other nations such as the UK and the US as well, namely finding the elusive equilibrium between embracing technological evolution, upholding human rights, and ensuring societal protection in a rapidly evolving digital.

5.5. Analysis at domestic level

Comparing and contrasting domestic frameworks across the UK, US and South Africa reveal complex challenges to regulating social media in the context of human rights. Despite these three countries' diverse socio-political histories and current constitutional frameworks, the overarching challenge seems to be balancing cybersecurity threat prevention, user protection, democratic ideals, and respect for human rights in general. Discourse regarding proposed

[1047] Pienaar C, *AI Regulation in South Africa and the Global Regulatory Trends*, 1 July 2019.
[1048] Oladotun E. Awosusi, 'The Imperative of Cyber Diplomacy and Cybersecurity in Africa: A New Means to a "Borderless" Regional End?', *Journal of African Foreign Affairs*, 9.3 (2022), 57–81 <https://doi.org/10.31920/2056-5658/2022/v9n3a3>.
[1049] ALT Advisory, *The Malabo Roadmap: Approaches to Promote Data Protection and Data Governance in Africa* (Johannesburg, September 2022).

legislative intervention suggests a deep concern for tipping the balance too heavily in one direction at the expense of others.

The UK's domestic legal framework suggests a commitment to the protection of human rights, with the adoption of several international[1050] and regional[1051] human rights treaties. This commitment is also mirrored in endeavours to protect those within the UK's jurisdiction in cyberspace, as illustrated by the evolution of the Online Harms White Paper[1052] into a proposed draft Online Safety Bill[1053], and the subsequent revised Online Safety Bill[1054]. A central concept present in the emergence of new social media regulation in the UK, is a "duty of care" towards users placed on corporations that deal in user-generated content[1055]. While unique and focussed in addressing the complex ramifications of regulating social media, the Online Safety Bill[1056] content personalisation runs the risk of infringing on freedoms that it is bound to uphold[1057]. The UK's process of consultation in developing the current revised Online Safety Bill, highlights the importance of large-scale collaboration on matters of cyber law as an operationalisation of the "duty of care" proved elusive. Originally proposed conceptualisations such as "harms which may be legal but harmful[1058]" were criticised for its ambiguity[1059] and were subsequently replaced, in the revised Bill, by clear guidelines for determining if content can be considered harmful[1060]. Yet, despite major advancements in domestic legal frameworks to protect users, the UK's current landscape is still criticised for not sufficiently addressing the specific problem of algorithm transparency[1061] that underly the risk of social media content

[1050] United Nations, 'Parties to the International Covenant on Civil and Political Rights'.
[1051] Council of Europe Treaty Office, 'Chart of Signatures and Ratifications of Treaty 009' <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=009> [accessed 19 April 2023].
[1052] Woods.
[1053] Section 1(1) of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].
[1054] House of Lords, 'Online Safety Bill', *Parliamentary Bills*, 2023 <https://bills.parliament.uk/bills/3137>.
[1055] Damian Tambini, 'The Differentiated Duty of Care: A Response to the Online Harms White Paper', *Journal of Media Law*, 11.1 (2019), 28–40 <https://doi.org/10.1080/17577632.2019.1666488>.
[1056] Section 13(2) of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].
[1057] Section 13(2) of the 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023].
[1058] Para. 3.5 of the 'Online Harms White Paper (CP 57)', *HM Government*, 2019 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf> [accessed 20 July 2023].
[1059] Peter Pomerantsev, 'A Cycle of Censorship: The UK White Paper on Online Harms and the Dangers of Regulating Disinformation', *Transatlantic Working Group on Content Moderation Online and Freedom of Expression*, 2019 <www.annenbergpublicpolicycenter.org/twg>.
[1060] M. MacCarthy, *U.K. Government Purges Legal but Harmful Provisions from Its Revised Online Safety Bill* (Washington D.C., 2022).
[1061] U. Reviglio and C. Agosti, 'Thinking Outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media', *Social Media+ Society*, 6.2 (2020), 2056305120915613.

personalisation interfering with the right to participate in the conduct of public affairs "by universal and equal suffrage" and in a manner that guarantees "the free expression of the will of the electors"[1062].

In the US, reverence for the First Amendment is central to the discourse, often invoked as a basis for resistance, regarding the regulation of social media[1063]. Given the current political landscape, tainted by events such as the January 6th Capitol attack and acts of violence against minority groups[1064], the urgency to regulate social media practices that facilitate such acts of violence becomes increasingly pronounced. Additionally, personalising social media content has drawn scrutiny for potentially interfering with the right to participate in public affairs "by universal and equal suffrage"[1065], as such practices risk compromising "the free expression of the will of the electors"[1066] by perpetuating and reinforcing pre-existing biases and skewed perspectives[1067]. In contrast to the UK's focus on protection from harm[1068], emerging social media regulation in the US seems to address the aforementioned concerns with a focus on protection against exploitation[1069, 1070]. This approach, however, has also not been without criticisms as a so-called "avalanche of algorithmic fairness regulations" has been argued to pose a risk to civil liberties[1071] and the country's capacity for technological innovation[1072].

After the fall of Apartheid in 1994, South Africa's legal landscape has been characterised by a strong focus on correcting the injustices of the past and preventing the perpetuation of widespread social inequalities. This focus on social justice and correcting pervasive inequalities is visible in an alignment with regional human rights standards[1073], as well as

[1062] Article 25(b) of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979*.
[1063] Conrad Wilton, 'Sony, Cyber Security, and Free Speech: Preserving the First Amendment in the Modern World', *Pace Intellectual Property, Sports & Entertainment Law Forum*, 7.1 (2017), 1–43 <https://heinonline.org/HOL/License>.
[1064] Nancy Unger, 'That the Worst Shooting in US History Took Place in a Gay Bar Is Unsurprising', *History News Network*, 13 June 2016 <https://www.advocate.com/politics/2022/8/16/attacks-lgbtq-community-amount-stochastic-terrorism>.
[1065] Article 25(b) of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979*.
[1066] Article 25(b) of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979*.
[1067] Jay W. Jackson and Verlin B. Hinsz, 'Group Dynamics and the U.S. Capitol Insurrection: An Introduction to the Special Issue', *Group Dynamics*, 26.3 (2022), 169–77 <https://doi.org/10.1037/gdn0000193>.
[1068] Irfan Chaudhry and Anatoliy Gruzd, 'Expressing and Challenging Racist Discourse on Facebook: How Social Media Weaken the "Spiral of Silence" Theory', *Policy and Internet*, 9999.9999 (2019), 1–21 <https://doi.org/10.1002/poi3.197>.
[1069] Section 2(1) of the *Nudging Users to Drive Good Experiences on Social Media (NUDGE) Act* (United States, 2022) <https://www.congress.gov/bill/117th-congress/senate-bill/3608/text?r=4&s=1> [accessed 31 July 2023].
[1070] T. A. Lipinski and K.A. Henderson, 'Fake Science: Legal Implications in the Creation and Use of Fake Scientific Data Published as Grey Literature and Disseminated through Social Media', *The Grey Journal*, 17.3 (2021).
[1071] Jack M Balkin, 'How to Regulate (and Not Regulate) Social Media', *Journal of Free Speech Law*, 1.1 (2021), 71–96.
[1072] Neil Chilson and Adam Thierer, *The Coming Onslaught of 'Algorithmic Fairness' Regulations, AIES 2018 - Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society* (Association for Computing Machinery, Inc, 2 November 2022) <https://doi.org/10.1145/3278721.3278731>.
[1073] African Commission on Human Rights, 'State Parties to the African Charter', *Available at: Https://Www.Achpr.Org/Statepartiestotheafricancharter (Accessed on 15 October 2022)*.

domestic legislation from family law[1074], to employment law[1075], to cyber law[1076]. Like the UK and US, South Africa has cyber law that contains substantive and procedural guidelines regarding criminal activity in cyberspace, however, the does not have regulation that addresses social media specifically. The recent Film and Publications Amendment Act that came into force in 2022, and the SAHRC's subsequent launch of its Social Media Charter in 2023, acknowledges social media as a legitimate site for prohibited activity, but it does not aim to regulate social media practices per se[1077]. Despite the absence of specialised regulation the application of human rights law to cyberspace, as seen in with the POPI Act,[1078] signals a rising concern regarding the potential for social media content personalisation practices to undermine post-Apartheid democratic ideals[1079].

Navigating the multifaceted global landscape of social media regulation, the UK, US, and South Africa each reflect distinctive challenges, intricately tied to their historical and socio-political contexts. The UK's legislative attempts highlight the tension between corporate responsibility and individual freedoms, particularly in light of evolving digital dynamics. The US finds itself at a crossroads, attempting to balance its constitutional ethos with the urgent need for digital oversight. South Africa's post-Apartheid ideals inform its regulatory stance, emphasising rectification and equity, though it confronts gaps in addressing social media's expansive domain. Juxtaposing these three nations' attempts at achieving an effective domestic framework for regulating social media, that is also aligned with regional and international commitments, serves as further evidence of the inherent complexities that arise at the intersection of human rights and cyber law. It is further evident that while each country's approach is informed by its unique circumstances, a shared global challenge in regulating social media is the delicate balance between the state's negative obligation to not interfere with the enjoyment of civil liberties and the state's positive obligation to ensure protection against harm and exploitation.

[1074] Chapter 7 Part 2 of the *Children's Act* (Republic of South Africa, 2005).
[1075] Para. 5 of the *Employment Equity Act* (Republic of South Africa, 1998).
[1076] Preamble to the *Protection of Personal Information Act* (Republic of South Africa, 2013).
[1077] Government Gazette, *Films and Publications Amendment Act* (Republic of South Africa, 2019).
[1078] Gilad Katzav, 'Compartmentalised Data Protection in South Africa: The Right to Privacy in the Protection of Personal Information Act', *South African Law Journal*, 139.2 (2022), 432–70.
[1079] Lena Nyahodza and Richard Higgs, 'Towards Bridging the Digital Divide in Post-Apartheid South Africa: A Case of a Historically Disadvantaged University in Cape Town', *South African Journal of Libraries and Information Science*, 83.1 (2017), 39–48 <https://doi.org/10.7553/83-1-1645>.

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

6.1. Introduction

This chapter critically reflects on analyses presented in the preceding chapters and offers answers to the research questions posed in Chapter 1. These include several gaps and complexities related to the enforcement of international human rights in the borderless realm of social media. The chapter also outlines how regional variations in the maturity and implementation of human rights and cyber law, across the European, American, and African regions present challenges. The chapter then presents an integration of the analyses at domestic level and offers commentary on how the UK, US, and South Africa approach social media regulation and the challenges they face in balancing cybersecurity, user protection, democratic values, and human rights. The chapter concludes by offering recommendations at international, regional, and domestic levels. These include revisiting international legal instruments for digital age compatibility, developing comprehensive international cyber law standards, monitoring social media corporations globally, harmonising robust regional cyber law frameworks, strengthening enforcement mechanisms, and establishing clear and comprehensive social media regulations within countries.

6.2. Answer to the research question

An analysis of international treaties, optional protocols, case law, and legal scholarship highlights significant gaps and challenges in international legal frameworks' capacity to safeguard against potential violations of Article 25(b) of the ICCPR by social media content personalisation practices. With significant international cyber law treaties still in development[1080, 1081, 1082], this study applied international human rights law to the context of social media. Substantively, the apparent underpinning assumption that individual enjoyment of specific human rights can be compartmentalised as independent state-actor dyads, may not sufficiently account for the *inter*-actor interconnectedness of these rights in cyberspace. Whilst the *intra*-actor interconnectedness of rights – such as overlaps between the right to health, life,

[1080] General Assembly, 'Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on Its Fourth Session', *A/AC.291/17, Adopted in Vienna on 2 February 2023* <www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fourth_session/main.html.>.

[1081] General Assembly, 'Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes Fifth Session', *A/AC.291/L.10, Adopted in Vienna on 21 April 2023* <www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/Revised_meth>.

[1082] United Nations Office on Drugs and Crime, 'Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes', *Meetings of the Ad Hoc Committee*, 2023 <https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home> [accessed 28 May 2023].

physical integrity, housing, food, and employment, for example – is widely acknowledged and practised[1083], international frameworks appear less attuned to inter-actor human right dynamics. Trends in online stochastic terrorism serve as an illustration: unchecked social media algorithms, intent on extracting maximum value from the Attention Economy, can escalate an individual's legitimate exercise of freedom of expression into a propagandist tool[1084]. This can inadvertently radicalise otherwise rational, "well-meaning" users, exerting undue influence over them[1085] and thus, compromising their ability for a free expression of will while participating in the conduct of public affairs[1086].

Procedurally, the manner in which international complaint mechanisms are structured appears to be incompatible with the human rights challenges associated with cyberspace. State parties to the First Optional Protocol to the ICCPR recognise the mandate of the UNHRC to receive and consider claims of human rights violations from individuals subject to its jurisdiction[1087]. This structure assumes linearly between the individual, the State party, and the UNHRC in the protection of human rights. The borderless nature of social media challenges this assumption, as the actions of both social media corporations and social media users in one jurisdiction can cascade across borders into real-world consequences in another, and thus the requirement to exhaust domestic remedies prior to an application to the UNHRC[1088] would not be possible. Recent steps taken by the UNHRC, such as expanding the mandate of the Special Rapporteur on the right to freedom of opinion and expression[1089], signal an acknowledgement of this challenge. The efficacy of these measures remains untested against the complexities of proprietary algorithms driving content personalisation, with the 'black box problem'[1090] they pose potentially undermining global rights like freedom of expression, association, and informed political participation. Furthermore, an evidentiary challenge to international frameworks providing effective mechanisms for preventing social media content

[1083] E.U. Petersmann, 'On "Indivisibility" of Human Rights', *European Journal of International Law*, 14.2 (2003), 381–85 <https://doi.org/10.1093/ejil/14.2.381>.
[1084] Nancy Unger, 'That the Worst Shooting in US History Took Place in a Gay Bar Is Unsurprising', *History News Network*, 13 June 2016 <https://www.advocate.com/politics/2022/8/16/attacks-lgbtq-community-amount-stochastic-terrorism>.
[1085] Fay Niker, Peter B. Reiner, and Gidon Felsen, 'Perceptions of Undue Influence Shed Light on the Folk Conception of Autonomy', *Frontiers in Psychology*, 9 (2018), 1–11 <https://doi.org/10.3389/fpsyg.2018.01400>.
[1086] Hannah Arendt, *Eichmann in Jerusalem: A Report on the Banality of Evil*, 2nd edn (London: Penguin, 2006) <https://doi.org/10.1057/palgrave.cpt.9300095>.
[1087] Article 1 of the UN General Assembly, 'Optional Protocol to the International Covenant on Civil and Political Rights', *2200A(XXI), Adopted 23 March 1976* <https://www.ohchr.org/Documents/ProfessionalInterest/ccpr-one.pdf>.
[1088] Article 2 of the UN General Assembly, 'Optional Protocol to the International Covenant on Civil and Political Rights', *2200A(XXI), Adopted 23 March 1976* <https://www.ohchr.org/Documents/ProfessionalInterest/ccpr-one.pdf>.
[1089] UN General Assembly, 'Resolution on the Special Rapporteur on the Right to Freedom of Opinion and Expression', *A/HRC/RES/43/4, Adopted 30 June 2020* <https://doi.org/10.1017/s0020818300031660>.
[1090] U. Reviglio and C. Agosti, 'Thinking Outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media', *Social Media+ Society*, 6.2 (2020), 2056305120915613.

personalisation from violating Article 25(b) of the ICCPR was also identified. Specifically, the impact of social media discourse on political outcomes is well documented at a societal level[1091]. However, if one were to bring a case before the UNHRC, claiming a violation of Article 25(b) of the ICCPR, a material connection between user-generated content, how it is presented and filtered to other users, and one's own ability to participate in the conduct of public affairs would arguably be very difficult to prove. The current burden of proof, in matters related to social media and democratic participation, might thus pose a significant barrier to safeguarding international human rights.

An analysis at the regional level reveals distinct differences in the maturity and implementation of human rights and cyber law across the European, American, and African regions. While human rights law is deeply entrenched in established conventions, cyber law, despite its rapid growth, shows gaps in providing comprehensive protections, particularly with regard to social media regulation. Tracing the legal development trajectories, distinct regional differences in substantive rights, procedural guarantees, and enforcement mechanisms emerge. Of the three regions, the European region stands out as the most evolved in its ability to acknowledge and address the complexities that arise from the intersection of human rights and of cyber law. Most notably, the Budapest Convention serves as an exemplary instrument, highlighting the European region's proactive approach to harmonising legal frameworks and facilitating international cooperation in addressing cybercrime[1092]. Given its comprehensive structure and relevance, various countries outside of the European region have also adopted the Convention. While primarily aimed at addressing criminal activity, the Budapest Convention sets a robust precedent for understanding the nuances and implications of online activity, arguably paving the way for the broader considerations of human rights in cyberspace, seen in instruments such as the GDPR[1093]. Setting stringent standards for data protection, and enshrining principles like the right to be forgotten, data portability, and data minimization[1094], the GDPR as a cyber law instrument, reflects more closely core human rights principles, such as the right to privacy[1095],

[1091] Orlowski.
[1092] Alexander Seger, 'The Budapest Convention 10 Years on: Lessons Learnt', in *Cybercriminality: Finding a Balance between Freedom and Security*, ed. by Stefano Manacorda, Roberto. Flor, and Joon Oh. Jang (Courmayeur: ISPAC, 2012), pp. 167–78.
[1093] Anup Kumar Das, 'European Union's General Data Protection Regulation, 2018: A Brief Overview', *Annals of Library and Information Studies*, 65 (2018), 139–40 <http://www.ifla.org/node/36104>.
[1094] He Li, Lu Yu, and Wu He, 'The Impact of GDPR on Global Technology Development', *Journal of Global Information Technology Management*, 22.1 (2019), 1–6 <https://doi.org/10.1080/1097198X.2019.1569186>.
[1095] Articles 5 and 6 of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].

freedom of expression[1096], and the right to effective remedy[1097]. However, the GDPR's emphasis on individual rights leaves ambiguity in its applicability to collective societal impacts. The jurisprudence emerging from Europe, such as the Google Spain[1098] and Delfi AS[1099] cases, offers some direction in the socially responsible use of personal data. Nevertheless, they largely focus on individual rights, thereby leaving the broader societal impacts of social media content personalisation, and the associated mechanisms for redress in instances of it violating human rights, largely unaddressed. Resultantly, the onus of navigating potential digital manipulation is largely placed on individuals, who are expected to actively opt out of content personalisation should they desire to do so. Even if state parties were to assume the positive obligation to prevent this specific type of human rights violation in cyberspace, it is unclear how the European framework will consider evidencing the societal consequences such as social fragmentation and political polarisation at an individual rights level. Thus, while Europe provides a robust framework at the intersection of cyber law and human rights, it falls short in specifically addressing the risks posed by social media content personalisation vis-à-vis Article 25(b) of the ICCPR.

OAS member states appear to have followed their own distinct trajectory in the American region, aligning cyber law frameworks with a strong emphasis on cybersecurity capacity building, threat mitigation, and the fostering of international cooperation[1100]. Their approach, markedly pragmatic, addresses immediate concerns of cyber threats, as evidenced by the Comprehensive Inter-American Cybersecurity Strategy, CMMs, and the GFCE-OAS Regional Hub[1101]. Yet, this emphasis on the technical intricacies of cybersecurity raises concerns about the broader human rights implications, particularly when assessing the region's safeguards against potential violations of Article 25(b) of the ICCPR that could arise from social media content personalisation. While the European region appears to has demonstrated that interweaving cyber law with human rights in a contemporary manner is indeed possible, the American trajectory, appears to tilt heavily towards the technical side of cyber threats. This more narrow focus has arguably left a chasm in the region's ability to protect human rights in cyberspace. Additionally, the region's reliance on regional networks like national CSIRTs and

[1096] Articles 77-79 of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].
[1097] Article 9(1) of the 'General Data Protection Regulation', *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023].
[1098] Google v. González.
[1099] 'Delfi AS v Estonia', *Application No. 64569/09 (ECtHR)*, 2013.
[1100] Contreras.
[1101] OAS General Assembly, 'Resolution Advancing Hemispheric Security: A Multidimensional Approach'.

REMJA serves as a testament to OAS member states' commitment to fortifying regional cyber law enforcement through cooperation. Yet, the effectiveness of these networks hinges on uniform interpretation and application of cyber laws, which introduces an additional layer of complexity given the region's political pluralism[1102]. The absence of a cohesive, harmonised legal doctrine in the American region[1103], particularly when juxtaposed against the European region's more synthesised approach, underlines the complexities in addressing human rights in cyberspace. Although the adherence of American nations to the Budapest Convention and the significant legal precedents established by the IACtHR in cases like *Escher et al. v Brazil*[1104] and *Rios et al. v Venezuela*[1105] indicates an acknowledgement of the need for legal mechanisms to protect rights such as privacy and freedom of thought within cyberspace, a discernible void remains with respect to social media content personalisation and its potential for interfering with the free expression of will through participation in the conduct public affairs by universal and equal suffrage.

Within the African region, human rights protections are fairly well developed with similar international treaties[1106], enforcement mechanisms[1107] and emerging jurisprudence[1108], mirroring the European and American regions. Distinguishing the African region from the European and American regions, is the presence of numerous sub-regional cyber law initiatives such as the EAC's harmonised regional cyber law framework[1109] and the ECOWAS Supplementary Act on Personal Data Protection in 2010[1110] and Directive on Fighting Cybercrime in 2011[1111]. While sub-regional instruments aim to protect individual rights[1112], there also appear to be a notable focus on facilitating the development of e-commerce within

[1102] Alejandro Fuentes, 'Judicial Interpretation and Indigenous Peoples' Rights to Lands, Participation and Consultation. The Inter-American Court of Human Rights' Approach', *International Journal on Minority and Group Rights*, 23.1 (2016), 39–79 <https://doi.org/10.1163/15718115-02202006>.
[1103] J. de Arimatéia da Cruz and N. Godbee, 'Cybercrime Initiatives South of the Border: A Complicated Endeavor', in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, ed. by T Thomas J. Holt and Adam M. Bossler (Cham: Palgrave Macmillan, 2020), pp. 365–84.
[1104] 'Case of Escher and Others v. Brazil: Global Perspective', *Global Freedom of Expression Columbia University*, 2023 <https://globalfreedomofexpression.columbia.edu/cases/case-of-escher-and-others-v-brasil/> [accessed 19 June 2023].
[1105] 'Ríos v Venezuela'.
[1106] Article 1 of the 'African Charter on Human and Peoples' Rights', *CAB/LEG/67/3, Adopted on 27 June 1982 in Banjul*, 1982 <https://doi.org/10.9783/9780812205381.713>.
[1107] Article 30 of the 'African Charter on Human and Peoples' Rights', *CAB/LEG/67/3, Adopted on 27 June 1982 in Banjul*, 1982 <https://doi.org/10.9783/9780812205381.713>.
[1108] Lilian Chenwi, 'Exhaustion of Local Remedies Rule in the Jurisprudence of the African Court on Human and Peoples' Rights', *Human Rights Quarterly*, 41.2 (2019), 374–98 <https://heinonline.org/HOL/License>.
[1109] UNCTAD, *Harmonizing Cyberlaws and Regulations: The Experience of the East African Community* (Geneva, 2012).
[1110] ECOWAS, 'Supplementary on Personal Data Protection within ECOWAS', *Act A/SA.1/01/10, Adopted in Abuja on 16 February 2010*.
[1111] ECOWAS, 'Directive on Fighting Cyber Crime within ECOWAS', *C/DIR.1/08/11, Adopted in Abuja on 19 August 2011*.
[1112] Article 23 of the 'Supplementary on Personal Data Protection within ECOWAS'.

the region[1113, 1114]. Yet, when examining the AU as a whole, especially at the intersection of human rights and cyber law, the regional framework is still in its infancy. Beyond the apparent economic focus, the African region resonates with elements of the European contexts, such as the Malabo Convention on Cyber Security and Personal Data Protection, which is similar to the legalistic approaches of the Budapest Convention and the GDPR. Similarly, parallels can be drawn between the OAS and AU's approaches to international collaboration. Through bodies such as the ACS3C and AUCSEG[1115], the AU reinforces the Malabo Convention's regional impact through monitoring and cooperation, in a similar manner to the OAS's CMMs and GFCE-OAS Regional Hub[1116]. However, considering regional mechanisms pertaining to social media regulation, the African narrative seems less concrete. The safeguards built into the AU's Internet Infrastructure Security Guidelines, coupled with the Malabo Convention's provisions, present an optimistic view of the protection of human rights protections in cyberspace, yet, any claims to this framework's efficacy hinge precariously on establishing a direct link between social media content personalisation and "the right to participate freely in the government of [one's] country, either directly or through freely chosen representatives"[1117]. In its current state, the African framework, like the European and American frameworks inadvertently places the onus of navigating the complex terrain of digital manipulation on the individual as opposed to the state. This challenge is further exacerbated by a notable disconnect between the adoption of this progressive legal scaffold and the actual on-ground enforcement capabilities across AU member states[1118, 1119]. Despite these challenges, the African region's distinct perspective on human rights – emphasising not just individual but also group rights[1120] – presents an alternative framework. This approach could inform regional cyber law instruments and mechanisms, potentially offering a more effective defence against social media's interference with democratic participation, and providing a model from which other regions might benefit.

[1113] UNCTAD, *Harmonizing Cyberlaws and Regulations: The Experience of the East African Community* (Geneva, 2012).
[1114] Article 13 of the 'Directive on Fighting Cyber Crime within ECOWAS'.
[1115] AU Executive Council, 'Decisions of the Thirty-Second Ordinary Session', *EX.CL/Dec.986-1007(XXXII), Adopted in Addis Ababa on 26 January 2018*.
[1116] OAS General Assembly, 'Resolution Advancing Hemispheric Security: A Multidimensional Approach'.
[1117] Article 13(1) of the 'African Charter on Human and Peoples' Rights', *CAB/LEG/67/3, Adopted on 27 June 1982 in Banjul*, 1982 <https://doi.org/10.9783/9780812205381.713>.
[1118] Tomiwa Ilori, 'Data Protection in Africa and the COVID-19 Pandemic: Old Problems, New Challenges and Multistakeholder Solutions', *Association for Progressive Communications*, 2020.
[1119] Alex B. Makulilo, 'The Long Arm of GDPR in Africa: Reflection on Data Privacy Law Reform and Practice in Mauritius', *International Journal of Human Rights*, 25.1 (2020), 117–46 <https://doi.org/10.1080/13642987.2020.1783532>.
[1120] M. Ssenyonjo, 'Responding to Human Rights Violations in Africa: Assessing the Role of the African Commission and Court on Human and Peoples' Rights (1987–2018)', *International Human Rights Law Review*, 7.1 (2018), 1–42.

The granularity of domestic legal frameworks seems to address some of the gaps present at international and regional levels. Among the three countries examined, the US has a notably more dynamic and steep upward cyber law development trajectory, while South Africa lags behind in developing domestic instruments and mechanisms for social media regulation. In particular, both the US[1121] and the UK[1122] have legislation under development that addresses the impact of social media and social media corporations' related responsibilities for this impact. In the UK, the evolution of the Online Harms White Paper into a revised Online Safety Bill, represents the country's commitment to develop nuanced cyber law that goes beyond cybercrime and data protection. Specifically, an introduction of the concept of a "duty of care" for social media corporations, the UK addresses the global and regional challenge where individuals bear the brunt of navigating potential digital manipulation, proposing instead that this responsibility be borne by social media corporations. Yet, despite advancements, criticisms particularly concerning algorithmic transparency[1123] highlight enduring gaps in the UK's domestic frameworks' capacity for preventing social media content personalisation from interfering with the rights enshrined in Article 25(b) of the ICCPR.

Unlike the UK's harm-centric approach, the US emphasises protection against exploitation. Arguably as a result of such an emphasis on exploitation, domestic cyber law developments in the US have shown a much more direct focus on the algorithms that drive social media corporation practices[1124], such as content personalisation. Such approaches to legislating, and regulating the specific mechanisms by which social media corporations operate, addresses the global and regional challenge where individuals bear the brunt of navigating potential digital manipulation, it resolve challenges regarding assumptions of linearity of human rights, and evidentiary challenges, and creates mechanisms which the state can use to fulfil its positive obligation to guarantee the right to participate in the conduct of public affairs "by universal and equal suffrage" and in a manner that guarantees "the free expression of the will of the electors"[1125]. However, this approach isn't without critique. There are concerns that while the state strives to uphold its positive obligation to ensure free democratic participation, it may

[1121] Neil Chilson and Adam Thierer, *The Coming Onslaught of 'Algorithmic Fairness' Regulations, AIES 2018 - Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society* (Association for Computing Machinery, Inc, 2 November 2022) <https://doi.org/10.1145/3278721.3278731>.
[1122] House of Lords, 'Online Safety Bill', *Parliamentary Bills*, 2023 <https://bills.parliament.uk/bills/3137>.
[1123] U. Reviglio and C. Agosti, 'Thinking Outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media', *Social Media+ Society*, 6.2 (2020), 2056305120915613.
[1124] Neil Chilson and Adam Thierer, *The Coming Onslaught of 'Algorithmic Fairness' Regulations, AIES 2018 - Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society* (Association for Computing Machinery, Inc, 2 November 2022) <https://doi.org/10.1145/3278721.3278731>.
[1125] Article 25(b) of the 'International Covenant on Civil and Political Rights', *2200A(XXI), adopted 23 March 1979.*

neglect its negative obligation to prevent undue interference with individual freedoms of thought and expression on regulated social media platforms. Lastly, South Africa presents a unique case, having its legal foundations deeply rooted in rectifying historical injustices and preventing the recurrence of systemic inequalities. While this ethos is manifest in alignment with regional human rights standards and widespread domestic legislation, there's a noticeable gap in its domestic legal frameworks concerning social media. Despite recognising the potential for cyberspace criminality, as seen in the Film and Publications Amendment Act of 2019 and the Cybercrimes Act of 2020, there's an absence of specific regulations tailored to social media. Consideration for human rights protections in cyberspace, represented in instruments such as the POPI Act, does hint at burgeoning concerns about social media's influence on South African society. Yet, the absence of specialised social media regulation, like those currently being developed in the UK and US, suggests an urgent need for more comprehensive legal frameworks to address social media more directly, especially given its potential to undermine post-Apartheid democratic ideals.

6.3. Way forward

6.3.1. International recommendations

6.3.1.1. Revisiting and reinterpreting international legal instruments

In order to acknowledge the changes in material threats to human rights globally, international instruments such as the ICCPR must be revisited and reinterpreted for compatibility with the digital age. Revision and reinterpretation should stress-test foundation instruments so ensure their rigour in holding states accountable for ensuring the enjoyment of human rights by those within its jurisdiction. The efficacy of both soft and hard law instruments at an international level in addressing the human rights implications of social media and other online activities necessitates a thorough examination. This includes re-evaluating widely accepted assumptions about (a) inter-actor interconnectedness, (b) the linear relationship among the individual, the State party, and the UNHRC, and (c) the burden of proof.

6.3.1.2. Develop comprehensive international standards for cyberspace

This research revealed a clear need for the international community to accelerate the development and adoption of comprehensive international cyber law treaties, which directly address the challenges posed by the widespread use of social media. One option for such a development of unified international standards is a new Optional Protocol to the ICCPR on Digital Rights. Such an Optional Protocol can draw on the gaps identified at international level

regarding substantive, procedural and evidentiary challenges, but also from insights gained at a domestic level regarding factors such as social media corporations' duty of care and algorithmic transparency.

6.3.1.3. International monitoring of social media corporations

An analysis of existing human rights monitoring and complaints mechanisms makes a compelling case for the creation of an international body or expansion of the mandate of existing bodies to monitor and regulate the practices of global social media corporations, and in particular how they impact on or interfere with fundamental rights. Such initiatives might include the establishment of an Expert Committee on Digital Rights, or further extending the mandate of the Special Rapporteur on the right to freedom of opinion and expression. An Expert Committee would ideally be composed of experts in digital technology, international law, and human rights, who can continually assess the evolving landscape of social media and its interplay with civil and political rights. Such a Committee could also be instrumental in providing guidance to State parties, issuing recommendations, and offering interpretative clarity on the provisions of the new Optional Protocol on Digital Rights. An extension of the Rapporteur's mandate should offer an acknowledgement of the evolving challenges of protecting human rights in cyberspace and provide such a key stakeholder with the necessary tools and jurisdiction to examine and address the nuances of these challenges effectively.

6.3.2. Regional recommendations

6.3.2.1. Harmonise robust regional cyber law frameworks

Regional bodies in the European, American, and African regions should actively collaborate to develop a harmonised legal approach to the challenges posed by rapid technological growth, particularly social media content personalisation. This includes incorporating established human rights law principles to ensure both regional provisions for individual rights and addressing the broader societal impacts. Regional bodies should take lessons from established frameworks, such as the GDPR, while also proactively addressing gaps like the relative lack of attention to societal implications. This would ideally involve a multi-stakeholder approach, ensuring that technologists, human rights experts, and legislators collaborate to craft legislation and policy guidelines that are both technically feasible and human rights-compliant.

6.3.2.2. Strengthen enforcement mechanisms

Given the disparity in enforcement capabilities across regions, especially noted in the African context, there is a pressing need to bridge the gap between progressive legal frameworks and

practical implementation. This involves empowering regional enforcement bodies, ensuring they are equipped with the necessary resources and expertise, and holding member states accountable. Given the borderless nature of digital threats, there is also a need for a coordinated, region-wide approach to enforcement that goes beyond current cooperation initiatives that are largely focussed on cybercrime.

6.3.2.3. Similar regional research in the Asian context

Considering the global influence of platforms like TikTok, which has its roots in the Asian region, it would be prudent to conduct similar regional analyses of cyber law, and its intersection with human rights law in Asia. TikTok's unprecedented growth and its CEO, Shou Zi Chew's, recent testimony before the US Congress highlight the international concerns surrounding content moderation, privacy, and potential state influences. Regional bodies in Asia should not only probe the implications of such platforms but also understand the broader dynamics of content personalisation and its societal impacts specific to the Asian context. Given the diverse socio-political and cultural landscapes in Asia, this research would offer invaluable insights into how the impact of social media content personalisation manifests as interference with human rights across regions.

6.3.3. Domestic recommendations

6.3.3.1. Establish clear and comprehensive social media regulation

Countries must recognise the intricate balance needed between cybersecurity, user protection, democratic ideals, and human rights. Taking cues from international and regional guidelines:

- The UK should further evolve Online Safety Bill, by maintaining an emphasis on the "duty of care", and by actively addressing gaps related to algorithmic transparency. The Bill should also be scrutinised for risks related to the infringements of other freedoms such as freedom of thought and expression.
- While upholding First Amendment rights, the US should continue to focus on regulatory measures that target the underlying algorithms and practices of social media corporations' practices (such as content personalisation), ensuring the preservation of free and fair democratic processes.
- Given the volumes of research proving the impact of social media on democratic processes, and South Africa's general socio-political efforts to correct injustices of the past and dismantle enduring systems of oppression, it is vital that the country develops

social media regulation that goes beyond the current considerations for cybercrime and individual privacy rights.

6.3.3.2. Address algorithmic transparency and accountability

Given the central role algorithms play in content personalisation and their inherent risks to democratic participation:

- The UK and US should delve deeper into the specifics of algorithmic operations, ensuring transparency and accountability. Legislation currently under development should not only address the surface challenges but aim to uncover the core mechanisms of digital manipulation within the Attention Economy.
- South Africa should use the current developments in other countries as an opportunity to learn and develop its own social media regulation that starts with algorithmic transparency, rather than working towards it.

6.3.3.3. Continuous monitoring and iteration of newly developed social media regulation

Given the rapid evolution of technology and the social media landscape:

- The UK should monitor the efficacy of the Online Safety Bill when it comes into power. It is recommended that a specialised body performs this monitoring of implementation in order for changes to the regulation that might be required, given technological changes, to be affected in a manner that is congruent with the speed at which technology advances.
- The US should regularly evaluate its aggressive approach to preventing exploitation, ensuring social media regulation remains constitutionally compliant.
- Similar to the preceding recommendation regarding algorithmic transparency, South Africa should use the current developments in other countries as an opportunity to learn and develop its own specialised monitoring body, concurrently, with regulatory developments that start with algorithmic transparency.

BIBLIOGRAPHY

@enlighten.mentality, 'School for Stochastic Swifties', *TikTok* <https://vm.tiktok.com/ZMYjvxAD7/>

Abbakumova, Daryna V., 'Procedural Aspects of the Functioning of the Committee of Ministers of the Council of Europe', *Journal of Eastern European Law*, 57.4 (2018), 25

Abbott, Kenneth W., and Duncan Snidal, 'Hard and Soft Law in International Governance', *Legalization and World Politics*, 54.3 (2000), 421–56

Abdulrauf, Lukman Adebisi, 'Giving "Teeth" to the African Union towards Advancing Compliance with Data Privacy Norms', *Information & Communications Technology Law*, 30.2 (2021), 87–107 <https://www.tau.ac.il/law/minerva2/Birnhack.pdf>

Abe, A., 'Data Mining in the Age of Curation', in *IEEE 12th International Conference on Data Mining Workshops*, 2012, pp. 273–79

Abraha, Halefom H, 'Government Access to Digital Evidence Across Borders: Some Lessons for Africa', in *The Internet and Policy Responses in Ethiopia: New Beginnings and Uncertainties*, ed. by K.M. Yilma (Addis Ababa: Addis Ababa University Press, 2020), pp. 11–49 <https://bit.ly/2Irp0jq>

Adjolohoun, Sègnonna Horace, 'A Crisis of Design and Judicial Practice? Curbing State Disengagement from the African Court on Human and Peoples' Rights', *African Human Rights Law Journal*, 20.1 (2020), 1–40 <https://doi.org/10.17159/1996-2096/2020/v20n1a1>

Adogamhe, Paul G, 'Pan-Africanism Revisited: Vision and Reality of African Unity and Development', *African Review of Integration*, 2.2 (2008), 1–34

Ægidius Mogensen, T., 'A Brief History of Programming Languages', in *Programming Language Design and Implementation. Texts in Computer Science* (Cham, Switzerland: Springer, 2002), pp. 1–21

African Union, 'About the African Union' <https://au.int/en/overview> [accessed 6 May 2023]

———, 'African Charter on the Rights and Welfare of the Child', *CAB/LEG/24.9/49, Adopted on 11 July 1990*

———, 'Member States', 2023 <https://au.int/en/member_states/countryprofiles2> [accessed 6 May 2023]

———, 'Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa', *AHG/Res.240 (XXXI), Adopted on 11 July 2003*

———, 'Specialised Technical Committees', 2023 <https://au.int/en/stc> [accessed 22 June 2023]

———, 'The Structure and Portfolios of The Senior Leadership of The AU Commission', 2020 <https://au.int/en/announcements/20200707/structure-and-portfolios-senior-leadership-au-commission> [accessed 23 June 2023]

AFRINIC, 'About Us', *African Network Information Centre: Internet Numbers Registry for Africa*, 2023 <https://afrinic.net/about> [accessed 26 June 2023]

———, ‘AFRINIC Government Working Group (AFGWG)’, *African Network Information Centre: Internet Numbers Registry for Africa*, 2023 <https://afrinic.net/committees/afgwg> [accessed 26 June 2023]

———, ‘Governance’, *African Network Information Centre: Internet Numbers Registry for Africa*, 2023 <https://afrinic.net/governance> [accessed 26 June 2023]

———, ‘IPv6 Resources from AFRINIC’, *African Network Information Centre: Internet Numbers Registry for Africa*, 2023 <https://afrinic.net/resources/ipv6> [accessed 26 June 2023]

Aguiar-Aguilar, Azul A., ‘Harmonizing National Law with Inter-American Human Rights Law: Evidence from Mexico’, *Journal of Human Rights*, 15.4 (2016), 477–95

Agung, Dirga, ‘The Role of Interpol in the Settlement of Cybercrime Cases under the Budapest Convention on Cybercrimes’, *International Journal of Global Community*, 5.1 (2022), 49–56

Alexy, Robert, ‘ The Responsibility of Internet Portal Providers for Readers’ Comments. Argumentation and Balancing in the Case of Delfi AS v. Estonia’, in *The Rule of Law in Europe: Recent Challenges and Judicial Responses*, ed. by M. Elósegui, A. Miron, and I. Motoc (Cham: Springer, 2021), pp. 199–213

Allcott, Hunt, and Matthew Gentzkow, ‘Social Media and Fake News in the 2016 Election’, *Journal of Economic Perspectives*, 31.2 (2017), 211–36 <https://doi.org/10.1257/jep.31.2.211>

Alley, Adam, and Jody Hanshew, ‘A Long Article about Short Videos: A Content Analysis of US Academic Libraries’ Use of TikTok’, *The Journal of Academic Librarianship*, 48.6 (2022), 102611

Alonso-Muñoz, Laura, and Andreu Casero-Ripollés, ‘Populism against Europe in Social Media: The Eurosceptic Discourse on Twitter in Spain, Italy, France, and United Kingdom during the Campaign of the 2019 European Parliament Election’, *Frontiers in Communication*, 5.54 (2020), 1–12 <https://doi.org/10.3389/fcomm.2020.00054>

Alston, Philip, ‘The Historical Origins of the Concept of “General Comments” in Human Rights Law’, in *The International Legal System in Quest of Equity and Universality*, ed. by Laurence Boisson de Chazournes and Vera Gowland-Debbas (The Hague: Brill Nijhoff, 2001), pp. 763–76

alt.advisory, ‘What Is the GDPR?’ <https://altadvisory.africa/gdpr/>

ALT Advisory, ‘Africa: AU’s Malabo Convention Set to Enter Force after Nine Years’, *Data Protection Africa*, 2023 <https://dataprotection.africa/malabo-convention-set-to-enter-force/#:~:text=The latest status list on,force by 8 June 2023.&text=This marks a significant milestone,of cybersecurity and data protection.> [accessed 23 June 2023]

———, *The Malabo Roadmap: Approaches to Promote Data Protection and Data Governance in Africa* (Johannesburg, September 2022)

Amazouz, S., ‘Cyber Capacity-Building and International Security’, in *Routledge Handbook of International Cybersecurity*, ed. by E. Tikk and M. Kerttunen (London: Routledge, 2020), pp.

201–13

American Civil Liberties Union, 'The Seven Reasons Why the Senate Should Reject the International Cybercrime Treaty', 2021 <https://www.aclu.org/other/seven-reasons-us-should-reject-international-cybercrime-treaty> [accessed 27 May 2023]

Amman, Molly, and J. Reid Meloy, 'Stochastic Terrorism: A Linguistic and Psychological Analysis', *Perspectives on Terrorism*, 15.5 (2021), 2–13

Anand, Bharat N., 'The US Media's Problems Are Far Bigger Than Fake News and Filter Bubbles', in *Domestic Extremism*, ed. by Eamon Doyle (New York: Greenhaven Publishing, 2022), pp. 138–51

Antunes, Théo, 'Artificial Intelligence as an Undue Influence in Criminal Trials: Issuing the Use of Algorithms under the Principle of Independence of Judges in Europe', in *Artificial Intelligence from the Perspective of Law and Ethics: Contemporary Issues, Challenges and Perspectives* (Košice, Slovakia, 2022)

'Apitz Barbera et Al. ("First Court of Administrative Disputes") v Venezuela', *Series C No. 182 (IACtHR)*, 2008

Arendt, Hannah, *Eichmann in Jerusalem: A Report on the Banality of Evil*, 2nd edn (London: Penguin, 2006) <https://doi.org/10.1057/palgrave.cpt.9300095>

de Arimatéia da Cruz, J., and N. Godbee, 'Cybercrime Initiatives South of the Border: A Complicated Endeavor', in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, ed. by T Thomas J. Holt and Adam M. Bossler (Cham: Palgrave Macmillan, 2020), pp. 365–84

Armstrong, David, 'Inside Purdue Pharma's Media Playbook: How It Planted the Opioid "Anti-Story"', *ProPublica*, 2019 <https://www.fiercepharma.com/pharma/inside-purdue-pharma-s-media-playbook-how-it-planted-opioid-anti-story>

Aschieris, Samantha, '6 Highlights of TikTok CEO's Testimony Before House Pane', *The Daily Signal*, 23 March 2023 <https://www.dailysignal.com/2023/03/23/6-highlights-tiktok-ceos-testimony/> [accessed 5 May 2023]

Assembly of the African Union, 'African Charter on Democracy, Elections and Governance', *Assembly/AU/Dec. 147(VIII), Adopted on 30 January 2007 in Addis Ababa*, 2007

———, 'Protocol of the Court of Justice of the African Union', *Treaty 0026, Adopted on 1 July 2003 in Maputo*, 2003

———, 'Protocol on the Statute of the African Court of Justice and Human Rights', *Adopted on 1 July 2004 in Sharm El-Sheikh*, 2004

———, 'Protocol to the African Charter on Human And Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights', *Treaty 0019, Adopted on 10 June 1998 in Maputo*, 1998

Aten, Jason, 'This Change Is How You Know Elon Musk's Twitter Experiment Has Already Failed: Musk Keeps Thinking He Can Make Twitter Better by Making It Worse', *Inc. Africa*, 16

February 2023

AU Commission, *Annexure 2 of the Draft Digital Transformation Strategy for Africa (2020-2030)* (Addis Ababa, 2 September 2020) <www.au.int>

———, *The Digital Transformation Strategy for Africa (2020-2030)* (Addis Ababa, 9 February 2020) <https://futurium.ec.europa.eu/en/Digital4Development/library/digital-transformation-strategy-africa-2020-2030> [accessed 23 June 2023]

AU Commission, and Internet Society, *Internet Infrastructure Security Guidelines for Africa: A Joint Initiative of the Internet Society and the Commission of the African Union* (Addis Ababa, 30 May 2017)

AU Executive Council, 'Decisions of the Thirty-Second Ordinary Session', *EX.CL/Dec.986-1007(XXXII), Adopted in Addis Ababa on 26 January 2018*

AU General Assembly, 'African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)', *EX.CL/846(XXV), Adopted in Malabo on 27 June 2014*

Auxier, Brooke, and Monica Anderson, 'Social Media Use in 2021', *Pew Research Center*, April, 2021 <https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/>

Aviram, A., and A. Assor, 'In Defence of Personal Autonomy as a Fundamental Educational Aim in Liberal Democracies: A Response to Hand', *Oxford Review of Education*, 36.1 (2010), 111–26

Awosusi, Oladotun E., 'The Imperative of Cyber Diplomacy and Cybersecurity in Africa: A New Means to a "Borderless" Regional End?', *Journal of African Foreign Affairs*, 9.3 (2022), 57–81 <https://doi.org/10.31920/2056-5658/2022/v9n3a3>

Ayalew, Yohannes Eneyew, 'The African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force Nearly after a Decade: What Does It Mean for Data Privacy in Africa or Beyond?', *Blog of the European Journal of International Law*, 15 June 2023 <https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-doe>

Babalola, Olumide, *Data Protection Legal Regime and Data Governance in Africa: An Overview* (Nairobi, February 2023)

Badawy, Adam, Emilio Ferrara, and Kristina Lerman, 'Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign', in *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 2017, pp. 258–65

Bailliet, Cecilia M, 'Measuring Compliance with the Inter-American Court of Human Rights: The Ongoing Challenge of Judicial Independence in Latin America', *Nordic Journal of Human Rights*, 31.4 (2013), 477–95 <www.latinobarometro.org/latino/>

Bakshi, P.M., 'Legal Research and Law Reform', in *Legal Research Methodology*, ed. by S.K. Verma and A. Wani, 2nd edn (New Delhi: Indian Law Institute, 2001), pp. 111–37

Barassi, Veronica, and Emiliano Treré, 'Does Web 3.0 Come after Web 2.0? Deconstructing Theoretical Assumptions through Practice', *New Media and Society*, 14.8 (2012), 1269–85

<https://doi.org/10.1177/1461444812445878>

Barker, Kim, and Olga Jurasz, 'Online Harms White Paper Consultation Response', *Stirling Law School & The Open University Law School*, 2019

de Barros, M.J.Z., and H. Lazarek, 'A Conceptual Model for the Development of Cybersecurity Capacity in Mozambique', in *European Conference on Cyber Warfare and Security* (Coimbra: Academic Conferences International Limited, 2019), pp. 623–XIII

Beagrie, Neil, 'Digital Curation for Science, Digital Libraries, and Individuals', *International Journal of Digital Curation*, 1.1 (2008), 3–16 <https://doi.org/10.2218/ijdc.v1i1.2>

Behan, Cormac, 'Embracing and Resisting Prisoner Enfranchisement: A Comparative Analysis of the Republic of Ireland and the United Kingdom', *Irish Probation Journal*, 11 (2014), 156–76 <www.oireachtas.ie>

Bell, Andrew P., 'Abuse of a Relationship: Undue Influence in English Law and French Law', *European Review of Private Law*, 15.4 (2007), 555–99 <https://doi.org/10.54648/erpl2007030>

Benes, Olga, 'Implementation of the Rulings of the European Court of Human Rights: The Latest Decisions of the Committee of Ministers', *Studii Juridice Universitare*, 2021, 50

Benesch, Susan, 'But Facebook's Not a Country: How to Interpret Human Rights Law for Social Media Companies', *Yale Journal on Regulation Bulletin*, 38, 2020, 86–111

Bennett, W. Lance, 'The Personalization of Politics: Political Identity, Social Media, and Changing Patterns of Participation', *Annals of the American Academy of Political and Social Science*, 644.1 (2012), 20–39

Bernal, Paul, *The Internet, Warts and All: Free Speech, Privacy and Truth* (Cambridge: Cambridge University Press, 2018) <https://doi.org/10.1017/9781108381161>

Bhargava, Vikram R., and Manuel Velasquez, 'Ethics of the Attention Economy: The Problem of Social Media Addiction', *Business Ethics Quarterly*, 31.3 (2021), 321–59 <https://doi.org/10.1017/beq.2020.32>

Bhattacharya, Sanmitra, Padmini Srinivasan, and Phil Polgreen, 'Engagement with Health Agencies on Twitter', *PLoS One*, 9.11 (2014), e112235

Bicudo, Helio, 'The Inter-American Commission on Human Rights and the The Inter-American Commission on Human Rights and the Process of Democratization in Peru', *Human Rights Brief*, 9.2 (2002), 18–20 <https://digitalcommons.wcl.american.edu/hrbrief>

Bignami, F., 'Introduction. A New Field: Comparative Law and Regulation', in *Comparative Law and Regulation: Understanding the Global Regulatory Process*, ed. by F. Bignami and D. Zaring (Cheltenham: Edward Elgar Publishing, 2016), pp. 1–52

Bigwood, Rick, 'Undue Influence: "Impaired Consent" or "Wicked Exploitation"?', *Oxford Journal of Legal Studies*, 16.3 (1996), 503–15

Binder, Matt, 'WordPress Drops Twitter Social Sharing Due to API Price Hike', *Mashable*, 1 May 2023

Birdsall, W., 'Web 2.0 as a Social Movement', *Webology*, 4 (2007), 234–60

Blauberger, Michael, and Susanne K. Schmidt, 'The European Court of Justice and Its Political Impact', *West European Politics*, 40.4 (2017), 907–18 <https://doi.org/10.1080/01402382.2017.1281652>

Bonikowski, Bart, 'Three Lessons of Contemporary Populism in Europe and the United States Populism in the Twenty-First Century', *Brown Journal of World Affairs*, 23.1 (2016), 9–24

Boppana, Samhi, 'TikTok Is Bad for Political Discourse and Furthers Polarization', *The Johns Hopkins News-Letter*, 1 October 2022

Born This Way Foundation, & Yale Center for Emotional Intelligence. 'Keynote Address: Lady Gaga' (2015) *Emotion Revolution Summit.*

Brauch, Jeffrey A., 'The Margin of Appreciation and the Jurisprudence of the European Court of Human Rights: Threat to the Rule of Law', *Columbia Journal Of European Law*, 11 (2004), 113

Briffault, R., *Dollars and Democracy: A Blueprint for Campaign Finance Reform* (New York: Fordham University Press, 2020)

de Brito, A.C., C. Kauffmann, and J. Pelkmans, 'The Contribution of Mutual Recognition to International Regulatory Co-Operation', *OECD Regulatory Policy Working Papers*, 2016

Brown, N. I., and J. Peters, 'Say This, Not That: Government Regulation and Control of Social Media', *Syracuse Law Review*, 68.3 (2018), 521–46 <https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/syrlr68&section=28>

Brown, Yanni, Barbara Pini, and Adele Pavlidis, 'Affective Design and Memetic Qualities: Generating Affect and Political Engagement through Bushfire TikToks', *Journal of Sociology*, 2022, 14407833221110268

Brunner, L., 'The Liability of an Online Intermediary for Third Party Content: The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia ', *Human Rights Law Review*, 16.1 (2016), 163–74

Buono, Laviero, 'Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and the Establishment of the European Cybercrime Centre (EC3)', *New Journal of European Criminal Law*, 3.3 (2012), 332–43

Burnett Heldman, Amy, Jessica Schindelar, and James B Weaver III, 'Social Media Engagement and Public Health Communication: Implications for Public Health Organizations Being Truly "Social"', *Public Health Reviews*, 35.1 (2013), 1–18

Bustamante, T., 'On the Argumentum Ad Absurdum in Statutory Interpretation: Its Uses and Normative Significance', in *Legal Argumentation Theory: Cross-Disciplinary Perspectives*, ed. by C. Dahlman and E. Feteris (Dordrecht: Springer, 2013), pp. 21–44

Callamard, Agnes, 'Are Courts Re---Inventing Internet Regulation?', *International Review of Law, Computers & Technology*, 31.3 (2017), 323–39 <http://www.asef.org/images/stories/publications/documents/ASEF->

Cançado Trindade, Antônio Augusto, 'Compliance with Judgments and Decisions: The Experience of the Inter-American Court of Human Rights: A Reassessment', in *Nigerian Yearbook of International Law*, ed. by Chile Eboe-Osuji and Engobo Emeseh (The Hague: Springer, 2018), pp. 3–16 <http://www.springer.com/series/14355>

Carbonell, F., 'Reasoning by Consequences: Applying Different Argumentation Structures to the Analysis of Consequentialist Reasoning in Judicial Decisions', in *Legal Argumentation Theory: Cross-Disciplinary Perspectives*, ed. by C. Dahlman and E. Feteris (Dordrecht: Springer, 2013), pp. 1–19

Carson, Devin, 'A Content Analysis of Political Discourse on TikTok', *Student Research Submissions*, 415 (2021) <https://scholar.umw.edu/student_research/415>

'Case of Escher and Others v. Brazil: Global Perspective', *Global Freedom of Expression Columbia University*, 2023 <https://globalfreedomofexpression.columbia.edu/cases/case-of-escher-and-others-v-brasil/> [accessed 19 June 2023]

'Castañeda Gutman v México', *Serie C No. 184 (IACtHR)*, 2008

Cauffman, C., and C. Goanta, 'A New Order: The Digital Services Act and Consumer Protection', *European Journal of Risk Regulation*, 12.4 (2021), 758–74

Celeste, Edoardo, 'Terms of Service and Bills of Rights: New Mechanisms of Constitutionalisation in the Social Media Environment?', *International Review of Law, Computers and Technology*, 33.2 (2019), 122–38 <https://doi.org/10.1080/13600869.2018.1475898>

Centieiro, H., 'The Insane Future of Web 3.0 and the Metaverse', *Medium*, 2022 <https://medium.datadriveninvestor.com/the-insane-future-of-web-3-0-and-the-metaverse-4cec3f13895a>

Cerf, Vinton, 'How the Internet Came to Be', in *The Online User's Encyclopedia*, ed. by Bernard Aboba (Boston, MA.: Addison-Wesley, 1993), pp. 103–37

CERN, 'The Birth of the Web' <https://home.cern/science/computing/birth-web#>

Cerna, Christina M., 'The Inter-American System for the Protection of Human Rights', *Florida Journal of International Law*, 16.1 (2004), 195–212

Ceruzzi, Paul E, *A History of Modern Computing* (MIT press, 2003)

Chander, Anupam, Meaza Abraham, Sandeep Chandy, Yuan Fang, Dayoung Park, and Isabel Yu, 'Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation', *Georgetown University Law Center*, 9594 (2021), 1–42 <https://scholarship.law.georgetown.edu/facpub/2374https://ssrn.com/abstract=3827228>

Charlesworth, A., 'Legislating against Computer Misuse: The Trials and Tribulations of the UK Computer Misuse Act 1990', *Journal of Law, Information and Science*, 4.1 (1993), 80–93

Chaudhry, Irfan, and Anatoliy Gruzd, 'Expressing and Challenging Racist Discourse on Facebook: How Social Media Weaken the "Spiral of Silence" Theory', *Policy and Internet*, 9999.9999 (2019), 1–21 <https://doi.org/10.1002/poi3.197>

Chenwi, Lilian, 'Exhaustion of Local Remedies Rule in the Jurisprudence of the African Court on Human and Peoples' Rights', *Human Rights Quarterly*, 41.2 (2019), 374–98 <https://heinonline.org/HOL/License>

Chesney, Robert, and Danielle Keats Citron, '21st Century-Style Truth Decay: Deep Fakes and the Challenge for Privacy, Free Expression, and National Security', *Maryland Law Review*, 78.4 (2019), 882–91 <https://www.washingtontimes.com/news/2019/jan/29/dan-coats-gina->

Christoffersen, Jonas, and Mikael Rask Madsen, *The European Court of Human Rights between Law and Politics* (Oxford: Oxford Academic, 2011)

Christofidou, Maria, Nathan Lea, and Pascal Coorevits, 'A Literature Review on the GDPR, COVID-19 and the Ethical Considerations of Data Protection During a Time of Crisis', *Yearbook of Medical Informatics*, 30.1 (2021), 226–32 <https://doi.org/10.1055/s-0041-1726512>

Chung, Myojung, and John Wihbey, 'Social Media Regulation, Third-Person Effect, and Public Views: A Comparative Study of the United States, the United Kingdom, South Korea, and Mexico', *New Media and Society*, 00.0 (2022), 1–20 <https://doi.org/10.1177/14614448221122996>

Cloarec, Julien, 'The Personalization–Privacy Paradox in the Attention Economy', *Technological Forecasting and Social Change*, 161 (2020), 120299 <https://doi.org/10.1016/j.techfore.2020.120299>

Clough, Jonathan, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation', *Monash University Law Review*, 40.3 (2014), 698–736 <http://www.youtube.com/yt/press/statistics.html>

Codding, George A, 'The International Telecommunications Union: 130 Years of Telecommunications Regulation Telecommunications Regulation', *Denver Journal of International Law & Policy*, 23.3 (1995), 501–11 <https://digitalcommons.du.edu/djilp/vol23/>

Collí Ek, Víctor Manuel, 'Improving Human Rights in Mexico: Constitutional Reforms, International Standards, and New Requirements for Judges International Standards, and New Requirements for Judges', *Human Rights Brief*, 20.2 (2012), 7–14 <https://digitalcommons.wcl.american.edu/hrbrief>

Conac, Pierre-Henri, Luca Enriques, and Martin Gelter, 'Constraining Dominant Shareholders' Self-Dealing: The Legal Framework in France, Germany, and Italy', *European Company and Financial Law Review*, 4.4 (2007), 491–528 <https://doi.org/10.1515/ecfr.2007.025>

Connolly, Anthea, Stephen Day, and Jo Shaw, 'The Contested Case of EU Electoral Rights', in *Making European Citizens: Civic Inclusion in a Transnational Context*, ed. by Richard Bellamy, Dario Castiglione, and Jo Shaw (New York: Palgrave Macmillan, 2006), pp. 31–55

Contesse, Jorge, 'Contestation and Deference in the Inter-American Human Rights System', *Law and Contemporary Problems*, 79.2 (2016), 123–45

Contreras, B., and K.A. Barrett, 'Challenges in Building Regional Capacities in Cybersecurity: A

Regional Organizational Reflection', in *Routledge Handbook of International Cybersecurity*, ed. by E. Tikk and M. Kerttunen (London: Routledge, 2020), pp. 214–17

Contreras, Belisario, *OAS Cybersecurity Capacity Building Efforts* (Washington D.C., 2016)

Conway, M, and J Dillon, 'Future Trends: Live-Streaming Terrorist Attacks?', *VOX-Pol.*, 2016 <http://www.voxpol.eu/download/vox-pol_publication/Live-streaming_FINAL.pdf>

Cop, Burak, and Dogan Eymirliglu, 'The Right of Self-Determination in International Law towards the 40th Anniversary of the Adoption of ICCPR and ICESCR', *Perceptions: Journal of International Affairs*, 10.4 (2018), 115–46

Copeland, B. Jack, and Diane Proudfoot, 'Alan Turing's Forgotten Ideas in Computer Science', *Scientific American*, 280.4 (1998), 98–103 <https://doi.org/10.1038/scientificamerican0499-98>

Corps législatif, 'Code Civil [Civil Code], République Française', 1804

Council of Europe, '46 Member States', *Administrative Entities*

———, 'Albania Becomes 36th State to Sign the Second Additional Protocol to Convention on Cybercrime', *News*, 2023

———, 'Chart of Signatures and Ratifications of Treaty 185', 2023 <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185> [accessed 30 May 2023]

———, 'Chart of Signatures and Ratifications of Treaty 224', 2023 <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224> [accessed 30 May 2023]

———, 'Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*

———, 'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for the High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and the Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)', *Official Journal of the European Union*, I. 333/80 (2022)

———, 'European Convention on Human Rights', *CoE Treaty Series 005, Adopted on 4 November 1950* <https://doi.org/10.1017/S0008197300013908>

———, 'European Convention on Human Rights', *ETS No. 005 Adopted in Rome on 4 November 1950*

———, 'Explanatory Report to the Convention on Cybercrime', *ETS No. 185 Adopted in Budapest on 23 November 2001*

———, 'Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY', *Parties to the Budapest Convention*, 2023 <https://www.coe.int/en/web/cybercrime/parties-observers> [accessed 19 June 2023]

———, 'Protocol No. 1 to the European Convention on Human Rights and Fundamental Freedoms', *ETS No. 009, Adopted in Paris on 20 March 1952*

———, 'Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019

on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 52', *Official Journal of the European Union*, I. 151/15 (2019)

———, 'Regulation 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*, I. 199/1 (2016)

———, 'Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence', *ETS No. 224 Adopted in Strasbourg on 12 May 2022*

———, 'Statute of the Council of Europe', *ETS No. 001, Adopted in London on 5 May 1949*

———, 'The Budapest Convention (ETS No. 185) and Its Protocols', 2023 <https://www.coe.int/en/web/cybercrime/the-budapest-convention> [accessed 19 June 2023]

Council of Europe Treaty Office, 'Chart of Signatures and Ratifications of Treaty 009' <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=009> [accessed 19 April 2023]

Cowell, F., 'Understanding the Legal Status of Universal Periodic Review Recommendations', *Cambridge International Law Journal*, 7.1 (2018), 164–84

CSIRTAmericas, 'Protecting the Americas in Cyberspace', 2023 <https://csirtamericas.org/es> [accessed 19 June 2023]

Cybercrime Directorate, *Global Cybercrime Strategy* (Lyon, France, 2017)

———, *National Cybercrime Strategy Guidebook* (Lyon, France, 2021)

Cybil Portal, 'AfricaCERT', 2023 <https://cybilportal.org/actors/africacert/> [accessed 26 June 2023]

Czapanskiy, Karen Syma, and Rashida Manjoo, 'The Right of Public Participation in the Law-Making Process and the Role of Legislature in the Promotion of This Right', *Duke Journal of Comparative & International Law*, 19:1.12 (2008), 1–40

D'Arcy, J., 'Direct Broadcast Satellites and the Right to Communicate', *EBU Rview*, 118 (1969), 14–18

Dahlmann, Anja, Jamila Venturini, Marcel Dickow, and Marilia Maciel, *Privacy and Surveillance in the Digital Age: A Comparative Study of the Brazilian and German Legal Frameworks* (Rio de Janeiro, 2015)

Dahre, Ulf Johansson, 'Searching for a Middle Ground: Anthropologists and the Debate on the Universalism and the Cultural Relativism of Human Rights', *International Journal of Human Rights*, 21.5 (2017), 611–28 <https://doi.org/10.1080/13642987.2017.1290930>

Daigle, Brian, and Mahnaz Khan, 'The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities', *United States International Trade Commission Journal of International Commerce and Economics*, 2020, 1–38 <https://www.usitc.gov/journals.>

Daly, Tom Gerald, and Micha Wiebusch, 'The African Court on Human and Peoples' Rights: Mapping Resistance against a Young Court', *International Journal of Law in Context*, 14.2 (2018), 294–313 <https://doi.org/10.1017/S1744552318000083>

Daniels, Toby, and Craig Hepburn, *On! The Future of Now: Making Sense of Our Always On, Always Connected World*, ed. by Caroline McCarthy (New York: Crowdcentric Media, 2014) <https://books.google.co.za/books?id=qOVaCAAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>

Das, Anup Kumar, 'European Union's General Data Protection Regulation, 2018: A Brief Overview', *Annals of Library and Information Studies*, 65 (2018), 139–40 <http://www.ifla.org/node/36104>

Davenport, T.H., and J.C. Beck, *The Attention Economy: Understanding the New Currency of Business* (Boston, MA.: Harvard Business School Press, 2001)

David, Raluca, 'Comparative Study of Three International Human Rights Systems and Their Enforcement Mechanisms', *SSRN*, 2009 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1566495> [accessed 19 June 2023]

'Delfi AS v Estonia', *Application No. 64569/09 (ECtHR)*, 2013

Denning, Peter J, 'The Science of Computing: The ARPANET after Twenty Years', *American Scientist*, 77.6 (1989), 530–34

Department for Digital, Culture, Media & Sport and Home Office, 'Draft Online Safety Bill (CP 405)', *House of Commons Bill, UK Parliament*, 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> [accessed 20 July 2023]

———, 'Online Harms White Paper (CP 57)', *HM Government*, 2019 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf> [accessed 20 July 2023]

Dertouzos, Michael L, and Joel Moses, *The Computer Age: A Twenty-Year View* (MIT Press, Cambridge, MA, 1980)

Deutscher Reichstag, 'Bürgerliches Gesetzbuch [Civil Code], Bundesrepublik Deutschland.', *Enacted on 18 August 1896*

Digital Development Partnership, *Integrating Cyber Capacity into the Digital Development Agenda* (The Hague, November 2021) <www.digitaldevelopmentpartnership.org.>

Dixon, M., R. McCorquodale, and S. Williams, *Cases & Materials on International Law*, 6th edn (Oxford: Oxford Press)

Djeffal, Christian, 'Dynamic and Evolutive Interpretation of the ECHR by Domestic Courts?', in *The Interpretation of International Law by Domestic Courts: Uniformity, Diversity, Convergence*, ed. by Helmut Philipp Aust and Georg Nolte (Oxford: Oxford University Press, 2016) <https://doi.org/10.1093/acprof:oso/9780198738923.001.0001>

Doan, L., ‘Queer History Queer Memory: The Case of Alan Turing’, *GLQ: A Journal of Lesbian and Gay Studies*, 23.1 (2017), 113–36

Dulitzky, Ariel, ‘Too Little, Too Late: The Pace of Adjudication of the Inter-American Commission on Human Rights American Commission on Human Right’, *Loyola of Los Angeles International and Comparative Law Review*, 35.2 (2013), 131–208

Dzehtsiarou, Kanstantsin, and Vassilis P. Tzevelekos, ‘The Conscience of Europe That Landed in Strasbourg: A Circle of Life of the European Court of Human Rights’, *European Convention on Human Rights Law Review*, 1.1 (2020), 1–6 <https://doi.org/10.1163/26663236-00101005>

ECOWAS, ‘Directive on Fighting Cyber Crime within ECOWAS’, *C/DIR.1/08/11, Adopted in Abuja on 19 August 2011*

———, ‘Supplementary on Personal Data Protection within ECOWAS’, *Act A/SA.1/01/10, Adopted in Abuja on 16 February 2010*

Edward, ‘The Man Behind the Curtain: The Algorithms of Social Media’, *Inkspire*, 2018 <https://inkspire.org/post/the-man-behind-the-curtain-the-algorithms-of-social-media/-KZd7qog2I8NXTEC5p2_>

Election Law of Bosnia and Herzegovina (Bosnia and Herzegovina, 2001)

Eliot, van Buskirk, ‘Overwhelmed? Welcome the Age of Curation’, *WIRED*, 2010 <https://www.wired.com/2010/05/feeling-overwhelmed-welcome-the-age-of-curation/>

Ellinger, E.P., and K.J. Keith, ‘Legal Research: Techniques and Ideas’, in *Legal Research Methodology*, ed. by S.K. Verma and A. Wani, 2nd edn (New Delhi: Indian Law Institute, 2001), pp. 219–40

Engle, Eric, ‘Universal Human Rights: Generational History’, *Annual Survey of International & Comparative Law*, 2012

Erlingsson, G. Ó., and J. Ödalen, ‘A Normative Theory of Local Government: Connecting Individual Autonomy and Local Self-Determination with Democracy.’, *Lex Localis*, 15.2 (2017), 329

‘Escher et Al. v Brazil’, *Serie C No. 200 (IACtHR)*, 2009

Eshet-Alkalai, Yoram, ‘Digital Literacy: A Conceptual Framework for Survival Skills in the Digital Era’, *Journal of Educational Multimedia and Hypermedia*, 13 (2004), 93–106

Etzioni, Amitai, ‘Should We Privatize Censorship?’, *Issues in Science and Technology*, 36.1 (2019), 19–22 <https://doi.org/10.2307/j.ctt1287kp1.15>

European Council, ‘Unfair Commercial Practices Directive’, *2005/29/EC, Adopted 11 June 2005* <https://doi.org/10.1007/978-3-540-71882-6_7>

European Parliament and of the Council, ‘General Data Protection Regulation’, *Regulation (EU) 2016/679, Adopted on 27 April 2016* <https://gdpr-info.eu/art-5-gdpr/> [accessed 19 June 2023]

Fagbayibo, Babatunde, ‘A Normative Appraisal of the African Union’s Membership Admission Rules’, *Verfassung in Recht Und Übersee*, 50.2 (2017), 156–74 <https://doi.org/10.5771/0506-7286-2017-2-156>

Fahey, Elaine, 'Developing EU Cybercrime and Cybersecurity On Legal Challenges of EU Institutionalisation of Cyber Law-Making', in *The Routledge Handbook of European Integrations*, ed. by T. Hoerber, G. Weber, and I. Cabras (Abingdon, UK: Routledge, 2022), pp. 270–84

Ferre-Pikal, Eva S., 'Frequency Standards, Characterization', ed. by Kai Chang, *Encyclopedia of RF and Microwave Engineering* (Hoboken, New Jersey: Wiley-Interscience, 2005), 1720–29 <http://www.mrw.interscience.wiley.com/erfme>

Føllesdal, A., B. Peters, and G. Ulfstein, *Constituting Europe: The European Court of Human Rights in a National, European and Global Context (Vol. 2)* (Cambridge, UK: Cambridge University Press, 2013)

Franklin, M., R. Bodie, D. Hawtin, and M. Moreira, *The Charter of Human Rights and Principles for the Internet (7th Ed.)* (Geneva, Switzerland: United Nations Internet Governance Forum: Internet Rights & Principles Coalition, 2019)

French, T.R., 'Minding the Gap: 21st Century International Foreign and Comparative Law Research Issues', *Syracuse Journal of International Law and Commerce*, 35 (2007), 159–64

Fuentes, Alejandro, 'Judicial Interpretation and Indigenous Peoples' Rights to Lands, Participation and Consultation. The Inter-American Court of Human Rights' Approach', *International Journal on Minority and Group Rights*, 23.1 (2016), 39–79 <https://doi.org/10.1163/15718115-02202006>

Gaillard, Alexandra, 'Cybersecurity Challenges and Governance Issues in the Cyberspace "When Stronger Passwords Are Not Enough: Governing Cyberspace in Contemporary African Nations" Case Study: Can South Africa and Nigeria Secure Cyberspace without a Lock?', *SSRN*, 2021, 3877526 <https://ssrn.com/abstract=3877526>

Ganesh, Bharath, and Jonathan Bright, 'Countering Extremists on Social Media: Challenges for Strategic Communication and Content Moderation', *Policy and Internet*, 12.1 (2020), 6–19 <https://doi.org/10.1002/poi3.236>

García-Sayán, Diego, 'The Inter-American Court and Constitutionalism in Latin America', *Texas Law Review*, 89 (2011), 1835–62 <http://corteidh.or.cr/historia.cfm>

General Assembly, 'Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes Fifth Session', *A/AC.291/L.10, Adopted in Vienna on 21 April 2023* <www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/Revised_meth>

———, 'Decision 74/567 on Establishing an Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes', *A/74/L.84, Adopted in New York on 14 August 2020*

———, 'Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention

on Countering the Use of Information and Communications Technologies for Criminal Purposes on Its First Session', *A/AC.291/7, Adopted in New York on 11 March 2022* <www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.>

———, 'Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on Its Fourth Session', *A/AC.291/17, Adopted in Vienna on 2 February 2023* <www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fourth_session/main.html.>

———, 'Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on Its Second Session', *A/AC.291/10, Adopted in Vienna on 27 June 2022* <www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home>

———, 'Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on Its Session on Organizational Matters', *A/AC.291/6, Adopted in New York on 24 February 2022* <www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-session->

———, 'Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on Its Third Session', *A/AC.291/14, Adopted in New York on 9 September 2022* <www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_third_session/main.html>

GFCE, 'GFCE Latin America and Caribbean (LAC) Meetings 2021', *GFCE-OAS Capacity Building Meeting*, 2021 <https://thegfce.org/events/gfce-latin-america-and-caribbean-lac-meetings-2021/> [accessed 19 June 2023]

Ghazi-Tehrani, Adam Kavon, and Henry N. Pontell, 'Phishing Evolves: Analyzing the Enduring Cybercrime', *Victims and Offenders*, 16.3 (2021), 316–42 <https://doi.org/10.1080/15564886.2020.1829224>

Global Cyber Security Capacity Centre, *Cybersecurity Capacity Maturity Model for Nations (CMM)* (Oxford, March 2021)

———, *Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition* (Oxford, 31 March 2016)

Goldman, Eric, 'The UK Online Harms White Paper and the Internet's Cable-Ized Future', *Ohio State Technology Law Journal*, 16.2 (2020), 351–62 <https://www.bbc.com/news/technology-50073102>

Good, R., 'Content Curation Approaches: Types and Formats', *Medium*, 2018 <https://medium.com/content-curation-official-guide/content-curation-approaches-types-and-formats-ae2b33fe6a18#>

Google v. González, 'Judgement of the Court of Justice of 13 May 2014 on the Case of Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González'

(C 131/12, p. 21, 2014)

Gosztonyi, Gergely, 'The European Court of Human Rights: Internet Access As a Means of Receiving and Imparting Information and Ideas', *International Comparative Jurisprudence*, 6.2 (2020), 134–40 <https://ucd.idm.oclc.org/login?url=https://www.proquest.com/scholarly-journals/european-court-human-rights-internet-access-as/docview/2516344253/se-2%0Ahttps://JQ6AM9XS3S.search.serialssolutions.com?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=in>

Graham, Roderick, and Ruth Triplett, 'Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization', *Deviant Behavior*, 38.12 (2017), 1371–82 <https://doi.org/10.1080/01639625.2016.1254980>

'Grand Chamber Case of Delfi AS v Estonia', *Application No. 64569/09 (ECtHR)*, 2015

Gray, Joanne E., 'The Geopolitics of "Platforms": The TikTok Challenge', *Internet Policy Review*, 10.2 (2021), 1–26 <https://doi.org/10.14763/2021.2.1557>

Graziadei, Stefan, 'Democracy v Human Rights? The Strasbourg Court and the Challenge of Power Sharing', *European Constitutional Law Review*, 12.1 (2016), 54–84 <https://doi.org/10.1017/S1574019616000043>

Greenleaf, Graham, and Bertil Cottier, 'Comparing African Data Privacy Laws: International, African and Regional Commitments', *University of New South Wales Law Research Series*, 2020 <https://au.int/memberstates>

'Greens and M.T. v the United Kingdom', *Application Nos. 60041/08 and 60054/08 (ECtHR)*, 2010

Grossetti, Quentin, Cédric Du Mouza, and Nicolas Travers, 'Community-Based Recommendations on Twitter: Avoiding The Filter Bubble', *Web Information Systems Engineering*, 2019, 1–16

Gulyás, Ágnes, 'Social Media and Journalism', in *The Routledge Companion to Digital Journalism Studies*, ed. by Bob Franklin and Scott Eldridge (New York: Routledge, 2016), pp. 396–406

Guzman, A., 'TikTok and the Public Sphere: Examining the Structure of Online Discourse' (Texas State University, 2021)

Guzman, Andrew T., and Timothy L. Meyer, 'International Soft Law', *Journal of Legal Analysis*, 2.1 (2010), 171–226 <https://doi.org/10.1093/acprof:oso/9780199299874.003.0005>

Haberfeld, M. R., Joseph F. King, and Charles Andrew Lieberman, 'The United Kingdom and Ireland', in *Terrorism Within Comparative International Context*, 2009, pp. 39–59

'Hack v Janes', *878 So.2d 440, 443 (Fla. Dist. Ct. App.)*, 2004

Handayanti, Asih, 'The Role of Cyber Law in The Use of Technology in Mass Media', *Legal Brief*, 11.5 (2022), 2722–4643 <https://doi.org/10.35335/legal>

Hanif, Ishtiaqe, 'New York City Subway Ends Twitter Service Alerts after Musk Imposes Price Tag on API', *Neowin*, 28 April 2023

Harbinja, Edina, M R Leiser, Kimberley Barker, David Mangan, Felipe Romero-Moreno, and Desara Dushi, *Online Harms White Paper: Consultation Response [BILETA Response to the UK*

Government Consultation 'Online Harms White Paper'], 2019 <http://www.europarl.europa.eu/charter/pdf/text_en.pdf.>

Harris, David, Michael O'Boyle, Edward Bates, and Carla Buckley, *Law of the European Convention on Human Rights*, 4th edn (Oxford: Oxford University Press, 2014)

Harris, Tristan, 'How a Handful of Tech Companies Control Billions of Minds Every Day', *TED*, April (2017)

Hayes, Nick, Cheryl McKinnon, Christopher McClean, and Thayer Frechette, *The Social Media Legal And Regulatory Landscape*, 2013

Heaven, Douglas, 'Taking on the Tech Giants', *New Scientist*, 242.3228 (2019), 18–19 <www.newscientist.com/insight>

Herb, Jeremy, Sara Murray, Alayna Treene, Annie Grayer, and Marshall Cohen, 'Twitter Execs Acknowledge Mistakes with Hunter Biden Laptop Story but Say No Government Involvement', *CNN Politics*, 8 February 2023 <https://edition.cnn.com/2023/02/08/politics/twitter-hearing-house-oversight/index.html>

Hernández-Aguado, Ildefonso, and Elisa Chilet-Rosell, 'Pathways of Undue Influence in Health Policy-Making: A Main Actor's Perspective', *Journal of Epidemiology and Community Health*, 72.2 (2018), 154–59 <https://doi.org/10.1136/jech-2017-209677>

Hernandez, G.I., 'Non-State Actors from the Perspective of the International Court of Justice', in *Participants in the International Legal System: Multiple Perspectives on Non-State Actors in International Law*, ed. by J. d'Aspremont (London: Routledge, 2011), pp. 140–64

Herrman, John, 'TikTok Is Shaping Politics. But How?', *The New York Times*, 28 June 2020 <https://nyti.ms/3g6oHq1>

Heyes, Cecilia, Dan Bang, Nicholas Shea, Christopher D. Frith, and Stephen M. Fleming, 'Knowing Ourselves Together: The Cultural Origins of Metacognition', *Trends in Cognitive Sciences*, 24.5 (2020), 349–62 <https://doi.org/10.1016/j.tics.2020.02.007>

Hintz, Arne, 'Social Media Censorship, Privatized Regulation and New Restrictions to Protest and Dissent', in *Critical Perspectives on Social Media and Protest: Between Control and Emancipation*, ed. by Lina Dencik and Oliver Leistert (London: Rowman & Littlefield, 2015), pp. 109–26 <https://books.google.co.za/books?hl=en&lr=&id=iOHaDwAAQBAJ&oi=fnd&pg=PA109&dq=social+media+privatized+censorship&ots=G88xOc1JLb&sig=-e_s8qW4wGR1oO2PacblII8CgT8&redir_esc=y#v=onepage&q=social media privatized censorship&f=false>

Hiremath, B K, and Anand Y Kenchakkanavar, 'An Alteration of the Web 1.0, Web 2.0 and Web 3.0: A Comparative Study', *Imperial Journal of Interdisciplinary Research*, 2.4 (2016), 705–10 <http://www.imperialjournals.com/index.php/IJIR/article/view/327/320>

'Hirst v the United Kingdom', *Application No. 74025/01 (ECtHR)*, 2005

Hogler, R. (2022). Why it may not matter whether Elon Musk broke US labor laws with his mass firings at Twitter. *The Conversation*. https://theconversation.com/why-it-may-not-matter-whether-elon-musk-broke-us-labor-laws-with-his-mass-firings-at-twitter-194149

Holzleitner, Marie Theres, and Johannes Reichl, 'European Provisions for Cyber Security in the Smart Grid – an Overview of TheNIS-Directive', *Elektrotechnik Und Informationstechnik*, 134.1 (2017), 14–18 <https://doi.org/10.1007/s00502-017-0473-7>

Home Office, *Exiting the European Union Data Protection Electronic Communications Draft Statutory Instruments* (United Kingdom, 2019)

'Horvath v Australia', *No. 1885/2009, U.N. Doc. CCPR/C/110/D/1885/2009*

'Horvath v Australia (HRC, 2014)', *Remedy Australia*

House of Lords, 'Online Safety Bill', *Parliamentary Bills*, 2023 <https://bills.parliament.uk/bills/3137>

Hurel, Louise Marie, 'Beyond the Great Powers: Challenges for Understanding Cyber Operations in Latin America', *Global Security Review*, 2.1 (2022), 21–31 <https://doi.org/10.25148/gsr.2.009786>

'Ibrahim Ben Mohamed Ben Ibrahim Belguith v Republic of Tunisia', *Application No. 017/2021 (ACJHR)*, 2021

Ifeanyi-Ajufo, Nnenna, 'Cybersecurity for Inclusive Digital Transformation in Africa', *Observer Research Foundation*, 2022 <https://www.orfonline.org/expert-speak/cybersecurity-for-inclusive-digital-transformation-in-africa/> [accessed 23 June 2023]

Ilbiz, Ethem, and Christian Kaunert, 'Europol and Cybercrime: Europol's Sharing Decryption Platform', *Journal of Contemporary European Studies*, 30.2 (2022), 270–83 <https://doi.org/10.1080/14782804.2021.1995707>

Ilori, Tomiwa, 'Data Protection in Africa and the COVID-19 Pandemic: Old Problems, New Challenges and Multistakeholder Solutions', *Association for Progressive Communications*, 2020

'In Re Carpenter's Estate', *253 So. 2d 697, 702, Fla.*, 1971

Inter-American Committee against Terrorism, *OAS Cybersecurity Program* (Bogotá, 24 March 2006) <www.oas.org/cyber/>

Inter-American Portal on Cybercrime, 'Home Portal', 2023 <http://www.oas.org/en/sla/dlc/cyber-en/homePortal.asp> [accessed 18 June 2023]

———, 'Working Group', 2023 <http://www.oas.org/en/sla/dlc/cyber-en/grupo-trabajo.asp> [accessed 18 June 2023]

International Telecommunication Union, 'GCI 2017', *ITU-D Cybersecurity*, 2017 <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx> [accessed 19 May 2023]

———, 'GCI Weightage Expert Group Terms of Reference', *ITU/BDT Cyber Security Program*, 2020

———, *Global Cybersecurity Index 2020: Measuring Commitment to Cybersecurity* (Geneva,

Switzerland, 2021)

———, ‘Global Cybersecurity Index Guidelines for Member States’, *ITU/BDT Cyber Security Programme*, Version 0.9 (2019)

INTERPOL, ‘INTERPOL 1923 – How Our History Started ’, 2023 <https://www.interpol.int/en/Who-we-are/INTERPOL-100/1923-how-our-history-started> [accessed 30 May 2023]

———, ‘INTERPOL and the African Union ’, 2023 <https://www.interpol.int/en/Our-partners/International-organization-partners/INTERPOL-and-the-African-Union> [accessed 30 May 2023]

———, ‘INTERPOL and the European Union ’, 2023 <https://www.interpol.int/en/Our-partners/International-organization-partners/INTERPOL-and-the-European-Union> [accessed 30 May 2023]

———, ‘INTERPOL and the United Nations ’, 2023 <https://www.interpol.int/en/Our-partners/International-organization-partners/INTERPOL-and-the-United-Nations> [accessed 30 May 2023]

INTERPOL, and ECOWAS, *WAPIS Guide: Best Practice on Personal Data Protection* (Lyon, June 2020)

Jackson, Jay W., and Verlin B. Hinsz, ‘Group Dynamics and the U.S. Capitol Insurrection: An Introduction to the Special Issue’, *Group Dynamics*, 26.3 (2022), 169–77 <https://doi.org/10.1037/gdn0000193>

James, Cordilia, ‘Your Share of the $725 Million Facebook Settlement Will Be Tiny’, *The Wall Street Journal* (New York City, 19 April 2023) <https://www.wsj.com/articles/your-share-of-the-725m-facebook-settlement-will-be-tiny-93265db0> [accessed 26 April 2023]

Jančiūtė, Laima, ‘European Data Protection Board: A Nascent EU Agency or an “Intergovernmental Club”?’, *International Data Privacy Law*, 10.1 (2020), 57–75

Jansson, Johan, and Brian J. Hracs, ‘Conceptualizing Curation in the Age of Abundance: The Case of Recorded Music’, *Environment and Planning A: Economy and Space*, 50.8 (2018), 1602–25 <https://doi.org/10.1177/0308518X18777497>

Jiang, Jialun Aaron, Skyler Middler, Jed R. Brubaker, and Casey Fiesler, ‘Characterizing Community Guidelines on Social Media Platforms’, in *ACM Conference on Computer Supported Cooperative Work*, 2020, pp. 287–91 <https://doi.org/10.1145/3406865.3418312>

Kaltwasser, Cristóbal Rovira, ‘Explaining the Emergence of Populism in Europe and the Americas’, in *The Promise and Perils of Populism: Global Perspectives*, ed. by Carlos de la Torre (Lexington: University Press of Kentucky, 2015), pp. 189–227

Karlsson-Vinkhuyzen, Sylvia I., and Antto Vihma, ‘Comparing the Legitimacy and Effectiveness of Global Hard and Soft Law: An Analytical Framework’, *Regulation and Governance*, 3.4 (2009), 400–420 <https://doi.org/10.1111/j.1748-5991.2009.01062.x>

Kashyap, Ankit, and Mehak Jonjua, 'Social Media - A New Digital Power to Influence Voters', *International Journal of Scientific and Technology Research*, 9.4 (2020), 693–99

Kekić, D., and D. Subošić, 'Inter-American Telecommunication Commission', *Međunarodna Politika*, 63.1148 (2012), 115–28 <http://www.>

Kemp, Simon, 'Digital 2023: The United Kingdom', 2023 <https://datareportal.com/reports/digital-2023-united-kingdom#:~:text=The UK was home to,percent of the total population.> [accessed 19 July 2023]

Kern, Rebecca, 'TikTok's CEO Did Not Pass the Vibe Check at His First Hill Hearing', *Politico*, 23 March 2023 <https://www.politico.com/news/2023/03/23/tiktok-congressional-hearing-ceo-testifies-over-national-security-concerns-00088498> [accessed 5 May 2023]

Khan, Irene, 'Myanmar: Social Media Companies Must Stand up to Junta's Online Terror Campaign Say UN Experts', *Special Rapporteur on the Right to Freedom of Opinion and Expression*, 2023

Kim, Angella J., and Kim K.P. Johnson, 'Power of Consumers Using Social Media: Examining the Influences of Brand-Related User-Generated Content on Facebook', *Computers in Human Behavior*, 58 (2016), 98–108 <https://doi.org/10.1016/j.chb.2015.12.047>

Kim, Young Mie, Jordan Hsu, David Neiman, Colin Kou, Levi Bankston, Soo Yun Kim, and others, 'The Stealth Media? Groups and Targets behind Divisive Issue Campaigns on Facebook', *Political Communication*, 35.4 (2018), 515–41

Kiyonaga, Anastasia, and Tobias Egner, 'Working Memory as Internal Attention: Toward an Integrative Account of Internal and External Selection Processes', *Psychonomic Bulletin & Review*, 20.2 (2013), 228–42 <https://doi.org/10.3758/s13423-012-0359-y.Working>

Kniestedt, J., 'The 1st 20 Years in the Development of the International-Telegraph-Union: Review on the International Telegraph Conference in Berlin in 1885', *Telecommunication Journal*, 55.9 (1988), 610–14

Koehler, Daniel, *Violence and Terrorism from the Far-Right: Policy Options to Counter an Elusive Threat* (The Hague: International Centre for Counter-Terrorism, 2019) <https://doi.org/10.19165/2019.2.02>

'Kouassi Kouame Patrice and Baba Sylla v Republic of Côte D'Ivoire', *Application No. 015/2021 (ACJHR)*, 2021

Kubin, Emily, and Christian von Sikorski, 'The Role of (Social) Media in Political Polarization: A Systematic Review', *Annals of the International Communication Association*, 45.3 (2021), 188–206 <https://doi.org/10.1080/23808985.2021.1976070>

Kunz, Josef L., 'The Bogota Charter of the Organization of American States', *American Journal of International Law*, 42.3 (1948), 568–89

Land, Molly K., 'Against Privatized Censorship: Proposals for Responsible Delegation', *Virginia Journal of International Law*, 60.2 (2020), 363–432 <https://doi.org/10.2139/ssrn.3442184>

Langin, Katie, 'Fake News Spreads Faster than True News on Twitter—Thanks to People, Not Bots:

Tweets Containing Falsehoods Were 70% More Likely to Be Retweeted than Truthful Tweets', *Science*, 8 March 2018 <https://www.science.org/content/article/fake-news-spreads-faster-true-news-twitter-thanks-people-not-bots>

Lavrysen, Laurens, 'Positive Obligations in the Jurisprudence of the Inter-American Court of Human Rights', *Inter-American and European Human Rights Journal*, 7 (2004), 94–115

Leahy, Denise, and Dudley Dolan, 'Digital Literacy: A Vital Competence for 2010?', in *IFIP TC 3 International Conference on Key Competencies in the Knowledge Society (KCKS) / Held as Part OfWorld Computer Congress (WCC)*, 2010, pp. 210–21

Leeuwen, J. V., and J. Wiedermann, 'The Turing Machine Paradigm in Contemporary Computing', in *Mathematics Unlimited—2001 and Beyond*, ed. by Björn Engquist and Wilfried Schmid (Berlin, Heidelberg: Springer, 2001), pp. 1139–55

Lewis, Tom, '"Diffcult and Slippery Terrain": Hansard, Human Rights and Hirst v UK', *Public Law*, 2006, 209–18

Li, He, Lu Yu, and Wu He, 'The Impact of GDPR on Global Technology Development', *Journal of Global Information Technology Management*, 22.1 (2019), 1–6 <https://doi.org/10.1080/1097198X.2019.1569186>

Lin, J., 'Social Media Has Changed the Lives of Modern Society', *Summit News*, 2020 <https://summitpsnews.org/2020/03/24/social-media-has-changed-the-lives-of-modern-society/>

Liu, Hin-Yan, 'The Digital Disruption of Human Rights Foundations', *Human Rights, Digital Society and the Law: A Research Companion*, June (2019), 75–86 <https://doi.org/10.4324/9781351025386-6>

Llamzon, Aloysius P., 'Jurisdiction and Compliance in Recent Decisions of the International Court of Justice', *European Journal of International Law*, 18.5 (2008), 815–52 <https://doi.org/10.1093/ejil/chm047>

'Lloyds Bank Ltd v Bundy', *[1975] QB 326*

De Londras, Fiona, and Kanstantsin Dzehtsiarou, 'Mission Impossible? Addressing Non-Execution through Infringement Proceedings in the European Court of Human Rights', *International and Comparative Law Quarterly*, 66.2 (2017), 467–90 <https://doi.org/10.1017/S002058931700001X>

Lucchi, Nicola, 'Internet Content Governance and Human Rights', *Vanderbilt Journal of Entertainment and Technology Law*, 16.4 (2014), 809–56

Lyon, Beth, 'The Inter-American Court of Human Rights Defines Unauthorized Migrant Workers' Rights for the Hemisphere: A Comment on Advisory Opinion 18', *New YorkUniversity Review of Law & Social Change*, 28.4 (2004), 547–96 <http://www.corteidh.or.cr/Serie_a_ 18_ing.doc>

MacCarthy, M., *U.K. Government Purges Legal but Harmful Provisions from Its Revised Online Safety Bill* (Washington D.C., 2022)

MacEwan, Neil, 'The Computer Misuse Act 1990: Lessons from Its Past and Predictions for Its

Future', *Criminal Law Review*, 12.1 (2008), 955–67

Magalhães, João Carlos, 'Do Algorithms Shape Character? Considering Algorithmic Ethical Subjectivation', *Social Media and Society*, 4.2 (2018) <https://doi.org/10.1177/2056305118768301>

Maine, H.S., *Ancient Law: Its Connection with the Early History of Society and Its Relation to Modern Ideas* (London: John Murray, 1905) <https://books.google.co.za/books/about/Ancient_Law.html?id=4_4MAAAAIAAJ&printsec=frontcover&source=kp_read_button&hl=en&redir_esc=y#v=onepage&q&f=false>

Makulilo, Alex B., 'The Long Arm of GDPR in Africa: Reflection on Data Privacy Law Reform and Practice in Mauritius', *International Journal of Human Rights*, 25.1 (2020), 117–46 <https://doi.org/10.1080/13642987.2020.1783532>

Makunya, Trésor Muhindo, 'Decisions of the African Court on Human and Peoples' Rights during 2020: Trends and Lessons', *African Human Rights Law Journal*, 21.2 (2021), 1230–64 <https://doi.org/10.17159/1996-2096/2021/v21n2a49>

Mangan, D., and L. Gillies, 'The Legal Challenges of Social Media', in *The Legal Challenges of Social Media*, ed. by D. Mangan and L. Gillies (London: Edward Elgar, 2017), pp. 1–10

Marko, Joseph, and Sergiu Constantin, 'Against Marginalisation', in *Human and Minority Rights Protection by Multiple Diversity Governance: History, Law, Ideology and Politics in European Perspective* (London: Routledge, 2019), pp. 340–95

Markopoulou, Dimitra, Vagelis Papakonstantinou, and Paul de Hert, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation', *Computer Law and Security Review*, 35.6 (2019), 1–11 <https://doi.org/10.1016/j.clsr.2019.06.007>

Martin, Kirsten, 'Ethical Implications and Accountability of Algorithms', *Journal of Business Ethics*, 160.4 (2019), 835–50 <https://doi.org/10.1007/s10551-018-3921-3>

———, 'Recommending an Insurrection: Facebook and Recommendation Algorithms', in *Ethics of Data and Analytics: Concepts and Cases*, ed. by Kirsten Martin (Oxon: CRC Press, 2022), pp. 225–39

Masullo Chen, Gina, Martin J. Riedl, Jeremy L. Shermak, Jordon Brown, and Ori Tenenboim, 'Breakdown of Democratic Norms? Understanding the 2016 US Presidential Election Through Online Comments', *Social Media + Society*, 5.2 (2019), 1–13 <https://doi.org/10.1177/2056305119843637>

Maswikwa, Belinda, Linda Richter, Jay Kaufman, and Arijit Nandi, 'Minimum Marriage Age Laws and the Prevalence of Child Marriage and Adolescent Birth: Evidence from Sub-Saharan Africa', *International Perspectives on Sexual and Reproductive Health*, 41.2 (2015), 58–68 <https://doi.org/10.1363/4105815>

'Mathieu-Mohin and Clerfayt v Belgium', *Application No. 9267/81 (ECtHR)*, 1987

Mazzoli, Eleonora Maria, and Damian Tambini, 'Prioritisation Uncovered: The Discoverability of Public Interest Content Online', *Council of Europe Study DGI(2020)19*, 2020 <https://rm.coe.int/publication-content-prioritisation-report/1680a07a57>

McCants, William, Jarret Brachman, and Joseph Felter, *Militant Ideology Atlas: Research Compendium* (West Point, NY: Combating Terrorism Center, 2006)

McGregor, Lorna, Daragh Murray, and Vivian Ng, 'International Human Rights Law as a Framework for Algorithmic Accountability', *International and Comparative Law Quarterly*, 68.2 (2019), 309–43 <https://doi.org/10.1017/S0020589319000046>

McMahon, Edward, and Marta Ascherio, 'A Step Ahead in Promoting Human Rights? The Universal Periodic Review of the UN Human Rights Council', *Global Governance*, 18.2 (2012), 231–48 <https://doi.org/10.1163/19426720-01802006>

Meeting of Ministers of Justice or Other Ministers or Attorney General of the Americas, 'Conclusions and Recommendations of REMJA IX', *REMJA-IX//Doc.2/12 Rev. 1, Adopted in Quinto, on 29 November 2012*, 2012

———, 'Conclusions and Recommendations to REMJA XI', *REMJA-IX/DOC.2/21 Rev. 1, Held Virtually on 19 May 2021*

———, 'Document on the REMJA Process (Document of Washington)', *REMJA-VII/Doc.6/08 Rev.4, Adopted in Washington D.C. on 19 May 2021*

Menkhaus, Ken, 'Al-Shabaab and Social Media: A Double Edged-Sword', *Brown Journal of World Affairs*, xx.11 (2014), 309–28

Meral, Kevser Zeynep, 'Social Media Short Video-Sharing TikTok Application and Ethics: Data Privacy and Addiction Issues', in *Multidisciplinary Approaches to Ethics in the Digital Era*, ed. by Meliha Nurdan Taskiran and Fatih Pinarbasi (IGI Global, 2021), pp. 147–65

Mercier, Hugo, and Dan Sperber, *The Enigma of Reason* (Boston: Harvard University Press, 2017)

Merrills, J.G., and A.H. Robertson, *Human Rights in Europe A Study of the European Convention on Human Rights* (Manchester: Manchester University Press., 2022)

Mihr, Anja, *Cyber Justice: Human Rights and Good Governance for the Internet* (Cham, Switzerland: Springer, 2017)

Miller, D., E. Costa, N. Haynes, T. McDonald, R. Nicolescu, J. Sinanan, and others, *How the World Changed: Social Media, How the World Changed Social Media* (London: UCL Press, 2016) <https://doi.org/10.14324/111.9781910634493>

Milo, Michael, and Jan Smits, 'Trusts in Mixed Legal Systems: A Challenge to Comparative Trust Law', *European Review of Private Law*, 8.3 (2000), 421–26 <https://doi.org/10.54648/273248>

Minárik, Tomáš, and Audrey Garcia, 'Internet Infrastructure Security Guidelines for Africa Unveiled by the African Union', *CCDCOE*, 2017 <https://ccdcoe.org/incyder-articles/internet-infrastructure-security-guidelines-for-africa-unveiled-by-the-african-union/> [accessed 19 July 2023]

Mittelstadt, Brent, 'Auditing for Transparency in Content Personalization Systems', *International Journal of Communication*, 10 (2016), 4991–5002

Molenberghs, Pascal, 'The Neuroscience of In-Group Bias', *Neuroscience and Biobehavioral Reviews*, 37 (2013), 1530–36

Monateri, P.G., 'Methods in Comparative Law: An Intellectual Overview', in *Methods of Comparative Law*, ed. by P.G. Monateri (Cheltenham: Edward Elgar Publishing, 2012), pp. 7–24 <https://books.google.co.za/books/about/Methods_of_Comparative_Law.html?id=Sw095Si6jgcC&printsec=frontcover&source=kp_read_button&hl=en&redir_esc=y#v=onepage&q&f=false>

Morgan, Julian A., 'Provate Censorship on Social Media: A Comparative Analysis of the Horizontal Application of Fundamental Rights', *Social Science Research Network*, 2021, 4012102

Mori, Shigeo, and Atsuhiro Goto, 'Reviewing National Cybersecurity Strategies', *Journal of Disaster Research*, 13.5 (2018), 957–66 <https://doi.org/10.20965/jdr.2018.p0957>

Moss, Lawrence C., 'Opportunities for Nongovernmental Organization Advocacy in the Universal Periodic Review Process at the UN Human Rights Council', *Journal of Human Rights Practice*, 2.1 (2010), 122–50 <https://doi.org/10.1093/jhuman/hup031>

Mostert, Frederick, '"Digital Due Process": A Need for Online Justice', *Journal of Intellectual Property Law & Practice*, 2020 <https://doi.org/10.1093/jiplp/jpaa024>

Moylan, James J, 'The Role of the International Telecommunications Union for the Promotion of Peace through Communication Satellites Promotion of Peace through Communication Satellites', *Case Western Reserve Journal of International Law*, 4.1 (1971), 61–78 <https://scholarlycommons.law.case.edu/jilAvailableat:https://scholarlycommons.law.case.edu/jil/vol4/iss1/5>

Muigua, Kariuki, 'African Court of Justice and Human Rights: Emerging Jurisprudence', *Kariuki Muigua and Company Advocates*, 2020, 1–9 <https://en.african-court.org/>

Mullender, Richard, 'Human Rights: Universalism and Cultural Relativism', *Critical Review of International Social and Political Philosophy*, 6.3 (2003), 70–103 <https://doi.org/10.1080/1369823032000233564>

Muneer, Amgad, and Suliman Mohamed Fati, 'A Comparative Analysis of Machine Learning Techniques for Cyberbullying Detection on Twitter', *Future Internet*, 12.11 (2020), 1–21 <https://doi.org/10.3390/fi12110187>

Murray, Daragh, 'How International Humanitarian Law Treaties Bind Non-State Armed Groups', *Journal of Conflict and Security Law*, 20.1 (2015), 101–31

Myllylahti, Merja, 'An Attention Economy Trap? An Empirical Investigation into Four News Companies' Facebook Traffic and Social Media Revenue', *Journal of Media Business Studies*, 15.4 (2018), 237–53 <https://doi.org/10.1080/16522354.2018.1527521>

Nahon, Karine, 'Where There Is Social Media There Is Politics', in *The Routledge Companion to*

Social Media and Politics, ed. by A. Bruns, E. Skogerbo, C. Christensen, O.A. Larsson, and G.S. Enli (New York: Routledge, 2015), pp. 39–55 <https://doi.org/10.4324/9781315716299>

Napoli, Philip M., 'Social Media and the Public Interest: Governance of News Platforms in the Realm of Individual and Algorithmic Gatekeepers', *Telecommunications Policy*, 39.9 (2015), 751–60 <https://doi.org/10.1016/j.telpol.2014.12.003>

Ndemo, Bitange, and Ben Mkalama, *The Context Digitalization and Financial Data Governance in Africa: Challenges and Opportunities* (Nairobi, June 2022)

Ndizera, Vedaste, and Hannah Muzee, 'A Critical Review of Agenda 2063: Business as Usual?', *African Journal of Political Science and International Relations*, 12.8 (2018), 142–54 <https://doi.org/10.5897/ajpsir2018.1114>

Newmeyer, K.P., 'Elements of National Cybersecurity Strategy for Developing Nations', *National Cybersecurity Institute Journal*, 1.3 (2015), 9–19

Ng, Lynnette Hui Xian, Iain J. Cruickshank, and Kathleen M. Carley, 'Cross-Platform Information Spread during the January 6th Capitol Riots', *Social Network Analysis and Mining*, 12.1 (2022), 1–16 <https://doi.org/10.1007/s13278-022-00937-1>

Niker, Fay, Peter B. Reiner, and Gidon Felsen, 'Perceptions of Undue Influence Shed Light on the Folk Conception of Autonomy', *Frontiers in Psychology*, 9 (2018), 1–11 <https://doi.org/10.3389/fpsyg.2018.01400>

Nix, E., 'The World's First Web Site', *History Channel*, 2018 <https://www.history.com/news/the-worlds-first-web-site>

Nkongho Eno-Akpa, Rene, *The Case for an African Solution to Cybercrime: A Critical Assessment of the African Union Convention on Security in Cyberspace and Personal Data Protection* (Nkozi, 2016) <https://www.newshosting.com/blog/internet-security-defending->

Nonkovic, Marija, 'Government Confirms Proposals to Reform the NIS Regulations in Order to Strengthen UK Cyber Resilience', *Lexology*, 2023 <https://www.lexology.com/library/detail.aspx?g=2309c1d3-7bec-4b2e-b7e1-a8824fe74777> [accessed 22 July 2023]

Ntanda Nsereko, D., and M. Ventura, 'Perspectives on the International Criminal Jurisdiction of the African Court of Justice and Human Rights Pursuant to the Malabo Protocol', in *He African Court of Justice and Human and Peoples' Rights in Context: Development and Challenges*, ed. by J.K. Clarke and V. Nmehielle (Cambridge: Cambridge University Press, 2019), pp. 257–84

Nyirenda-Jere, T., and T. Biru, 'Internet Development and Internet Governance in Africa', *Internet Society*, 2015, 1–44

O'Reilly, Tim, *What Is Web 2.0* (Sebastopol, CA.: O'Reilly Media, Inc., 2009)

OAS General Assembly, 'Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity', *AG/RES. 2004 (XXXIV-O/04), Adopted in Washington D.C. on 8 June 2004*

———, ‘Appendix A: A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity’, *AG/RES. 2004 (XXXIV-O/04), Adopted in Washington D.C. on 8 June 2004*

———, ‘Resolution Advancing Hemispheric Security: A Multidimensional Approach’, *AG/RES. 2945 (XLIX-O/19), Adopted in Washington D.C. on 28 June 2019*

———, ‘Resolution Establishing the Inter-American Telecommunication Commission (CITEL)’, *AG/RES. 1259 (XXIV-O/94), Adopted in Belém on 10 June1994*

‘OAS Member States’ <https://www.oas.org/en/member_states/default.asp> [accessed 25 April 2023]

OAU Assembly, ‘Constitutive Act of the African Union’, *CAB/LEG/23.15, Adopted in Lomé, on 11 July 2000*

———, ‘Treaty Establishing the African Economic Community (Abuja Treaty)’, 1991

Obar, J.A., and S. Wildman, ‘Social Media Definition and the Governance Challenge: An Introduction to the Special Issue’, *Telecommunications Policy*, 39.9 (2015), 745–50

Oberlo, ‘Why Do People Use Social Media’, 2022 <https://www.oberlo.com/statistics/why-do-people-use-social-media>

Obokata, Tom, and Rory O’Connell, ‘The Universal Declaration of Human Rights and the United Kingdom: Developing a Human Rights Culture’, in *60 Years of the Universal Declaration of Human Rights in Europe*, ed. by M. Suksi and V. Jaichand (Antwerp: Intersentia, 2009)

OHCHR, ‘Special Rapporteur on Freedom of Opinion and Expression’

Okoloise, Chairman, ‘Circumventing Obstacles to the Implementation of Recommendations by the African Commission on Human and Peoples’ Rights’, *African Human Rights Law Journal*, 18.1 (2018), 28–57 <https://doi.org/10.17159/1996-2096/2018/v18n1a2>

Organisation of African Unity, ‘OAU/AU Declaration on the Principles Governing Democratic Elections in Africa’, *AHG Decl. 1 (XXXVIII), Adopted on 8 July 2002 in Durban* , 2002

Organization of African Unity, ‘African Charter on Human and Peoples’ Rights’, *CAB/LEG/67/3, Adopted on 27 June 1982 in Banjul*, 1982 <https://doi.org/10.9783/9780812205381.713>

Organization of American States, ‘American Convention on Human Rights’, *No. 17955 Vol. 1144, I-17955, Adopted on 22 November 1969*

———, ‘Charter of the Organization of American States’, *No. 1609*, 1948

Orlowski, Jeff, *The Social Dilemma* (United States: Netflix, 2020) <netflix.com/title/81254224>

Ornes, Stephen, ‘The Internet of Things and the Explosion of Interconnectivity’, *Proceedings of the National Academy of Sciences of the United States of America*, 113.40 (2016), 11059–60 <https://doi.org/10.1073/pnas.1613921113>

Ortutay, B., & O’Brien, M. (2022, November 5). Twitter slashes its staff as Musk era takes hold on platform. *AP News*.

Osaro Edo, Victor, and Michael Abiodun Olanrewaju, ‘An Assessment of the Transformation Of The Organization of African Unity (OAU) To The African Union (AU), 1963-2007’, *Journal of the*

Historical Society of Nigeria, 21 (2012), 41–69 <https://about.jstor.org/terms>

Ostrovsky, Adam M., and Joshua R. Chen, 'TikTok and Its Role in COVID-19 Information Propagation', *Journal of Adolescent Health*, 67.5 (2020), 730 <https://doi.org/10.1016/j.jadohealth.2020.07.039>

Pace, L, and P. Cornish, 'Cybersecurity Capacity Building', in *The Oxford Handbook of Cyber Security*, ed. by The Oxford Handbook of Cyber Security (Oxford: Oxford University Press, 2021), pp. 463–78

Padelford, N.J., 'The Organization of African Unity', *International Organization*, 18.3 (1964), 521–42

Pan American Union General Secretariat of the Organization of American States, 'Fifth Meeting of Consultation of Ministers of Foreign Affairs Santiago, Chile', 1959

Parliament of the United Kingdom, *Data Act Protection* (United Kingdom, 2018)

———, *European Union (Withdrawal) Act* (United Kingdom, 2018)

———, *Human Rights Act* (United Kingdom, 1998)

———, 'Representation of the People Act', 1983 <https://www.legislation.gov.uk/ukpga/1983/2> [accessed 18 April 2023]

———, *The Data Protection, Privacy and Electronic Communications (Amendments Etc) (EU Exit) Regulations* (United Kingdom, 2019) <https://www.legislation.gov.uk/ukdsi/2019/9780111177594/contents> [accessed 21 July 2023]

Parliamentary Assembly of Bosnia and Herzegovina, *Constitution of Bosnia and Herzegovina*, 1995

Pasqualucci, J. M., *The Practice and Procedure of the Inter-American Court of Human Rights* (Cambridge: Cambridge University Press, 2003) <https://doi.org/10.1017/CBO9780511494055.004>

Pathak, R.K., 'Historical Approach to Legal Research', in *Legal Research and Methodology: Perspectives, Process and Practice*, ed. by B.C. Nirmal, R. Kumar Singh, and A. Nirmal (New Delhi: Satyam Law International, 2019), pp. 83–92

Paul, Alvaro, 'Controversial Conceptions: The Unborn and the American Convention on Human Rights Recommended Citation', *Loyola University Chicago International Law Review*, 9.2 (2012), 209–47 <http://lawecommons.luc.edu/lucilr/vol9/iss2/2>

Paul, Kari, 'Ex-Twitter Exec Details "Homophobic and Antisemitic" Abuse over Handling of Hunter Biden Story', *The Guardian*, 8 February 2023

Pauselli, Gino, Francisco Urdinez, and Federico Merke, 'Shaping the Liberal International Order from the Inside: A Natural Experiment on China's Influence in the UN Human Rights Council', *SSRN Electronic Journal*, 2022 <https://doi.org/10.2139/ssrn.4299087>

Pawlak, P., and P. N. Barmpaliou, 'Politics of Cybersecurity Capacity Building: Conundrum and Opportunity', *Journal of Cyber Policy*, 2.1 (2017), 123–44

Pawlak, Patryk, 'Capacity Building in Cyberspace as an Instrument of Foreign Policy', *Global Policy*,

7.1 (2016), 83–92 <https://doi.org/10.1111/1758-5899.12298>

Peisah, C., S. Finkel, K. Shulman, P. Melding, J. Luxenberg, J. Heinik, and others, 'The Wills of Older People: Risk Factors for Undue Influence', *International Psychogeriatrics*, 21.1 (2009), 7–15 <https://doi.org/10.1017/S1041610208008120>

Perera, C., R. Ranjan, L. Wang, S. U. Khan, and A. Y. Zomaya, 'Privacy of Big Data in the Internet of Things Era', *IT Professional*, 17.3 (2015), 32–39

Peters, Allison, and Amy Jordan, 'Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime', *Journal of National Security Law & Policy*, 10 (2019), 487–524 <https://perma.cc/A4YA-X5X6.>

Petersmann, E.U., 'On "Indivisibility" of Human Rights', *European Journal of International Law*, 14.2 (2003), 381–85 <https://doi.org/10.1093/ejil/14.2.381>

Peterson, Larry L, and Bruce S Davie, *Computer Networks: A Systems Approach*, 6th edn (Cambridge, MA: Morgan Kaufmann, 2022)

Petrov, J., 'The Populist Challenge to Human Rights', *International Journal of Constitutional Law*, 18.2 (2020), 476–91 <https://doi.org/10.1093/jhuman/hux007>

Petrović, Saša, Miles Osborne, Richard McCreadie, Craig MacDonald, Iadh Ounis, and Luke Shrimpton, 'Can Twitter Replace Newswire for Breaking News?', in *7th International Conference on Weblogs and Social Media*, 2013, pp. 713–16 <https://doi.org/10.1609/icwsm.v7i1.14450>

Piza, Rodolfo, 'Coordination of the Mechanisms for the Protection of Human Rights in the American Convention with Those Established by the United Nations', *The American University Law Review*, 30.1 (1980), 167

Plagis, M.A., 'The Makings of Remedies: The (R)Evolution of the African Court on Human and Peoples' Rights' Remedies Regime in Fair Trial Cases', *African Journal of International and Comparative Law*, 28 (2020), 45–71

Police and Justice Act (United Kingdom, 2006)

Pomerantsev, Peter, 'A Cycle of Censorship: The UK White Paper on Online Harms and the Dangers of Regulating Disinformation', *Transatlantic Working Group on Content Moderation Online and Freedom of Expression*, 2019 <www.annenbergpublicpolicycenter.org/twg>

———, 'To Unreality—and Beyond', *Journal of Design and Science*, 6.1 (2019) <https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html>

Powell, G.L., 'The Council of Europe', *International Law Quarterly*, 3.2 (1950), 164–96 <https://heinonline.org/HOL/License>

Purdon, L., and F. Vera, 'Regional Cybersecurity Approaches in Africa and Latin America', in *Routledge Handbook of International Cybersecurity*, ed. by E. Tikk and M. Kerttunen (London: Routledge, 2020), pp. 234–46

Quashigah, E.K., 'The African Court of Human Rights: Prospects, in Comparison with the European

Court of Human Rights and the Inter-American Court of Human Rights', *Annual Conference - African Society of International and Comparative Law*, 1998, 59–69

Quinn, Joy Mary, 'Defining Undue Influence: A Look at the Issue and at California's Approach', *BIFOCAL: A Journal of the ABA COmmission on Law and Aging*, 35.3 (2014), 72–75

'R (on the Application of Animal Defenders International) v Secretary of State for Culture, Media and Sport', *[2008] UKHL 15 on Appeal from: [2006] EW 3069*, 2008

Redondo, Elvira Domínguez, 'The Universal Periodic Review of the UN Human Rights Council: An Assessment of the First Session', *Chinese Journal of International Law*, 7.3 (2008), 721–34

Reed, C., and A. Murray, *Rethinking the Jurisprudence of Cyberspace* (Cheltenham: Edward Elgar Publishing, 2018)

Reitano, Tuesday, Troels Oerting, and Marcena Hunter, 'Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce (J-CAT)', *The European Review of Organised Crime*, 2.2 (2015), 142–54

'Resolution Creating the Inter-American Committee against Terrorism (CICTE)', *AG/RES. 1650 (XXIX-O/99), Adopted in Guatemala City on 7 June 1999* <https://2001-2009.state.gov/p/wha/rls/fs/2006/64283.htm> [accessed 18 June 2023]

Reuters, 'Big Tech Starts Requiring Vaccines; Twitter Closes Re-Opened U.S. Offices', *Thomson Reuters*, 28 July 2021

Reviglio, U., and C. Agosti, 'Thinking Outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media', *Social Media+ Society*, 6.2 (2020), 2056305120915613

Ribeiro-Navarrete, Samuel, Jose Ramon Saura, and Daniel Palacios-Marqués, 'Towards a New Era of Mass Data Collection: Assessing Pandemic Surveillance Technologies to Preserve User Privacy', *Technological Forecasting & Social Change*, 167 (2021), 120681

'Ríos v Venezuela', *Serie C No. 194 (IACtHR)*, 2009 <https://globalfreedomofexpression.columbia.edu/cases/rios-v-venezuela/#:~:text=The>

Rodríguez-Santiago, Elizabeth, 'The Evolution of Self-Determination of Peoples in International Law', in *The Theory of Self-Determination*, ed. by F.R.. Tesón (Cambridge: Cambridge University Press, 2016), pp. 201–41

'Royal Bank of Scotland Plc v Etridge', *(No 2), [2001] UKHL 44 (Oct. 11, 2001)*

Rubinstein, Amnon, Yaniv Roznai, Roznai Yaniv, and Yaniv Roznai, *The Right to a Genuine Electoral Democracy Recommended Citation Symposium Article The Right to a Genuine Electoral Democracy*, *Genuine Electoral Democracy*, 2018, XXVII <https://scholarship.law.umn.edu/mjilhttps://scholarship.law.umn.edu/mjil/266>

'Ruling No. 2022-006119 of the Constitutional Chamber', *File No. 22-001848-0007-CO (Supreme Court of Costa Rica)*, 2022 <https://vlex.co.cr/libraries/jurisprudencia-425> [accessed 25 April 2023]

Sahadžić, Maja, 'Bosnia and Herzegovina', *The I·CONnect-Clough Center 2018 Global Review of*

Constitutional Law, 2019, 28–32

SAHRC, 'Social Media Charter', *Adopted in Gqeberha on 15 March 2023.*

Samme-Nlar, Tomslin, 'Cyberspace Security in Africa – Where Do We Stand?', *African Academic Network on Internet Policy* , 2020 <https://aanoip.org/cyberspace-security-in-africa-where-do-we-stand/> [accessed 23 June 2023]

Sanchez, Maria A., 'The African Court on Human and Peoples' Rights: Forging a Jurisdictional Frontier in Post-Colonial Human Rights', *International Journal of Law in Context*, 2023, 1–15 <https://doi.org/10.1017/s1744552323000046>

Saputra, Meidi, and Imamul Huda Al Siddiq, 'Social Media and Digital Citizenship: The Urgency of Digital Literacy in the Middle of a Disrupted Society Era', *International Journal of Emerging Technologies in Learning*, 15.7 (2020), 156–61 <https://doi.org/10.3991/IJET.V15I07.13239>

Savin, A., 'The EU Digital Services Act: Towards a More Responsible Internet', *CBS Law Research*, 2021, 21–04

Scalise, R.J., 'Undue Influence and the Law of Wills: A Comparative Analysis', *Duke Journal of Comparative International Law*, 19 (2008), 41–106

Schabas, William A., *The European Convention on Human Rights: A Commentary* (Oxford: Oxford University Press, 2015)

Schiffer, Zoë, Casey Newton, and Alex Heath, 'Tears, Blunders and Chaos: Inside Elon Musk's Twitter', *The Guardian*, 29 January 2023

Schjølberg, Stein, *ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG)* (Geneva, Switzerland, 2007) <http://www.itu.int/osg/csd/cybersecurity/gca/hleg/members.html>

Seger, Alexander, 'The Budapest Convention 10 Years on: Lessons Learnt', in *Cybercriminality: Finding a Balance between Freedom and Security*, ed. by Stefano Manacorda, Roberto. Flor, and Joon Oh. Jang (Courmayeur: ISPAC, 2012), pp. 167–78

'Sejdić and Finci v Bosnia and Herzegovina', *Application No. 34836/06 (ECtHR)*, 2009

Serious Crime Act (United Kingdom, 2015)

Seymour, Richard, 'Elon Musk Never Cared If Twitter Was a Business Failure – He Wants a Political Win', *The Guardian*, 22 November 2022

Shaffer, Gregory C., and Mark A. Pollack, 'Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance', *Minnesota Law Review*, 94.3 (2010), 706–99

Sheinin, David, *The Organization of American States* (New Brunswick: Transaction Publishers, 1995)

Shekhar, Shashi, Rohit Agrawal, and Karm Veer Arya, 'An Architectural Framework of a Crawler for Retrieving Highly Relevant Web Documents by Filtering Replicated Web Collections', in *2010 International Conference on Advances in Computer Engineering* (IEEE, 2010), pp. 29–33 <https://doi.org/10.1109/ACE.2010.64>

Shelton, Dinah, 'Soft Law', in *Routledge Handbook of International Law*, ed. by David Armstrong (New York: Routledge, 2009), pp. 68–80

Shepardson, David, and Rami Ayyub, 'TikTok Congressional Hearing: CEO Shou Zi Chew Grilled by US Lawmakers', *Reuters*, 24 March 2023 <https://www.reuters.com/technology/tiktok-ceo-face-tough-questions-support-us-ban-grows-2023-03-23/#:~:text=WASHINGTON%2C March 23 (Reuters),the app's power over Americans.> [accessed 5 May 2023]

Singer, P.W., and E.T. Brooking, *LikeWar: The Weaponization of Social Media* (Boston, MA.: Houghton Mifflin, 2018)

Siregar, Gomgom TP, and Sarman Sinaga, 'The Law Globalization in Cybercrime Prevention', *International Journal of Law Reconstruction*, 5.2 (2021), 211–27 <https://doi.org/10.26532/ijlr.v5i2.17514>

Solar, Carlos, 'Cybersecurity and Cyber Defence in the Emerging Democracies', *Journal of Cyber Policy*, 5.3 (2020), 392–412 <https://doi.org/10.1080/23738871.2020.1820546>

Somé, K.A., P.N. Forkum, A. Tanoh, M.G. Techane, S. Nabaneh, M.G. Nyarko, and others, *The Impact of the African Charter and the Maputo Protocol in Selected African States* (Pretoria: PULP, 2016)

Sonboli, Nasim, Jessie J. Smith, Florencia Cabral Berenfus, Robin Burke, and Casey Fiesler, 'Fairness and Transparency in Recommendation: The Users' Perspective', in *29th ACM Conference on User Modeling, Adaptation and Personalization*, 2021, pp. 274–79 <https://doi.org/10.1145/3450613.3456835>

Spring, Marianna, '"Stop the Steal": The Deep Roots of Trump's "voter Fraud" Strategy', *BBC News* (London, 23 November 2020) <https://www.bbc.com/news/blogs-trending-55009950> [accessed 25 July 2023]

Ssenyonjo, M., 'Responding to Human Rights Violations in Africa: Assessing the Role of the African Commission and Court on Human and Peoples' Rights (1987–2018)', *International Human Rights Law Review*, 7.1 (2018), 1–42

Stanovich, Keith E, and Richard F West, 'Evolutionary versus Instrumental Goals: How Evolutionary Psychology Misconceives Human Rationality', in *Evolution and the Psychology of Thinking*, ed. by David E. Over (Oxon: Psychology Press, 2004), pp. 176–235

STC-MAEPI, 'Agenda 2063 Progress Report', *Eco/STC/MAEPI(IV)/EXP/8, Adopted on 11 March 2020*

Steele, C., 'A Look Back at the Earliest Websites', *PC Mag*, 2014 <https://www.pcmag.com/news/a-look-back-at-the-earliest-websites>

Storey, Alice, 'Challenges and Opportunities for the United Nations' Universal Periodic Review: A Case Study on Capital Punishment in the United States', *UMKC Law Review*, 90.1 (2020), 129–52

Sunstein, Cass R., 'Is Social Media Good or Bad for Democracy?', *The SUR File on Internet and Democracy*, 15.27 (2018), 83–89

Suripeddi, Mani Karthik Suhas, and Pradnya Purandare, 'Blockchain and GDPR - A Study on

Compatibility Issues of the Distributed Ledger Technology with GDPR Data Processing', in *Journal of Physics: Conference Series* (IOP Publishing Ltd, 2021), MCMLXIV <https://doi.org/10.1088/1742-6596/1964/4/042005>

Susilo, M.E., S. Afifi, and S. Yustitia, 'Hoax as a Reflection on the Low Digital Literacy in Indonesia', in *2nd International Conference on Social, Economy, Education and Humanity*, 2019, pp. 165–74

Tambini, Damian, 'The Differentiated Duty of Care: A Response to the Online Harms White Paper', *Journal of Media Law*, 11.1 (2019), 28–40 <https://doi.org/10.1080/17577632.2019.1666488>

Tanenbaum, Andrew S., *Computer Networks* (Singapore: Pearson Education, 2013)

'Tanganyika Law Society & the Legal and Human Rights v the United Republic of Tanzania', *Application No. 009/2011 (ACJHR)*, 2011

Teevan, Chloe, and Lidet Tadesse Shiferaw, *Briefing Note No. 150: Digital Geopolitics in Africa: Moving from Strategy to Action* (Maastricht, October 2022)

Teuscher, C., *Alan Turing: Life and Legacy of a Great Thinker* (Berlin: Springer, 2013)

'The Matter of Lewis', *2018 NY Slip Op 50599(U), Sur. Ct. Kings Cty.*, 2018

'The Matter of the Probate of the WILL of Katherine WALTHER, Deceased', *159 N.E.2d 665, 6 N.Y.2d 49, 188 N.Y.S.2d 168, NY Ct. App.*, 1959

Theil, Stefan, 'The Online Harms White Paper: Comparing the UK and German Approaches to Regulation', *Journal of Media Law*, 11.1 (2019), 41–51 <http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=E23D493>

Thorbecke, Catherine, 'TikTok CEO in the Hot Seat: 5 Takeaways from His First Appearance before Congress', *CNN Business*, 23 March 2023 <https://edition.cnn.com/2023/03/23/tech/tiktok-ceo-hearing/index.html>

Trengove, Markus, Emre Kazim, Denise Almeida, Airlie Hilliard, Sara Zannone, and Elizabeth Lomas, 'A Critical Review of the Online Safety Bill', *Patterns*, 3.8 (2022), 100544 <https://doi.org/10.1016/j.patter.2022.100544>

Trivedi, Sonu, 'African Unity', *World Affairs: The Journal of International Issues*, 13.1 (2009), 12–30

Tropina, Tatiana, 'Cybercrime: Setting International Standards', in *Routledge Handbook of International Cybersecurity*, ed. by Eneken Tikk and Mika Kerttunen (Oxon: Routledge, 2020), pp. 148–60

Tufekci, Zeynep, 'How Social Media Took Us from Tahrir Square to Donald Trump', *MIT Technology Review*, 14.18 (2018), 1–12 <https://www.technologyreview.com/s/611806/how-social-media-took-us-from-tahrir-square-to-donald-trump/amp/%0Ahttps://medium.com/mit-technology-review/how-social-media-took-us-from-tahrir-square-to-donald-trump-6226231ac162>

Tully, S., ‘A Human Right to Access the Internet? Problems and Prospects’, *Human Rights Law Review*, 14.2 (2014), 175–95

U.S. Department of Justice, *Report on the Investigation into Russian Interference in the 2016 Presidential Election (Mueller Report), Government Publishing Office*, 2019

Ulu, Akturan, ‘Green Walk and Green Talk: How Oil Companies Position Themselves in Social Media’, in *9th Annual Conference of the EuroMed Academy of Business*, 2016, pp. 51–63

UN General Assembly, ‘International Covenant on Civil and Political Rights’, *2200A(XXI), Adopted 23 March 1976*

———, ‘Optional Protocol to the International Covenant on Civil and Political Rights’, *2200A(XXI), Adopted 23 March 1976* <https://www.ohchr.org/Documents/ProfessionalInterest/ccpr-one.pdf>

———, ‘Resolution on the Special Rapporteur on the Right to Freedom of Opinion and Expression’, *A/HRC/RES/43/4, Adopted 30 June 2020* <https://doi.org/10.1017/s0020818300031660>

———, ‘Universal Declaration of Human Rights’, *217 A (III), Adopted 10 December 1948*

UN Human Rights Committee, ‘General Comment No. 25 on Article 25 of the International Covenant on Civil and Political Rights, on the Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service’, *CCPR/C/21/Rev.1/Add.7, Adopted on 12 July 1996*

UNCTAD, *Harmonizing Cyberlaws and Regulations: The Experience of the East African Community* (Geneva, 2012)

Unger, Nancy, ‘That the Worst Shooting in US History Took Place in a Gay Bar Is Unsurprising’, *History News Network*, 13 June 2016 <https://www.advocate.com/politics/2022/8/16/attacks-lgbtq-community-amount-stochastic-terrorism>

UNHRC, ‘Italy Failed to Rescue More than 200 Migrants, UN Committee Finds’, *Office of the United Nations High Commissioner for Human Rights*, 2021

United Nations, *Charter of the United Nations, 1 UNTS XVI*, 1945 <https://www.un.org/en/about-us/un-charter/chapter-1>

———, ‘Member States’, *Universal Declaration of Human Rights* <https://www.un.org/en/about-us/member-states#gotoU> [accessed 22 July 2023]

———, ‘Parties to the International Covenant on Civil and Political Rights’, *Available at: Https://Treaties.Un.Org/Pages/ViewDetails.Aspx?Src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en (Accessed on 11 June 2022)*

United Nations Office on Drugs and Crime, ‘Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes’, *Meetings of the Ad Hoc Committee*, 2023 <https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home> [accessed 28 May 2023]

———, ‘Global Programme on Cybercrime ’, 2023 <https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html> [accessed

30 May 2023]

———, ‘Logistical and Procedural Information for the Holding of the Organizational Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes’, *A/AC.291/CRP.3, Adopted 12 May 2021* <https://coronavirus.health.ny.gov/covid-19-travel-advisory;>

———, ‘Promoting Technical Assistance and Capacity-Building to Strengthen National Measures and International Cooperation against Cybercrime’, *Resolution 22/8 Adopted on 10 September 2013*

———, ‘Strengthening International Cooperation to Combat Cybercrime’, *Resolution 22/7 Adopted on 10 September 2013*

———, *UNODC Strategy 2021 - 2025* (Vienna, 2021)

United Nations Treaty Collection, ‘Parties to the First Optional Protocol to the International Covenant on Civil and Political Rights’, *Available at: Https://Treaties.Un.Org/Pages/ViewDetails.Aspx?Src=IND&mtdsg_no=IV-5&chapter=4&clang=_en (Accessed on 13 June 2022)* (United Nations Treaty Collection, 2022)

Vaidhyanathan, Siva, *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy* (Oxford: Oxford University Press, 2018)

Vallée, Etienne, and Yu Chang Hsu, ‘Protecting Students: Data Privacy in the African Union’, *TechTrends*, 67 (2023), 203–6 <https://doi.org/10.1007/s11528-023-00834-0>

Vandenhole, W., G.E. Türkelli, and S. Lembrechts, *Children’s Rights: A Commentary on the Convention on the Rights of the Child and Its Protocols* (Cheltenham: Edward Elgar Publishing, 2019)

Vaqué, Luis González, ‘Directive 2005/29/EC on Unfair Commercial Practices and Its Application to Food-Related Consumer Protection’, *European Food and Feed Law Review*, 10.3 (2015), 210–22

de Varennes, Fernand, ‘The Fallacies in the Universalism Versus Cultural Relativism Debate in Human Rights Law’, *Asia-Pacific Journal on Human Rights and the Law*, 1 (2006), 67–84

Vernick, G., ‘EU Poised to Impose Sweeping Social Media Regulation with Digital Services Act’, *Reporters Committee*, 2022 <https://www.rcfp.org/eu-dsa-social-media-regulation/>

Del Vicario, Michela, Gianna Vivaldo, Alessandro Bessi, Fabiana Zollo, Antonio Scala, Guido Caldarelli, and others, ‘Echo Chambers: Emotional Contagion and Group Polarization on Facebook’, *Scientific Reports*, 6 (2016), 1–12 <https://doi.org/10.1038/srep37825>

‘Views Adopted by the Committee under Article 5(4) of the Optional Protocol, Concerning Communication No. 2059/2011’, *CCPR/C/116/D/2059/2011*

Voss, W. Gregory, ‘The Concept of Accountability in the Context of the Evolving Role of ENISA in

Data Protection, Privacy, and Cybersecurity', in *Technocracy and the Law Accountability, Governance and Expertise*, ed. by Alessandra Arcuri and Florin Coman-Kund (London: Routledge, 2021), p. 323

Wachira, G.M., and A. Ayinla, 'Twenty Years of Elusive Enforcement of the Recommendations of the African Commission on Human and Peoples' Rights: A Possible Remedy', *African Human Rights Law Journal*, 6.2 (2006), 465–92

Watson, H. J., and C. Nations, 'Addressing the Growing Need for Algorithmic Transparency', *Communications of the Association for Information Systems*, 45.1 (2019), 26

Watt, Eliza, *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law* (Cheltenham: Edward Elgar Publishing, 2021)

Wayne, Sandy J, and David Rubinstein, 'Extending Game Theoretic Propositions about Slack and Scarcity in Managerial Decision Making', *Human Relations*, 45.5 (1992), 525–36

Westbrook, Lorena, Aurel Pera, Octav Neguriță, Iulia Grecu, and Gheorghe Grecu, 'Real-Time Data-Driven Technologies: Transparency and Fairness of Automated Decision-Making Processes Governed by Intricate Algorithms', *Contemporary Readings in Law and Social Justice*, 11.1 (2019), 45–50 <https://doi.org/10.22381/CRLSJ11120197>

Wiebusch, Micha, Chika Charles Aniekwe, Lutz Oette, and Stef Vandeginste, 'The African Charter on Democracy, Elections and Governance: Past, Present and Future', *Journal of African Law*, 63.S1 (2019), 9–38 <https://doi.org/10.1017/S002185531900007X>

Wiggins, Christopher, 'Attacks on the LGBTQ+ Community Amount to Stochastic Terrorism', *Advocate*, 16 August 2022 <https://www.advocate.com/politics/2022/8/16/attacks-lgbtq-community-amount-stochastic-terrorism>

Wilton, Conrad, 'Sony, Cyber Security, and Free Speech: Preserving the First Amendment in the Modern World', *Pace Intellectual Property, Sports & Entertainment Law Forum*, 7.1 (2017), 1–43 <https://heinonline.org/HOL/License>

Winter, Stephan, Ewa Maslowska, and Anne L. Vos, 'The Effects of Trait-Based Personalization in Social Media Advertising', *Computers in Human Behavior*, 114 (2021), 106525 <https://doi.org/10.1016/j.chb.2020.106525>

Wolfson, Josiah, 'The Expanding Scope of Human Rights in a Technological World — Using the Interamerican Court of Human Rights to Establish a Minimum Data Protection Standard Across Latin America', *University of Miami Inter-American Law Review*, 48.3 (2017), 188–232 <http://repository.law.miami.edu/umialrhttp://repository.law.miami.edu/umialr/vol48/iss3/8>

Wood, Stacey, and Pi Ju Liu, 'Undue Influence and Financial Capacity: A Clinical Perspective', *Generations*, 36.2 (2012), 53–58

Woods, L., 'The Duty of Care in the Online Harms White Paper', *Journal of Media Law*, 11.1 (2019), 6–17

Woolfson, Charles, 'Working Environment and 'Soft Law'in the Post-Communist New Member

States', *Journal of Common Market Studies*, 44.1 (2006), 195–215

Wróblewski, J., 'Legal Reasoning in Legal Interpretation', *Logique et Analyse*, 12.48 (1969), 3–31

Yang, Aimei, Jieun Shin, Alvin Zhou, Ke M. Huang-Isherwood, Eugene Lee, Chuqing Dong, and others, 'The Battleground of COVID-19 Vaccine Misinformation on Facebook: Fact Checkers vs. Misinformation Spreaders', *Harvard Kennedy School Misinformation Review*, 2.4 (2021), 1–15 <https://doi.org/10.37016/mr-2020-78>

'YATAMA v Nicaragua', *Serie C No. 127 (IACtHR)*, 2005

Yerkes, Sarah, and Maha Alhomoud, 'One Year Later, Tunisia's President Has Reversed Nearly a Decade of Democratic Gains', *Carnegie Endowment for International Peace*, 2022

'Yevdokimov and Rezanov v Russian Federation', *CCPR/C/101/D/1410/2005*

Yilek, Caitlin, 'TikTok CEO Faces Intense Questioning from House Committee amid Growing Calls for Ban', *CBS News*, 23 March 2023 <https://www.cbsnews.com/news/tiktok-hearing-ceo-shou-zi-chew-house-committee-testimony/>

Yilma, Kinfe, 'African Union's Data Policy Framework and Data Protection in Africa', *Journal of Data Protection and Privacy*, 5.3 (2022), 1–7 <https://ssrn.com/abstract=4253828>

Yoon, Gunwoo, Cong Li, Yi Ji, Michael North, Cheng Hong, and Jiangmeng Liu, 'Attracting Comments: Digital Engagement Metrics on Facebook and Financial Performance', *Journal of Advertising*, 47.1 (2018), 24–37

Yuwannita, Lia, 'The Development of Law in The Digital Era Towards Globalization', in *Roceedings from the 1st International Conference on Law and Human Rights* (Jakarta, Indonesia, 2021) <https://doi.org/10.4108/eai.14-4-2021.2312312>

Zahn, Max, 'A Timeline of Elon Musk's Tumultuous Twitter Acquisition', *ABC News*, 11 November 2022

Zalnieriute, Monika, 'Reinvigorating Human Rights in Internet Governance: The UDRP Procedure through the Lens of International Human Rights Principles', *Columbia Journal of Law & Arts*, 43 (2020), 197–235 <https://heinonline.org/HOL/Page?handle=hein.journals/cjla43&id=205&div=11&collection=us journals>

'Ždanoka v Latvia', *Application No. 58278/00 (ECtHR)*, 2006

Zeng, Jing, and Crystal Abidin, '"#OkBoomer, Time to Meet the Zoomers": Studying the Memefication of Intergenerational Politics on TikTok', *Information Communication and Society*, 24.16 (2021), 2459–81 <https://doi.org/10.1080/1369118X.2021.1961007>

Zhuravskaya, E., M. Petrova, and R. Enikolopov, 'Political Effects of the Internet and Social Media.', *Annual Review of Economics*, 12 (2020), 415–38

Zlitescu, Irina Moroianu, 'Towards a Reform of the European Court of Human Rights', *Drepturile Omului*, 1 (2012), 7–12

Zuñiga, Natalia Torres, 'The Image of the Inter-American Court of Human Rights as an Agent of

Democratic Transformation: A Tool of Self-Validation', *Araucaria: Revista Iberoamericana de Filosofía, Política, Humanidades y Relaciones Internacionales*, 23.46 (2021), 483–504 <https://doi.org/10.12795/ARAUCARIA.2021.I46.24>