Research Program
on Digital Constitutionalism
Project Aristotle

South Africa

Country Report

November 2021

Authors

Anhad Kaur Mehta, NLSIU Legal Services Clinic
Anmol Kohli, NLSIU Legal Services Clinic
Kshitij Goyal, NLSIU Legal Services Clinic
Lakshmi Nambiar, NLSIU Legal Services Clinic
Sandli Pawar, NLSIU Legal Services Clinic

Institute
for Internet &
the Just Society

project
Aristotle

Research Program on Digital Constitutionalism
Project Aristotle

South Africa
Country Report

Authors
Anhad Kaur Mehta, NLSIU Legal Services Clinic
Anmol Kohli, NLSIU Legal Services Clinic
Kshitij Goyal, NLSIU Legal Services Clinic
Lakshmi Nambiar, NLSIU Legal Services Clinic
Sandli Pawar, NLSIU Legal Services Clinic

November 2021

Inquiries may be directed to digitalgovdem@internetjustsociety.org

DOI: 10.5281/zenodo.5716221

About us

The Institute for Internet & the Just Society is a think and do tank connecting civic engagement with interdisciplinary research focused on fair artificial intelligence, inclusive digital governance and human rights law in digital spheres. We collaborate and deliberate to find progressive solutions to the most pressing challenges of our digital society. We cultivate synergies by bringing the most interesting people together from all over the world and across cultural backgrounds. We empower young people to use their creativity, intelligence and voice for promoting our cause and inspiring others in their communities. We work pluralistically and independently. Pro bono.

Project Aristotle is the flagship project of the Digital Constitutionalism cycle of the Institute for Internet and the Just Society. Together with our international partners, we publish a research guide on what a structure of governance for the digital realm can look like when it is informed by interdisciplinary country-specific legal and policy research and analysis. We believe that delving deep into these bodies of knowledge, as shaped by a people within a particular national context, has much to offer in response to the pressing questions posed by the digital ecosystem.

A. Digital Constitutionalism and Internet Governance

Introducing Digital Constitutionalism

1. What factors can be considered important to ground Digital Constitutionalism in traditional constitutional concepts?

The *South African Constitution* is transformative. It goes beyond the descriptive regulation of state powers via its prescriptive restructuring of society.[1] A transformative digital Constitutionalism can be interpreted by future adjudicators for resolving new, previously-unimagined disputes. Universal adult suffrage under the *South African Constitution* translates to a representative government which considers citizens' opinions in decision-making. Therefore, those who are governed by rules of digital spaces must have a say in the framing of those rules. Digital Constitutionalism should work off its own bill of rights like the *South African Constitution*. The *Bill of Rights* applies to all 'juristic persons',[2] and so may apply to corporations and other entities. *Section 10 of the South African Constitution* ensures the right to human dignity. Digital Constitutionalism can emphasize on protecting individuals from different kinds of online harms. *Section 12* refers to the right to be protected from violence, torture, cruel/inhuman treatment, the right to bodily integrity and reproductive rights. Digital Constitutionalism should ensure that content which promotes such violations is not spread online. The third chapter of the *South African Constitution* creates "cooperative government".[3] This encourages the different spheres of federal government to cooperate in good faith and to act in the best interests of all citizens. So, grounding digital Constitutionalism in a federal structure is important. This can be achieved through a system of nested enterprises which can oversee the actions of each other through a system of checks and balances.

2. How can we define Digital Constitutionalism?

Digital Constitutionalism is an ideology that "adapts the values of contemporary Constitutionalism to the digital society."[4] It must use these existing constitutional mechanisms to address the new possibilities and threats created by the disruptive impact of digital technology in South Africa.[5] The *South African Constitution* addresses and limits private power in significant arenas. As the digital world seems to be increasingly controlled by private stakeholders, a working definition of digital Constitutionalism must address this by regulating actions of private parties while establishing their rights and freedoms.[6] Digital Constitutionalism provides answers to three new challenges of modern society: digitalization, globalization, and privatization.[7] Given that South Africa has a widespread digital divide, digital Constitutionalism must involve tools to address this digital inequality.[8]

Digital Constitution

3. What should be the core tenets of a Digital Constitution?

The first core tenet is the adoption of legal instruments to regulate parties by the discourse of digital Constitutionalism. Digital Constitutionalism need not restrict itself to the Constitution and can consider the decisions of constitutional and subordinate courts when these decisions touch on issues affecting the digital domain. It must also consider ordinary law which is established *under* the Constitution, when these ordinary laws deal with issues related to digital Constitutionalism. Further, it can employ policy instruments that may

[1] *State v Makwanyane and Another* (CCT3/94) [1995] ZACC 3 (Mahommed J).
[2] Constitution of South Africa 1996, art 8(2).
[3] Constitution of South Africa 1996, art 41.
[4] Edoardo Celeste, 'Digital constitutionalism: a new systematic theorisation' (2019) International Review of Law, Computers & Technology 1.
[5] ibid 2.
[6] Lex Gill, Dennis Redeker and Urs Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights' (2015) Berkman Center Research Publication No. 2015-15.
[7] Gunther Teubner, 'Societal Constitutionalism; Alternatives to State-Centred Constitutional Theory?' in Christian Joerges, Inger-Johanne Sand, and Gunther Teubner (eds.), *Transnational Governance and Constitutionalism. International Studies in the Theory of Private Law* (Hart 2004) 3.
[8] 'Digital Divide in South Africa' (*Huge Connect*, 4 February 2021) <https://hugeconnect.co.za/digital-divide-in-south-africa/> accessed 16 April 2021.

also lie outside the legal enterprise. For example, digital Constitutionalism can study how nudges in digital policy design affect the behaviour of both digital intermediaries and netizens. Another core tenet of digital Constitutionalism may involve incorporation of the *Internet Bill of Rights* and other such instruments in South African constitutional and ordinary law. These instruments are a set of norms concerning the fundamental rights of citizens and private parties.[9] They limit potential rights violations and balance the powers that operate in the digital domain.[10] International internet bills of rights like the *Internet Constitution*[11] and *Rep. Ro Khanna's Internet Bill of Rights*[12] must be used to critique domestic internet governance laws.

Digital Constitutionalism must ensure that the domestic law of South Africa can regulate the present and upcoming advancements in the digital world. It can be argued that the current ordinary laws of South Africa are not cut out for this task. South Africa has recognised electronic communication as a legally valid and recognisable form of communication for a few decades now under the *Electronic Communications and Transactions Act, 2002*. A newer development in the sphere of data collection and privacy has been the *Protection of Personal Information Act (POPIA).* This statute provides valid and invalid circumstances for the collection, processing, storage, and re-usage of personal data of netizens by private companies and public governmental bodies. The *POPIA* is lacking in many aspects, and cannot sufficiently address the data collection and privacy practices of today.[13] It identifies individual-based privacy issues which fail to address the collection of aggregated information by big data companies.

4. How can Digital Constitutionalism present a constitutional model for the people, by the people, and of the people?

Digital Constitutionalism must broadly follow the domestic principles of constitutional law in South Africa. The *South African Constitution* creates a democracy with universal adult franchise.[14] Digital Constitutionalism can adopt similar practices in the development of digital constitutional discourse and the framing of digital policies. Democratic digital Constitutionalism should be iterative and consultative in nature. Freedoms in the digital sphere must include the right to visit whatever website a netizen wishes, and to make any comments that the netizen may wish to make. These freedoms may be limited only when it causes harm to other netizens, and not when government bodies dislike particular content. The difference between morally offensive speech and hate speech must be applied to digital Constitutionalism. While hate speech may be prohibited, morally offensive speech must be tolerated.

Representativeness of Online Platforms

5. How can online platforms be made more inclusive, representative, and equal?

South Africa is a multi-cultural and multi-ethnic society. In the online sphere, there is a huge digital divide, further deepened due to the gap between the rich and the poor and lack of resources with vulnerable groups like women, tribal and indigenous communities like Xun, Khwe amongst others.[15] A number of social concerns have also impeded an inclusive and representative online sphere. As the telecommunication market is mainly run by the private sector, it has led to technological advancement at the cost of widening the gap between the haves and have nots.[16] In the absence of stringent regulatory mechanisms and a nascent legislation for data protection (the *Protection of Personal Information Act or POPIA*), the privacy of citizens is also threatened

[9] ibid.

[10] 'The 10 Internet Rights & Principles' (*Internet Rights and Principles Coalition*) <https://internetrightsandprinciples.org/campaign> accessed 16 April 2021.

[11] 'Internet Constitution' (*Internet Bill of Rights*) <https://billofrights.world/w/Internet_Constitution> accessed 3 July 2021.

[12] 'Internet Bill of Rights (*Ro Khanna: Democrat for Congress*) <https://www.rokhanna.com/issues/internet-bill-rights> accessed 3 July 2021.

[13] Jared Nickig, 'SA needs new laws for the digital world' (*I0L*, 22 May 2017) <https://www.iol.co.za/business-report/sa-needs-new-laws-for-the-digital-world-9275092> accessed 16 April 2021.

[14] Constitution of South Africa 1996, art 1(d).

[15] Manda and Backhouse, 'Inclusive digital transformation in South Africa: an institutional perspective' (2018) ICEGOV'18 464, 465-467

[16] ibid.

in the online sphere.[17] It is also necessary for the online sphere to have content in different languages to widen the access to these platforms.[18] In this context, the South African Government has enacted several policies and introduced initiatives like South Africa Connect to facilitate digital access and inclusivity.[19] ICT policies also focus on digital literacy, e-skilling and targeted solutions for different marginalised communities.[20] Moreover, the government also initiated a Broadcast Migration policy to make the set-top boxes cheaper for the poor citizens.[21] However, these policies have been unable to make substantial transformation in the digital sphere or resolve inequities. There are issues of policy inertia, infighting among government departments and failures in coordination.[22] This has impacted public trust in the capacity of the government.[23] There is a need for proper execution of government policies to regain the public's trust. Supervisory authorities must act as a check against inordinate delays. Lastly, structural problems like poverty and patriarchal institutions must be resolved.

Open Source Intelligence

6. What role should open-source intelligence (=OSINT: the discipline of assembling and analyzing publicly available information) play in the future of our society?

OSINT comprise analyses of publicly available information for different purposes, be it governance or national security.[24] South Africa has not conducted specific research on OSINT. However, it released a White Paper on National Security which briefly touched upon the importance of OSINT for development.[25] It can be inferred that open-source intelligence will have two benefits — lower cost and better access.[26] In South Africa, OSINT will ensure a democratised process of free-flow of information, wherein it becomes a communally owned resource.[27] Apart from increasing access, the cost of this information will also come down, furthering R&D.[28] OSINT can also aid the state in monitoring conflicts[29] — thus preventing skirmishes among different communities from escalating into violent conflicts, thereby advancing peace, prosperity and development.[30] However, certain problems with OSINT may crop up. There could be privacy violations, if there is insufficient anonymization of data;[31] and rapid spread of false news when intelligence is not verified.[32] It is important to have regulatory mechanisms in place to counter this.

---

[17] ibid.
[18] ibid.
[19] 'South Africa Connect: Creating Opportunities, Ensuring Inclusion' (2013) South Africa's Broadband Policy, Government of South Africa. Accessed 10 March, 2021.
[20] 'Integrated ICT Policy Framework' Department of Telecommunications and Postal Services, Government of South Africa (2016). <https://www.gov.za/documents/electronic-communications-act-national-integrated-ict-policy-white-paper-3-oct-2016-0000> Accessed 15 March, 2021.
[21] Broadcasting Digital Migration, Government Programme, Government of South Africa <https://www.gov.za/about-government/government-programmes/digital-migration> Accessed 20 March, 2021
[22] Naidoo, 'Implementation of E-government in South Africa– successes and challenges: the way forward' (2012) 1(1) International Journal of Advances in Computing and Management, 62.
[23] Manda (n 15), 468-469
[24] Bianna E, 'Hidden in Plain Sight: The Ever-Increasing Use of Open-Source Intelligence' (2011) 29(2) American Intelligence Journal, 141.
[25] Government of South Africa, Intelligence White Paper (1995) <https://www.gov.za/documents/intelligence-white-paper>
[26] Bianna E (n 24)
[27] Michael Kwet, 'A Digital Tech New Deal to break up Big Tech' Al Jazeera (26 Oct 2020) <https://www.aljazeera.com/opinions/2020/10/26/a-digital-tech-new-deal-to-break-up-big-tech> Accessed 10 March, 2021.
[28] Bianna E (n 24)
[29] Senekal and Kotzé, 'Open-source intelligence (OSINT) for conflict monitoring in contemporary South Africa: Challenges and opportunities in a big data context' (2019) 28 African Security Review 19 https://doi.org/10.1080/10246029.2019.1644357.
[30] ibid; Government (n 25)
[31] Government Gazette 43164, GN 417, 26 March 2020 <https://www.gov.za/sites/default/files/gcis_document/202003/43164gon-417.pdf>
[32] 'South Africa brings law into place to stop the spread of fake COVID-19 news' Computer Security Incident Response Team, University of Cape Town <https://csirt.uct.ac.za/south-africa-brings-law-place-stop-spread-fake-covid-19-news> Accessed 20 March, 2021.

7. Should the Digital Constitution be an integrative model, which draws upon and comprehensively presents standards for specific laws (e.g. antitrust, evidentiary standards etc.) as opposed to grounding ideals? If so, how should it fulfil the responsibilities of a pluralistic enterprise such as this as well as the specific needs of a pluralistic global society?

A digital Constitution should reflect the ideals of equality, non-discrimination and welfare of citizens. It should foster the development and well-being of all, irrespective of the community they belong to.[33] It should also limit the powers of the state and governance norms for the digital society.[34] A pluralistic global society acknowledges diversity and the presence of different states.[35] In South Africa, one finds the presence of different tribes and communities,[36] so a pluralistic global society must cater to the interests of these different stakeholders. An *Internet Charter of Rights*, stipulates substantive rights for citizens and acknowledges the needs of disabled, indigenous communities, illiterate and minority language speakers. [37] The *African Declaration on Internet Rights and Freedoms* has a section dedicated to marginalised communities.[38] Standards must accompany these rights for better enforcement, and prevention of abuse by the government or elites. Thresholds, like evidentiary standards or regulations, if drafted like rules would give a precise picture of the procedure to be followed for enforcement of that right and method of recourse.[39] Grounding ideals in the absence of the procedure to be followed will be difficult to enforce, especially in developing countries wherein the State plays a central role in implementing laws and dictating the public sphere. Thus, an integrative model is better suited to enforce the digital Constitution in letter and spirit.

Competition Law and the Internet

8. How can competition and antitrust laws of different jurisdictions protect the global market from big-tech domination, and is there a need to?

Big Tech companies have built up a significant consumer base in developing countries.[40] Due to upfront costs in the digital market, 'first mover advantage' and network externalities smaller firms have found it difficult to survive.[41] South African citizens are also dependent on these companies for their products and services.[42] This indicates a worrying trend of big companies generating huge profits at the cost of competition and public welfare in South Africa. Additionally, Big Tech corporations have centralised digital infrastructure and knowledge. Thus, privately-ownership of these resources due to IPRs than a communally-owned ecosystem, impedes access of digital infrastructure to smaller firms. They have to pay high costs to utilize the same.[43] Furthermore, there are concerns of abuse of personal data and invasion of citizens' privacy by these companies.[44] The current competition law in South Africa, fails to adequately resolve these concerns. *Section 8 of the Act* stipulates abuse of dominant position through measures like predatory pricing etc.[45] However, the

[33] Gill, Lex, Redeker, and Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights' (2015) Berkman Klein Center for Internet & Society Research, Publication 2015-15.

[34] ibid

[35] 'Defining Pluralism' (Jan 2012) Global Centre for Pluralism, Centre Mondial Du Pluralisme, Pluralism Papers, 1, chap 1, 1. <https://www.pluralism.ca/wp-content/uploads/2017/10/defining_pluralism_EN.pdf> Accessed 30 March, 2021.

[36] 'South Africa's Diverse Culture Artistic and Linguistic Heritage' South African History Online <https://www.sahistory.org.za/article/south-africas-diverse-culture-artistic-and-linguistic-heritage> Accessed 26 March, 2021

[37] 'APC Internet Rights Charter: Internet for Social Justice and Sustainable Development' (2011) Association for Progressive Communications <https://www.apc.org/en/pubs/about-apc/apc-internet-rights-charter-download> Accessed 30 March, 2021.

[38] 'African Declaration on Internet Rights and Freedoms', African Declaration Coalition <http://africaninternetrights.org/declaration> Accessed 31 March, 2021.

[39] Schaefer, Rowley., Schneider, 'Legal Rules and Standards' The Encyclopedia of Public Choice (Springer, Boston, MA (2004) 347-348. https://doi.org/10.1007/978-0-306-47828-4_132.

[40] Kwet (n 27).

[41] Heimler and Mehta, 'Monopolization in Developing Countries' (2015) 2 The Oxford Handbook of Antitrust Economics 237; Ademuyiwa and Adeniran, 'Assessing Digitalization and Data Governance Issues in Africa' (Centre for International Governance Innovation, 2020) 8.

[42] Kwet (n 27)

[43] Michael Kwet, 'People's Tech for People's Power: A guide to digital empowerment and self-defense'(Aug 2020) Right2Know Campaign, Chap 19, 63-65 <https://www.r2k.org.za/wp-content/uploads/Peoples-Tech_August-2020.pdf> Accessed 26 March, 2021.

[44] ibid.

[45] Competition Act (Act 89 of the 1998), s. 8(d)(iv).

same can be condoned if pro-competitive effects are proven.[46] The *Competition Act* also does not resolve the issue of network effects,[47] or abuse of personal data. Even if their dominance is proven and the market is opened for different firms, companies from developed countries with adequate resources can control the market, thus resembling an anti-competitive oligopoly.[48]

Certain solutions may help counter the above issues. The *Competition Act* should be amended to include provisions dealing with network effects. The government should provide smaller firms adequate resources and digital infrastructure to advance competition. Competition enhancing commitments from these companies should be obtained and their activities should be supervised.[49] The Competition Commission and the *POPIA* regulator should also coordinate with each other to address abuse of personal data of citizens.[50] Lastly, the country should aim towards digital socialism.[51] Thus, South Africa could counter Big Tech dominance in the country.

The Regional, Constitutional and Transnational Aspects of a Digital Constitution

9. What is the role of regional/grassroots actors as well as inter-judicial cooperation/coordination in the digital ecosystem? Which other mechanism(s) might be more helpful?

In the digital ecosystem, civil society organizations, judicial actors, regional organizations and social media play a key role in governance. Different platforms like Open Net Africa have highlighted the digital divide in the country and lack of internet access in many regions.[52] Moreover, it has also been instrumental in highlighting online censorship and the absence of internet freedoms.[53] The Association for Progressive Communications has put forth a seven step plan for resolving this issue including initiatives pertaining to — "public access at government sites, free of cost; free public Wi-Fi; free basic internet; zero rated access to government websites and data; digital literacy programs; oversight and monitoring of the progressive realization of free access and minimum protections in the provision of free access."[54] Hence, different grassroots actors have brought to light the digital divide in South Africa. However, they have been suppressed by the state, through censorship and deprivation of adequate funding.[55] Regional organizations like the Southern Africa Development Community, of which South Africa is a member, have also proposed various policies for ensuring equitable distribution of digital resources.[56] Furthermore, regional multilateral organizations like the African Union have also stipulated the need for data protection and regulation in African countries, while organizations like the African Competition Forum have initiated measures to protect citizens from market dominance by big firms.[57] With regards to the Constitutional Court of South Africa, in a recent judgement, it held that state surveillance cannot violate the privacy of individuals — a constitutional right.[58]

---

[46] ibid.
[47] Ademuyiwa (n 41)
[48] ibid; Kwet (n 27)
[49] Ademuyiwa (n 41)
[50] Koornhof and Pistorius, 'Convergence between competition and data protection law: a South African perspective' (2018) 8(3) IDPL 277.
[51] Kwet (n 43) Digital socialism is an idea of digital resources being owned by the community at large.
[52] 'State of Internet Freedoms in South Africa: An Investigation Into The Policies And Practices Defining Internet Freedom in South Africa' (2014) OpenNet Africa and CIPESA, 14-15 <https://cipesa.org/?wpfb_dl=107> Accessed 23 March, 2021.
[53] Ibid.
[54] Universal Access to the Internet and Free Public Access In South Africa: A seven-point implementation Plan (Sept 2019) <https://internetaccess.africa/wp-content/uploads/2019/10/UA-Report.pdf> Accessed 15 March, 2021.
[55] William Gumede, '25 years later, South African civil society still battling government in people's interests' Civicus (3 Oct 2018) <https://www.civicus.org/index.php/media-resources/news/civicus-at-25/3531-25-years-later-south-african-civil-society-still-battling-government-in-people-s-interests> Accessed 29 March, 2021.
[56] 'Declaration on Information and Communications Technology'(2001) Southern Africa Development Community <https://www.sadc.int/files/7813/5292/8380/Declaration_on_Information_and_Communication_Technology2001.pdf> Accessed 27 March, 2021.
[57] African Union, Convention on Cyber Security and Personal Data Protection (Convention) 2014; Ademuyiwa (n 41)
[58] AmaBhungane Centre for Investigative Journalism NPC & Anr. v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC & Ors. [2021] ZACC 3.

Finally, social media provides agency, and opportunities for dialogue to the South African people.[59] Cumulatively, these actors will help the South African digital ecosystem to be inclusive and representative.

10. Can the Digital Constitution present an anchor for the governance of the virtual world similar to a traditional constitutional model or will it always be in flux? Is there a need for constitutional innovation, and if so, in which areas (e.g. the right to be forgotten as a novel right)?

The traditional concept of Constitutionalism has never been static.[60] When these values are reconfigured in the digital space, which is inherently dynamic, changes must be expected. A digital Constitution must not be inflexible to the proliferation of emerging technologies as it would become obsolete otherwise.[61] Extraterritorial application is required as the international network increases threats to rights and freedoms beyond territorial borders.[62] However, consensus is difficult to achieve unless substantial freedom is given to the nations for designing their country-specific provisions. For instance, recently the UN's efforts for protection of internet freedom was voted against by South Africa, amongst other countries.[63] This could also limit the application and affect the static nature of the digital Constitution.

The collection and processing of data by the government raises concerns for privacy and state surveillance. For instance, Johannesburg recently upgraded to a CCTV system to allow for facial recognition and effective collaboration with police forces which could be used against minorities.[64] This is against the traditional constitutional spirit of South Africa. The technical jargon makes it difficult to exercise rights which further impacts the governance of online platforms.[65] After the recognition of the right to be forgotten, online platforms are required to take down information about an individual in case the privacy rights outweigh the public interest served by the information.[66] Similarly, in the model of digital Constitutionalism, innovation occurs, as it seeks to control and limit the powers of private actors such as intermediaries, MNCs etc. This is a constitutional innovation because the concept of Constitutionalism was initially aimed towards limiting the government or the sovereign's powers.

The advancement in the digital era has also led to the recognition of digital citizenship, various digital ethics and digital rights.[67] However, the regulatory uncertainties are yielding huge scope for digital innovation. One such area is competition, which provides immense opportunities for innovation.[68] Fair competition must be ensured by considering net neutrality, transparency, decentralisation, infrastructure and consumer rights.[69] Digital models of governance must move beyond traditional models in order to account for these changes.

---

[59] Oginni and Moitui, 'Social Media and Public Policy Process in Africa: Enhanced Policy Process in the Digital Age'(2015) 14 Consilience , 158.

[60] ibid.

[61] Kenny MacIver & Rae Ritchie. 'The importance of developing a digital constitution' (*Fujitsu*, November 2019) <https://www.i-cio.com/big-thinkers/andreas-ekstroem/item/the-importance-of-developing-a-digital-constitution> accessed March 28, 2021.

[62] Fabbrini F and Celeste E, 'The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection beyond Borders' (2020) 21 German Law Journal 55 <https://www.cambridge.org/core/journals/german-law-journal/article/right-to-be-forgotten-in-the-digital-age-the-challenges-of-data-protection-beyond-borders/3E3E182352F1AD555CBB788E2380E23F>.accessed March 25, 2021.

[63] Misha Ketchell, 'South Africa's vote against internet freedom tarnishes its global image' (*The Conversation* 15 July 2016) <https://theconversation.com/south-africas-vote-against-internet-freedom-tarnishes-its-global-image-62112> accessed March 27, 2021.

[64] Heidi Swart, 'Joburg's new hi-tech cameras surveillance cameras: A threat to minorities that could see the law targeting thousands of innocents' (*Daily Maverick* 28 September 2018) <https://www.dailymaverick.co.za/article/2018-09-28-joburgs-new-hi-tech-surveillance-cameras-a-threat-to-minorities-that-could-see-the-law-targeting-thousands-of-innocents/> accessed March 29, 2021.

[65] Association for Progressive Communications, *Global Information Society Watch 2019*, (2019) <https://giswatch.org/sites/default/files/gisw2019_artificial_intelligence.pdf> accessed March 28, 2021.

[66] Avani Singh, 'Do South Africans have a right to be forgotten? European court says not yet.' (*Altadvisory* 15 October 2019) <https://altadvisory.africa/2019/10/15/do-south-africans-have-a-right-to-be-forgotten-european-court-says-not-yet/> accessed 28 March 2021.

[67] 'Digital Rights, essential in the Internet Age' <https://www.iberdrola.com/innovation/what-are-digital-rights> accessed 27 March 2021.

[68] OECD, 'Key Issues for Digital Transformation in the G20' (G20 German Presidency Report, 12 January 2017). <https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf> accessed 04 July 2021.

[69] Paula Forteza, 'A constitution for the digital era: why it's time to reboot democracy' (*Apolitical*, 21 November 2018) <https://apolitical.co/solution-zs/en/constitution-digital-era-reboot> accessed 03 July 2021.

11. How is it possible to harmonise diverse national frameworks in order to achieve a global Digital Constitution?

One of the fundamental challenges to the recognition of the global digital Constitution is the accommodation of the envisaged rights and duties across different countries and cultures.[70] At the ideological level, the African countries were able to reconcile Global Constitutionalism *vis-a-vis* cultural diversity through the operation of jurisgenerative Constitutionalism, i.e. by accommodating the plural voices within the constitutional text.[71] As per the model of jurisgenerative Constitutionalism, it is the interaction, instead of singularity, of these systems in time and place that determine the prevalent constitutional practice or outcome. This approach is reflected in the South African Constitution wherein it recognizes the right to culture reconciled with equality, dignity and democracy.[72] For instance, it recognizes Islamic and customary laws, and liberal notions of women rights simultaneously. The former are not held unconstitutional as long as they can be assimilated in the liberal tenets of the Constitution.[73]

For the harmonisation at the technological and implementational level, nations could come together to pool ideas and exchange human resources to set up various processes, structures and algorithms to protect citizens' rights. This would require collaboration from specialists, and engaging these professionals from different nations would allow for diverse ideas.[74] For example, the African Union is trying to harmonize various global, national and sub-national regulations regarding the issues of Artificial Intelligence at a policy level.[75] Despite this, the nations are free to pursue the interpretations and the legal framework around these policies governing transparency and accountability. In response to this, the South African government has established a regulatory body under *POPIA*, to design and promote better data and AI governance in the country.[76]

B. Human and Constitutionally Guaranteed Rights

Internet Users and Online Platforms

1. Which human and constitutionally guaranteed rights do online platforms affect, and how?

As a member of the United Nations, South Africa must inspire its human rights jurisprudence from the *Universal Declaration of Human Rights*.[77] *Article 7 of the UDHR*, similar to *Article 9(1) of the South African Constitution* mandates equality before the law and equal protection against discrimination.[78] Online platforms affect this right in their discrimination and content removal policies. It must be ensured that these policies uniformly moderate all content and do not arbitrarily remove harmless content while retaining harmful content. *Article 10*, mandating a fair and public hearing is also relevant. Online platforms must ensure that individuals whose content gets removed are given a chance to be heard. *Article 12 of the UDHR* and *Article 14 of the Constitution* specifies that no individual may be subjected to arbitrary interference with their privacy.[79] Privacy violations may result where online platforms do not specify the user information they are accessing via their terms and conditions. Further, the *POPIA* requires intermediaries to comply with law enforcement authorities in supplying personal details of data subjects, which may contradict privacy rights.

Article 17 of the UDHR and *Article 25 of the Constitution* provide for the right to property and prohibit arbitrary deprival of property. This may apply in the context of data uploaded by users on online platforms.

---

[70] ibid.

[71] Evadne Grant, 'Human Rights, Cultural Diversity and Customary Law in South Africa' (2006) 50 Journal of African Law 2 <https://www.cambridge.org/core/journals/journal-of-african-law/article/abs/human-rights-cultural-diversity-and-customary-law-in-south-africa/13FA3709962BDA73CED97592932F0FA0> accessed 28 March 2021.

[72] ibid.

[73] Berihun Adugna Gebeye, 'A Theory of African Constitutionalism' (OUP, 2021).

74 SM Shakhrai, 'Digital Constitution: Fundamental Rights and Freedoms of an individual in a Totally Informational Society' (2018) 88(6) Herald of Russian Academy of Sciences 441-447 <https://link.springer.com/article/10.1134/S1019331618060126> accessed 28 March 2021.

75 François Candelon, 'Developing an Artificial Intelligence for Africa strategy' (OECD Development Matters, 9th February 2021) <https://oecd-development-matters.org/2021/02/09/developing-an-artificial-intelligence-for-africa-strategy/> accessed on 28 March 2021.

76 APC (n 65).

77 Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR).

78 Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 7.

79 Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 12.

Individuals must be notified if their uploaded data is being taken down by an online platform. *Article 19* provides the right to freedom of opinion and expression. Online platforms have the power to restrict speech on various grounds by censoring user content. The *Constitution* has a positive right to privacy as well as a negative right against arbitrary deprivation of privacy. *Article 14(b) of the Constitution* provides that everyone has a right not to have their property searched. *Article 14(d)* provides the same for their communications. This can arguably be applied to the context of online platforms that affect privacy. However, the *UDHR* in *Article 17* adopts a wider definition of property rights than the *South African Constitution.*

2. Who can be defined as a netizen?

A netizen is "an active participant in the online community of the internet".[80] In South Africa, netizens have generated discourse against internet censorship and argued that governmental freedom in this aspect would lead to arbitrary removal of content. However, most laws regulating the internet are made entirely by governmental bodies without any public consultation. One way to develop the active participation of internet users who wish to be netizens is to promote public consultation before the passage of laws that affect internet usage. For example, the *POPIA* outlines various exceptions to data subject rights.[81] These are situations where the consent of the user is not required for processing their personal information. Netizens should have been consulted for these exceptions to understand whether they are required for the protection and development of cyberspace.

3. Who can be classified as a 'bad actor', and can 'bad actors' be netizens?

In the context of the digital sphere, a 'bad actor' would be an individual that creates a negative effect on the internet by their presence on the same.[82] South Africa is generally a country with low internet censorship, though this has been changing recently with an increase in political censorship to protect corrupt officials, according to the Freedom in the World Index 2021[83] .The Constitutional Court of the country has held that pre-screening internet content under the *Films and Publications Act 1996* would violate the freedom of expression under the Constitution. Therefore, an individual using their freedom of expression within the limits prescribed under the Constitution cannot be a 'bad actor'. Further, this legislation also applies to uploaders of child pornography and other illegal content.

Safeguarding the Digital Ecosystem: Minority Rights Protection and Consent

4. How can we embed within the digital ecosystem approaches which are responsive to the needs of minorities (e.g. ethnic minorities, racial minorities, gender minorities, religious minorities)?

Digital transformation must work hand-in-hand with inclusive growth. South Africa is trying to promote inclusion and digital access in an integrated approach.[84] In South Africa, the three key factors determining access to the internet apart from age and location are race, gender and income.[85] As a response to this, the government is promoting the development of information and communication technology based on three pillars: (i) digital transformation, (ii) digital inclusion, and (iii) digital access.[86] These three pillars have been furthered in the National Development Plan which seeks to ensure greater inclusivity in ICT by 2030.[87] Digital inclusion is concerned about the mitigation of the problems of digital literacy and the digital divide and therefore comprises policies for the promotion of access to ICT to all, including persons with special needs,

[80]'Netizen' (Merriam-Webster) <https://www.merriam-webster.com/dictionary/netizen> accessed 16 April 2021.
[81]Preeta Bhagattjee, 'South Africa – Data Protection Overview' (*Data Guidance*, July 2020) <https://www.dataguidance.com/notes/south-africa-data-protection-overview> accessed 16 April 2021.
[82]Amelia DeLoach, 'What is a Netizen?' (*CMC Magazine*, September 1996) <https://www.december.com/cmc/mag/1996/sep/netizen.html> accessed 16 April 2021.
[83]'Freedom in the World 2021 – South Africa' (*Freedom House*) <https://freedomhouse.org/country/south-africa/freedom-world/2021> accessed 16 April 2021.
[84] Manda (n 15).
[85] Manda (n 15).
[86] Manda (n 15).
[87] Manda (n 15).

women, children etc.[88] Two important means to achieve digital inclusion, which has also been deployed by South Africa, are (i) Telecommunications technologies (ii), and E-readiness or E-literacy. The factors acting as constraints in Telecommunication technologies are — affordability, infrastructure, regulation and perceived values.[89] South Africa has deployed techniques such as investment in technological infrastructure as well as social infrastructure, and the introduction of the SA Connect Project, which aims to provide 100% connectivity by 2030 to all citizens.[90] The South African government has implemented programmes such as Ikamva National e-skills Institute to promote e-readiness and e-skilling.[91] However, similar to other African states, South Africa has not explicitly addressed the gender digital divide.[92] In the early phases of the pandemic, the South African government was more responsive in promoting continued digital access than other African countries.[93] As a result of directions issued, the Independent Communications Authority of South Africa (ICASA) allocated temporary spectrum to major mobile networks and prohibited licensed entities from increasing the price.

5. How should the digital age of consent be arrived at and what should it be? In pursuance of which child rights should such an age be identified?

The digital space could pose various risks to the children such as exposure to upsetting content or harmful individuals, or irresponsible behaviour online.[94] Policymakers must discuss and deliberate to ensure safe, diverse and inclusive access to technology as well as an equitable and protective digital space.[95]

The General Comment 25 on the rights of children regarding the digital environment was adopted by the UN Committee in February 2021. This is relevant to contexts such as South Africa, where a significant population of children are unable to enjoy their digital rights. For instance, in the first wave of COVID-19, around 13 million children in South Africa were unable to access adequate forms of schooling due to digital divide in the education system.[96] Though the legislative framework of South Africa contains multiple laws and policies in relation to the rights of children, very few have directly addressed digital rights. *Chapter 2 of the South African Constitution*, the *Bill of Rights*, addresses children's rights and states that they have the same constitutional rights as adults. It also enshrines the right to privacy, however, since the document was drafted in the early days of the internet, it has little relevance to the digital rights of children. The *Children's Act 2005* identifies and provides legal definitions of abuse. It includes harms that are perpetrated online, however, the *Act* does not mention this. Recently, the Department of Telecommunications and Postal Service has launched the Children and ICTs Strategy. This strategy adopts a rights-based approach to promote internet access among vulnerable groups, however, the results of the same are unknown yet. There are other penal legislations, such as *The Protection from Harassment Act of 2011*, to deal with potential crimes and abuses done via the internet. Despite multiple laws, the overall framework is not very comprehensive and coherent. There is a need for reform to effectively manage online victimization and to uphold the digital rights of children.[97]

The concept of the 'digital age of consent' has been recently brought into light by the *General Data*

[88] Vidisha Mishra, 'Empowering women in a digital age in South Africa' (*Observer Research Foundation*, 12 July 2017) <https://www.orfonline.org/research/digital-age-south-africa-empowerment-women/> accessed 28 March 2021.
[89] Manda (n 15).
[90] Manda (n 15).
[91] Manda (n 15).
[92] 'The impact of COVID19 on digital rights in South Africa' (African Declaration on Internet Rights and Freedoms, November 2020) <https://www.apc.org/sites/default/files/impactCOVID-19-Africa.pdf> accessed 29 March 2021.
[93] ibid.
[94] Burton, P., Leoschut, L. & Phyfer, J *South African Kids Online: A glimpse into children's internet use and online activities* (Centre for Justice and Crime Prevention, 2016) <http://www.cjcp.org.za/uploads/2/7/8/4/27845461/south_africa_kids_online_full_report.pdf> accessed 28 March 2021.
[95] Anri Van Der Spuy, 'South Africa: How do we protect children's rights in a digital environment only available to some' (*Africa Portal*, 23 February 2021) <https://www.africaportal.org/features/south-africa-how-do-we-protect-childrens-rights-in-a-digital-environment-only-available-to-some/> accessed 29 March 2021.
[96] ibid.
[97] Burton (n 94).

Protection Regulations (GDPR).[98] It defines consent as "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes...signifies agreement to the processing of personal data relating to him or her."[99] As a step to ensure protection to young people, it has mandated parental consent for processing the data of children below 16 years. Countries around the globe have the legal age of consent between 14 and 18 years, therefore, fixing the age within this range would align with other national laws too.[100] The age restrictions must primarily be guided by the children's right to privacy on the internet. Ensuring child privacy in the digital space has a positive impact on the enjoyment of other rights on the internet.[101] Arriving at an age of digital consent based on this right would prevent data collection without informed consent based on an accessible, clear and unambiguous statement. It would also discourage monitoring activities undertaken without explicit consent from either children or parents in case the children are not yet capable of consenting.[102]

Public Order

6. How should public order be defined for the digital space? Should situations of disorder in the offline world influence the definition and management of public order online, and if so why and when?

There is little mention on public order and disorder in the digital space in South African legislation, reports and civil society. There is no discussion in South African law, executive reports or speeches by government/political officials regarding public order or disorder online. There is little on the same by civil society groups as well. Even the Annual Report by the South African Police Service makes no report to online incidents that the Public Order Police Unit worked on.[103]

A report by the African Policing Civilian Oversight Forum sheds some light on this issue. The report mentioned that an SAPS official said that social media can fuel violence[104] — referring to the fact that the online world can affect the offline. Further, the report also highlighted the fact that the provisions which give the police the power to use force does not consider the use of online force.[105]

Therefore, this is an area of policy and regulation that remains yet to be covered by South African legislation. It is clear that there is a need to do so, given that disorder in the offline world influences the online world and vice-versa. However, this has not yet been acknowledged and recognised explicitly by South Africa.

7. Should the state be allowed to impose internet shutdowns, slowdowns and communication throttles? What socio-legal rationale could be adopted by states in order to do so?

The 2020 Freedom on the Net report by Freedom House has classified South Africa as a free country with respect to internet freedom.[106] The report states that no reported instances of blocking, filtering or restrictions on the use of social media or online mobilization took place in the country. There was a reported instance of slowdown in early 2020, however this was a consequence of malfunctions in undersea cables and not a government-imposed slowdown. There is no evidence to show that the government exercises any control

[98] Ashin Perumall, 'South Africa: COVID-19-Digital Marketing to children in the age of social distancing' (*BackerMcKenzie* 07 May 2020). <https://insightplus.bakermckenzie.com/bm/data-technology/south-africa-covid-19-digital-marketing-to-children-in-the-age-of-social-distancing> accessed 27 March 2021.

[99] Article 4(11), General Data Protection Regulation.

[100] 'Digital Consent around the world' (Global Data Hub, September, 2019) <https://globaldatahub.taylorwessing.com/article/digital-consent-around-the-world> accessed March 29, 2021.

[101] UNICEF, 'Child Privacy in the Age of Web 2.0 and 3.0: Challenges and opportunities for policy' Innocenti Discussion Paper No. 03 (2017) <https://www.unicef-irc.org/publications/pdf/Child_privacy_ challenges _opportunities.pdf> accessed 28 March 2021.

[102] Child Rights International Network, 'Children's rights in the digital age' (*CRIN Briefing)* <https://home.crin.org/issues/digital-rights/childrens-right-digital-age> accessed 29 March 2021.

[103] South African Police Service, 'Submission of the Annual Report to the Minister of Police' (SAPS 2019) 151; South African Police Service, 'Submission of the Annual Report to the Minister of Police' (SAPS 2020).

[104] 'Dialogue on Public Order Policing in South Africa' (African Policing Civilian Oversight Forum 2017) <http://apcof.org/wp-content/uploads/dialogue-on-public-order-policing-in-south-africa-11-12-july-2017-johannesburg.pdf> accessed 9 April 2021.

[105] ibid 16.

[106] 'Freedom on the Net 2020: South Africa' (Freedom House 2020) <https://freedomhouse.org/country/south-africa/freedom-net/2020> accessed 21 March 2020.

over infrastructure for ISPs in South Africa and there have been no intentional disruptions to connectivity. The government does not have direct control over the country's internet backbone or connection to international internet.[107]

The Independent Communications Authority of South Africa, which is the regulatory body, has its independence and autonomy protected under the Constitution.[108] However, there has been a perception that there is some amount of political interference and membership on the board. This has led to a view that there is no comprehensive approach to regulation of ICTs.[109] There is no blocking or filtering of internet and other ICT content by either the state or other actors.[110]

Social Media Councils

8. Could the Social Media Councils (SCMs) model, as introduced by Article 19, be reinterpreted on a larger scale, with the purpose of monitoring human rights, within the context of Digital Constitutionalism?

The South African government has put forth a *type* of Social Media Council (SMC) in South Africa. This was first brought about in April 2019 during the election period by Media Monitoring Africa (an independent think tank) and the Independent Electoral Commission of South Africa (IEC) with the aim of combating disinformation.[111] Dissemination of false statements intended to harm or disrupt the conduct or outcome of elections is prohibited under *Section 89(2) of the Electoral Act*.[112]

A Digital Disinformation Complaints Committee (DDC) was set up to receive all the complaints. Each complaint would be reviewed by a council with three members, each having expertise in media, digital and legal respectively. If the complaint constituted disinformation the IEC would review it and make a final decision. This decision was to be based on a domestic and international legal framework on the right to freedom of expression, public interest, and other relevant factors. The outcome could also entail further action being taken such as publication of a counter-narrative, referral to another appropriate body, etc. Outcomes of all complaints were published on the website to promote transparency and accountability, and a review mechanism before the Electoral Court was also set up.[113]

The IEC and MMA have now launched the REAL411 platform with the same process which has a broader focus on the speech offences of disinformation, incitement to violence, hate speech and harassment of journalists in any online space in South Africa. The project is continuing to emphasize the importance of a multi-stakeholder approach, and prioritizing the need for transparency and accountability in resolving complaints of speech offences.[114]

C. Privacy, Information Security, and Personal Data

Personal and Non-Personal Data

1. How do we define personal and non-personal data?

The different legislations governing data protection in South Africa are — *POPIA; Promotion of Access to Information Act, 2002* and the *Cybersecurity Bill 2015-16*. The *POPIA* is the primary legislation for regulating the usage, transmission etc. of personal data in South Africa. Though it was enacted in 2013, substantive provisions came into force in July 2020. The definition of personal information in the same is quite comprehensive.[115] Drawing on other legislations like the *Promotion of Access to Information Act, 2002* and

[107] ibid.
[108] South African Constitution 1996, ch 9.
[109] 'Freedom on the Net' (n 106)
[110] ibid.
[111] Electoral Commission, 'Electoral Commission launches online reporting platform for digital disinformation' (*Electoral Commission of South Africa*, April 2019) <https://www.elections.org.za/content/About-Us/News/Electoral-Commission-launches-online-reporting-platform-for-digital-disinformation/> accessed 20 March 2020.
[112] Electoral Act 1988, s 89(2).
[113] 'Submission by Media Monitoring Africa: Consultation Paper on Social Media Councils' (*Media Monitoring Africa*, December 2019) <https://mediamonitoringafrica.org/wp-content/uploads/2020/02/Untitled-attachment-00172.pdf> accessed 20 March 2020
[114] ibid.
[115] Protection of Personal Information Act, 2013, s. 1, 14.

reflected in bills like the *Cyber Security Bill, 2015-16*, personal information is defined to include biometrics, personal identifiers like name and address etc.[116] Furthermore, being an inclusive definition and not an exhaustive one, it also extends to online identifiers.[117]

However, the definition still extends to juristic persons. This was contested in a public hearing to deliberate upon *the Protection of Personal Information Bill*. Various groups like the Nelson Mandela Foundation posited that the inclusion of juristic persons within the ambit of personal information would defeat the very spirit of the *POPIA*.[118] It was claimed that big corporations, which fall within the ambit of juristic persons, could avoid scrutiny of their actions as they would have a right to privacy under the *Act*.[119] Equating the privacy of South African citizens and big corporations was considered unjust and unfair to the public at large.[120] Since the same has not been addressed in the *POPIA*, the possible misuse of the provision stipulated above stands.

With respect to non-personal information, the same has not been explicitly defined in the *POPIA*. In the definitions section of the Act, the meaning of de-identified information has been provided.[121] The clause posits that personal information devoid of personal identifiers, or any other information which can reasonably lead to the identification of an individual, is not covered within the ambit of the *POPIA*.[122] It has been inferred that though non-personal information has not been expressly defined, it has been excluded from the protection offered by the *POPIA*.

2. What should be the ethical, economic, and social considerations when regulating non-personal data?

Non-personal information has not been defined in the *POPIA* which makes it difficult to gauge the possible economic, ethical and social considerations arising from its use. However, the definition of de-identified data in the *POPIA* stipulates that information devoid of personal identifiers like name, address, email address, etc. will not be accorded protection.[123] In this context, it has been pointed out that the process of anonymization or de-identifying information has loopholes which can be exploited to violate the privacy of citizens.[124] This has adverse consequences in a two-fold manner. Firstly, the digital rights of citizens, especially vulnerable communities like women, indigenous groups, and tribals will be violated.[125] Secondly, private corporations would be able to profit through allegedly non-personal information and thus, infringe on the rights of South African citizens.[126] Apart from these ethical and social concerns, smaller businesses will be unable to compete with bigger firms in South African markets, putting forth certain economic considerations.[127] Neither do small businesses have sufficient resources to engage in adequate de-identification of information, easily afforded by bigger corporations, nor does this dataset have any utility for them.[128] Hence, this could potentially hinder competition and impact their survival? To accommodate these three considerations, regulations must be devised accordingly. As stipulated in the South African Law Commission Report, it must be ensured that de-identified data is audited to not indicate the identity of an individual.[129] Moreover, even if some information could potentially be used to ascertain the identity of an individual, then it falls under the ambit of the *POPIA*, thereby protecting the privacy of individuals.[130] With respect to the economic considerations, it is suggested that rules be devised to not threaten the activities of small businesses, like in the tele-marketing sector. A mechanism must be put in place which helps to retain the utility of non-personal data. Sufficient resources to

[116] ibid; Promotion of Access to Information Act, chap 1; Cyber Crime and Cyber Security Bill, s.1.
[117] Protection of Personal Information Act, 2013
[118] Public Meeting (2009) <https://pmg.org.za/committee-meeting/10876/> Accessed 10 March, 2021.
[119] ibid.
[120] ibid.
[121] Protection of Personal Information Act, 2013, s. 12.
[122] Protection of Personal Information Act, 2013, s. 6.
[123] ibid.
[124] Sweeney, 'k-Anonymity: A Model for Protecting Privacy'(2002) 10(05) *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 557; Constitution of South Africa, 1996, art 14.
[125] Manda (n 15).
[126] Martin Hesse, 'Protection of personal information laws kick in' Independent Online (IOL) (7 July 2020) <https://www.iol.co.za/personal-finance/protection-of-personal-information-laws-kick-in-50486568> Accessed 29 March, 2021.
[127] ibid.
[128] ibid.
[129] South African Law Commission, 'Privacy and Data Protection Report' (Project 124, 2009), s. 3.3.119.
[130] ibid, s. 3.3.120.

de-identify the data must also be provided so as to not attract the provisions of the *POPIA*.[131] This can be achieved through a risk assessment report by the concerned authorities.[132]

End-to-end Encryption

3. Should there be a backdoor to end-to-end encryption/Should traceability be enabled to prevent and mitigate instances of online harms? What would the benefits and detriments of the same be?

Tech companies have placed heavy reliance on security and privacy since the 2010s, and many messaging platforms such as WhatsApp have added end-to-end encryption to their user's communications.[133] While encryption may come in several forms, the goal has always been of protecting data confidentiality. End-to-end encryption attains that goal by creating an encrypted channel where only the client applications can access the decryption keys.

The legislation which governs this topic in South African is the *Electronic Communications and Transaction Act of 2002* (*ECTA*)[134] and the *Regulation of Interception of Communications and Provision of Communication-related Information Act of 2002* (*RICA*).[135] However, neither of these acts deal directly with the encryption. As per *ECTA*, cryptography providers have to register themselves with the Minister of Communications before providing any cryptographic services in South Africa.[136] Cryptography services are supposed to be provided in South Africa if the cryptography service is given to a person present in South Africa at the time of the person making use of the service. Any person who disregards the provisions of *ECTA* is guilty of an offence and would be subject to up to two years' imprisonment. [137]*RICA* on the other hand, provides for application for various types of directions to be issued, such as archived-communication directions, real-time communication directions, interception and decryption directions.

However, the *POPIA* gives South African data subjects nine enforceable rights over their personal information — including the rights to correction, access, and deletion. It also requires that companies follow eight minimum requirements for data processing (e.g., requiring consent as a legal basis). So, a lot of E2E platforms that share metadata, even contact details to Law Enforcement Agencies, on request in the name of enforcing protection mechanisms against harms from the 'disadvantages' of the technology, will not be able to do so now.

The development in encryption technology can have far-off consequences and potentially hamper the ability of legal authorities to get access to information exchanged between criminal groups on various platforms. As is usually the case with a privacy expansion of this nature, the individual's constitutional rights must be balanced up against public policy considerations in a subtle balancing act.

Regulatory Sandbox

4. How important is compliance with complex/technical/lengthy data protection and privacy statutes in events of crises (e.g. such as during pandemics, where time is essential)? In that regard, is there a need to provide regulatory sandboxes, and if so what could be the grounding philosophy to shape the rules of control for such ecosystems?

Ground-breaking events have profoundly impacted privacy and the significance assigned to protecting the personal data. The dispensation of special categories of personal data is permitted when it is essential for reasons of public interest in the area of public health, "such as protecting against serious cross-border threats

[131] ibid, s. 3.3.125.
[132] ibid, s. 3.3.123.
[133] Marc Laliberte, 'The question of building backdoors into encryption' (*Fintech futures*, 17 Nov 2020) <https://www.fintechfutures.com/2020/11/the-question-of%E2%80%AFbuilding%E2%80%AFbackdoors-into%E2%80%AFencryption%E2%80%AF%E2%80%AF%E2%80%AF/> accessed 4 April 2021.
[134] Electronic Communications and Transaction Act 2002.
[135] Regulation of Interception of Communications and Provision of Communication-related Information Act 2002.
[136] Electronic Communications and Transaction Act 2002, s 29(1).
[137] Electronic Communications and Transaction Act 2002, s 32(2).

to health [138]." Particularly with COVID-19, the ICT (Information and Communication Technology) tools are increasingly becoming common, and countries across the world have begun placing confidence in 'digital contact tracing apps' to lessen the harmful consequences of the emergency. The ICT allows people as well as organizations (i.e., governments, businesses, non-profit agencies, and criminal enterprises) to meet in the digital world. Although controllers may have ample room for manoeuvre while choosing the relevant legal bases for processing personal data to contain the virus, an assessment based on proportionality remains the basis for the application of measures that should neither be discriminatory nor excessive.

In this regard, there is a need to provide regulatory sandboxes, and the grounding philosophy must have three principles to shape the rules of control for such ecosystems – confidentiality, integrity, and availability.

Intelligence Agency

5. According to which principles and regulations should intelligence agencies operate online?

"Principles Governing Intelligence Agencies while Operating Online in South Africa:[139]

1. The principle of national intelligence organisation: Regardless of South Africa's constitutional model, there is a need for a national intelligence capability to exist. The national intelligence organisation must uphold the principles of objectivity, integrity, and credibility. Further, it shall strive to be relevant to the promotion, maintenance, and protection of national security.
2. The principle of departmental intelligence capabilities: Departmental intelligence capabilities must observe a similar fundamental approach to their tasks that apply to the national intelligence organisation. Such structures must observe the style, legal obligations, culture and character of the departments they serve.
3. The principle of political neutrality: No security service/organisation or intelligence shall be permitted to carry out any activities or operations that are intended to destabilize, endorse or influence any South African political party or organisation at the cost of another by any acts (e.g., "covert action" or "active measures") or by means of disinformation.
4. The principle of legislative sanction, parliamentary control and accountability: Legislation must provide the intelligence service with the mandate to bring out their typical activities pertaining to the stability, security, well-being, and interests of the State and its citizens.
5. The principle of the balance between transparency and secrecy: While requiring the vital component of secrecy, effective intelligence needs to be sensitive to the values and interests of a democratic society. To achieve it, a reasonable balance between transparency and secrecy needs to be found.
6. The principle of effective management and organisation and sound administration: The drift of intelligence to the Government should always be maintained. Continuity and Efficiency should be relentless objectives while making provision for transformational needs. The national intelligence organisation shall warrant effective management, administration and organisation of its activities. It shall strive to endorse a strong organizational culture that reflects professionalism, high standards, and moral integrity.
7. An ethical code of conduct for intelligence work: The code of conduct should have the backing of all pertinent parties, be based on commonly accepted democratic principles and all-encompassing of accepted intelligence principles, norms and practices.
8. Coordination of intelligence and liaison with departmental intelligence structures: A well-functioning intelligence coordinating mechanism is indispensable to manage the flow of priorities, information, duplication of resources, the audi alteram partem principle regarding the interpretation and other matters relating to the other functions of intelligence. The scope and degree of coordination between a national intelligence organisation and departmental intelligence/information structures must be influenced by the constitutional arrangements of the

[138] Nicole Scholz, 'Cross-border threats to health' (*ERPS*, Jan 2020) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646123/EPRS_BRI(2020)646123_EN.pdf> accessed 5 April 2021.

[139] 'Intelligence White Paper' (*South African Government*) <https://www.gov.za/documents/intelligence-white-paper> accessed 5 April 2021.

new South African state.140 Ultimately, the state of personal data protection is a mirror of the state of internet freedom in a country."

D. Intermediary Regulation

Online Harms and Netizens

1. How do we define online harms?

There is no overarching definition for 'online harms' in South African legislation. However, there are various offences across different legislations that could be classified as online harms. It include Publishing/distributing of child pornography and specific types of sexual content;[141] Hateful or discriminatory speech online;[142] Cybercrimes like unlawful acquiring of data, cyber fraud, forgery and uttering, and cyber extortion;[143]and Malicious communications.[144]

Apart from the above, Research ICT Africa made a joint submission urging the government to make laws on online gender-based violence, and the right to privacy.[145] They urged the government to consider the constantly evolving nature of online harms and include protection for various forms of online harms.[146]

2. How should community guidelines for online platforms be drafted, disseminated, and enforced? To what legal standards of accountability and transparency should online platforms be held, and in what capacity? Can you suggest any mechanisms (judicial, or otherwise) which might be capable of ensuring such a check on the functioning of these platforms?

As of now, there is no explicit law regulating social media platforms and requiring online harms to be dealt with. In formulating community guidelines, the social context of the region and historical violations against minority communities must be given importance. As highlighted earlier, the rights of (racial, sexual, gender, and other) minorities must be balanced with freedom of expression.[147]

Intermediaries must ensure that moderators handling reports are adequately trained and sensitised with respect to gender-based violence and human rights, and these standards must be used in responding to reports.[148] In the past year (from March 2020 to March 2021), the REAL411 platform received 1300 complaints in total, out of which 929 were disinformation complaints and 41% of those were determined to be disinformation.[149]

These platforms and their community guidelines should be held to and aligned with international human rights standards, and not with varying law of states or private interests.[150] Three key principles that must govern any legitimate intervention by governments or intermediaries are: (1) minimum intervention as per

---

[140] 'Intelligence White Paper' (*South African Government*) <https://www.gov.za/documents/intelligence-white-paper> accessed 5 April 2021.

[141] Film and Publications Act 1996, schedule 6; Sexual content with bestiality, degradation or extreme violence

[142] South African Constitution 1955, s 16; Promotion of Equality and Prevention of Unfair Discrimination Act 2000 (Equality Act), ss 10 and 12

[143] Cybercrimes and Cybersecurity Bill 2017, ss 3 to 10

[144] ibid, s 16 to 18

[145] 'Domestic Violence Amendment Bill' (Research ICT Africa, APC, ALT Advisory and Feministing While African Network 2020) <https://researchictafrica.net/wp/wp-content/uploads/2020/10/Domestic_Violence_Amendment_BillB20-2020-Joint-SubmissioRIA-APC-ALT-FWA.pdf> accessed 20 March 2020.

[146] ibid; Harms such as surveillance tracking & monitoring, controlling devices, online harassment, direct threats & violence, malicious distribution, intimate images and intimate audio recordings.

[147] Rima Athar, 'From impunity to justice: Improving corporate policies to end technology-related violence against women' (APC 2015).

[148] ibid.

[149] William Bird and Thandi Smith, 'Disinformation in a time of Covid-19: A year on, here's the 411 on what we have learnt about disinformation' *Daily Maverick* (22 March 2021) <https://www.dailymaverick.co.za/article/2021-03-22-disinformation-in-a-time-of-covid-19-a-year-on-heres-the-411-on-what-we-have-learnt-about-disinformation/> accessed 3 July 2021. Also *see*, 'See our latest trends' (*REAL 411*) <https://www.real411.org/trends> accessed 3 July 2021.

[150] ibid.

necessity and proportionality; (2) inclusive consultation with all relevant stakeholders; and (3) not strengthen the dominant position of the large incumbents.[151]

3. Should online platforms be immune from liability from third-party, user generated content [refer to intermediary liability laws]?

In South Africa, defamation, obscenity and indecency and hate speech can expose internet intermediaries to liability.[152] The standard for defamation is as given in common law, and for obscenity, indecency and hate speech is in legislations.[153] Under the *Film and Publications Act*, intermediaries may be liable for content on their networks that has been censored, or is not classified by the Film and Publications Board.[154] Hate speech is regulated under the *South African Constitution* and *the Equality Act*.

South Africa follows a safe harbor model with notice and takedown for intermediary liability. Intermediaries are not liable for being conduits, automatic caching, hosting or damages arising from data stored at user's request.[155] The intermediary is not liable as long as they did not have knowledge of the infringing data or act.[156] They are not liable for being a tool for information location — like a search engine or aggregator.[157] There are no checks or balances on perceived biases in searches or aggregations in South Africa. Hence intermediaries are, *for most part*, immune from liability from third-party user-generated content.

The concern with the safe harbor approach, is that intermediaries err on the side of caution and take down content that is treading the fine line between legal and not, resulting in a chilling effect.[158] Rather than holding intermediaries liable for failure to takedown illegal content, a governance approach that focuses on regulating company processes is the way to go. This would require governments to regulate the amplification of harmful and illegal content by requiring companies to make design choices in features like recommendations, search engine results, and trends to avoid such content. This should be checked by an independent regulator on the basis of fixed standards,[159] based on international human rights law. Governments should take active efforts to ensure that platforms adhere to these laws, while protecting net neutrality and encryption.[160]

4. What should the parameters to define problematic user-generated content be?

1. Publishing Without Permission: Make rights management imperative to make sure that only the approved content is published. While user-generated content can be voluntarily created and circulated, one should dodge misunderstandings and breaches of trust by asking for customer's consent. It is imperative to reach out to the content creator and ask them to grant one rights to their content. The scope of the rights is controlled by one through the terms and conditions that one attached to the request. One can make sure that one points out both distribution and contribution rights in one's terms and conditions, and after understanding the conditions and terms of social networks, one can use them well.
2. Sexual Content / Child Pornography: Under the *Film and Publications Act 1996* films containing explicit violent sexual conduct, child pornography, bestiality, which constitute incitement to cause harm and explicit infliction of extreme violence are all classified as XX and distributing/broadcasting/advertising/selling/publishing these are an offence.[161]

[151] Mathias Vermeulen, 'Online Content: To Regulate or Not to Regulate – Is that the question?' (APC 2019) <https://www.apc.org/sites/default/files/OnlineContentToRegulateOrNotToRegulate.pdf> accessed 21 March 2020.
[152] Alex Comnios, 'Intermediary Liability in South Africa' (APC 2012) <https://www.apc.org/sites/default/files/Intermediary_Liability_in_South_Africa-Comninos_06.12.12.pdf> accessed 20 March 2020.
[153] ibid.
[154] Film and Publications Act 1996, s 21
[155] ECTA, ss 73 and 74
[156] ibid, s 75
[157] ibid, s 76
[158] Comnios (n 152).
[159] ibid.
[160] ibid.
[161] Film and Publications Act 1996, schedule 6.

3. Hate speech: Online speech that would be incitement of imminent violence, or hate speech and propaganda for war would all constitute online harms. Further, under *Section 10 of the Equality Act*: "10. (1) Subject to the proviso in section 12, no person may publish, propagate, advocate or communicate words based on one or more of the prohibited grounds, against any person, that could reasonably be construed to demonstrate a clear intention to — (a) be hurtful; (b) be harmful or to incite harm; (c) promote or propagate hatred."[162] Therefore, Online speech, which is hate speech, would constitute online harm.
4. Cybercrimes: In 2017, the *Cybercrimes and Cybersecurity Bill* was laid down in the South African National Assembly.[163] Under the bill, the following online harms have been included — unlawful acts in respect of software or hardware tool;[164] unlawful acquiring of data;[165] unlawful interference with data or computer program;166 unlawful acquisition, possession, provision, receipt, or use of passwords;[167] cyber fraud, forgery, and uttering;[168] and cyber extortion.[169]
5. Malicious Communications: The Cybercrimes Bill also includes online harms of malicious communications, including data message which is harmful;[170] data message which incites damage to property or violence; and distribution of data messages of intimate images without consent.[171]

5. Should online platforms moderate 'fake news', and if so, why?

On one hand, one can view social media platforms as technologies that simply permit people to share and publish material. On the other hand, one could argue that social media systems have now grown curators of content but these platforms ought to take some obligation over the content published on their systems. From the very inception of the pandemic, there were some misconceptions flowing that due to perhaps the topographical conditions of the continent, the instrumental organisms of the virus would not flourish. *Section 11(5) of the Regulations* issued in terms of *Section 27(2) of the Disaster Management Act*, *2002* creates several content-related offences punishable with respect to publishing misleading statements regarding COVID-19. These offences are punishable up to six months imprisonment. Specifically, *Section 11(5)* criminalizes publication, in "any medium" of information with "intention to deceive any other person about" COVID-19, the COVID-19 infection status of any person; or government measures taken in response to COVID-19.[172] However, a set of techniques is recommended to help them with dealing with hate speech and fake news.

A. Artificial and Human Intelligence together

In the beginning, social media companies recognised themselves not to hold any accountability over the content being published on their platform.[173] In the intervening years, they have since set up a mix of human-driven and automated editorial processes to filter certain types of content.[174] The large volume of content disseminated on social media makes it impossible to create a comprehensive editorial system. For example: It is estimated that 500 million tweets are sent per day on Twitter.[175] The focus and terminology of hate speech vary over time, and most fake news articles do not comprise at least some level of truthfulness in them. Therefore, they must advance approaches that utilize human and artificial intelligence together.

[162] Promotion of Equality and Prevention of Unfair Discrimination Act 2000 (Equality Act), s 10.
[163] Cybercrimes and Cybersecurity Bill 2017.
[164] ibid, s 4.
[165] ibid, s 3.
[166] ibid, s 5.
[167] ibid, s 7.
[168] ibid, ss 8 and 9.
[169] ibid, s 10.
[170] ibid, s 17.
[171] ibid, s 18.
[172] 'South Africa: Prohibitions of false COVID 19 information must be amended' (*Article 19*, 23 April 2021) <https://www.article19.org/resources/prohibitions-of-false-covid-information-must-be-amended/> accessed 12 July 2021.
[173] Dipayan Ghosh, 'Are We Entering a New Era of Social Media Regulation' (*Harvard Business Review*, 14 Jan 2021) <https://hbr.org/2021/01/are-we-entering-a-new-era-of-social-media-regulation> accessed 4 April 2021.
[174] Lee Rainie, Janna Anderson and Jonathan Albright, 'The Future of Free Speech, Trolls, Anonymity and Fake News Online' (*Pew Research Centre*, 29 March 2017) <https://www.pewresearch.org/internet/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online/> accessed 29 March 2021.
[175] 'Twitter Usage Statistics' (*Internet Live Stats*) <https://www.internetlivestats.com/twitter-statistics/> accessed 27 March 2021.

B. Finding the Needle in a Haystack

It's vital to not forget how recommendation algorithms on social media structures might also inadvertently promote fake and hateful speech. At their core, these recommendation systems classify users primarily based on their shared interests and then promote the same type of content to all users inside each group. The most suitable response is to censor and ban the content material without any hesitation in rare instances.

C. Fight Misinformation with Information

Presently, social media groups have adopted two techniques to fight misinformation. The first one is to dampen such content outright. As an example, Pinterest banned anti-vaccination content, and Facebook banned white supremacist content material.[176] The opposite is to offer alternative information alongside the content material with fake information to expose the correct information and truth. This approach, which YouTube carries out, inspires customers to click on the hyperlinks with validated and vetted data that might debunk the inaccurate claims made in fake or hateful content.

Disinformation amid the Pandemic

Using social media for peddling fake news and hate speech is not always a new phenomenon. Before the pandemic, episodes of information removal peaked at some point of elections,[177] socio-political movements,[178] while controlling financial markets.[179] Amidst the COVID-19 crisis, it has become quite clear that sizable fake news can threaten public health.[180] Public awareness is fundamental in battling a health disaster. But, if the regulation of misinformation remains in the hands of systems or government agencies, it becomes susceptible to perception-alteration processes.[181]

Fact-checking bodies are also working day in and out to counter fake news drives, including, in India — reports about alleged 'cures' against the COVID-19.[182] Of all the content in these platforms, extremist, fake, and populist often garner high 'interaction' numbers.[183] For example, Facebook took down 40 million deceptive posts in March 2020 alone and another 50 million the subsequent month.[184]

The question, therefore, is whether these platforms are beset with unethical and manipulative content, can they still democratize? In theory, the principle so-called 'marketplace of ideas' is a basis of free speech laws; it assumes that 'truth' would prevail in a level playing field. In the marketplace of ideas, this theory fails — it appears social media is neither equal nor fair.[185] A platform's design to make the most of financial gains through data monetisation techniques can engulf 'truth' with inbuilt susceptibility to viral, sensationalist,

---

[176] Mark Wilson, 'The tech giant fighting anti-vaxxers isn't twitter or Facebook. It's Pinterest' (*Fast Company*, 26 Feb 2019) <https://www.fastcompany.com/90310970/the-tech-giant-fighting-anti-vaxxers-isnt-twitter-or-facebook-its-pinterest> accessed 30 March 2021.

[177] Arjun Sidharth, 'How misinformation was weaponized in 2019 Lok Sabha election – A compilation' (*ALT News*, *18 May* 2019) <https://www.altnews.in/how-misinformation-was-weaponized-in-2019-lok-sabha-election-a-compilation/> accessed 1 April 2021.

[178] Snigdha Poonam and Samarth Bansal, 'Misinformation Is Endangering India's Election' (*The Atlantic*, 1 April 2019) <https://www.theatlantic.com/international/archive/2019/04/india-misinformation-election-fake-news/586123/> accessed 1 April 2021.

[179] Shimon Kogan, Tobias J. Moskowitz, and Marina Niessner, 'Fake News in Financial Markets' (*SSRN*, 31 Aug 2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3237763> accessed 29 March 2021.

[180] 'How fake news has exploited COVID-19' (*PWC*) <https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/how-fake-news-has-exploited-covid19-cyber.html> accessed 29 March 2021.

[181] Bhaskar Chakravorti, 'The countries that trust Facebook the most are also the most vulnerable to its mistakes' (*The Conversation*, 27 March 2018) <https://theconversation.com/the-countries-that-trust-facebook-the-most-are-also-the-most-vulnerable-to-its-mistakes-93706> accessed 31 March 2021.

[182] Julie Posetti and Kalina Bontcheva, 'Disinfodemic Deciphering COVID-19 disinformation' (*UNESCO*, 2020) <https://en.unesco.org/sites/default/files/disinfodemic_deciphering_covid19_disinformation.pdf> accessed 1 April 2021.

[183] United Nations, 'UN chief Global Appeal to Address and Counter COVID-19 Related Hate Speech' Countering COVID-19 Hate Speech <https://www.un.org/sg/en/node/251827> accessed 29 March 2021.

[184] IANS, 'Facebook flagged 50 million misleading COVID-19 posts in April' (*India TV News*, 13 May 2020) <https://www.indiatvnews.com/technology/news-facebook-flagged-50-million-misleading-covid-19-posts-in-april-616897> accessed 30 March 2021.

[185] Richard Stengel, 'Why America needs a hate speech law' (*The Washington Post*, 29 October 2019) <https://www.washingtonpost.com/opinions/2019/10/29/why-america-needs-hate-speech-law/> accessed 30 March 2021.

curated campaigns. Problematic speech is heightened due to the polarisation online and the asymmetry of information.[186] The Indian approach must leave excessive criminalisation and, as a substitute, adopt a holistic approach to operationalize a model with essential safeguards.

6. Should safe-harbour protections be offered to online platforms, given that the grant of such a protection will come at the cost of fundamental rights (e.g. privacy) of citizens? If affirmative, how should this balance be achieved? [Read with Questions in Part B.]

Certain immunity is conferred on intermediaries in the form of 'safe harbor' for third parties' unlawful and illegal acts. The safe harbor exempts intermediaries who store, host, and disseminate data from any liability unless they were conscious of any illegal content being transmitted and stored on their platform, which was not acted upon under a reasonable time. The purpose of the safe harbor is limited to the preservation of intermediaries from any arbitrary penalty. In South Africa, the service providers are liable for many things for which they seek safe harbor. For instance, 'indirect' copyright infringement is the broad category making the service providers seek safe harbor. Still, there has not been any case in South Africa holding Internet Service Providers (ISPs) liable. It may be that *Section 16 of the Bill of Rights* requires that ISPs should not be made liable at all.

Chapter 11 of the South African Electronic Communications Act 25 of 2002 makes available limited liability of internet intermediaries subject to a condition of a takedown notice.[187] These provisions apply to members of the Internet Service Providers Association. An instant response to takedown notices is essential though turnaround time is not stipulated, failing which the protection from liability is forfeited. Concerns have been raised regarding South Africa's framework, like most of the concerns around the safe harbor approach: ISPs stumble on the side of caution and are rapid in removing content without even providing the content provider with an opportunity to defend the content. There exist no appeal mechanisms for content providers or creators. This is a matter of concern, given the fact that any person can submit a take-down notice.[188]

In South Africa, regarding copyright infringements by third parties, there is a uncertainty about the scope of the 'safe harbor' for service providers.[189] When the liability of a particular service provider is to be determined, one should remember that the law of copyright imposes liability for acts or omissions in certain specific instances. For instance, when a service provider makes unauthorised reproductions of a protected work, it may be liable for infringement of copyright. But in a case where it merely transmits or eases access to copyright-infringing material, it may be held liable only for 'contributory infringement' in the common law. However, the principle of 'contributory infringement' has not been established in any of the reported decisions on South African copyright law.[190]

Further, there is no appeals mechanism for take-down notices, leaving third parties and ISPs who posted or created the content in question with limited options to challenge take-down notices other than through the mechanism of courts. All users of the internet are not on the same footing regarding take-down procedures. Due to the *Electronic Communications and Transactions Act 2002* (*ECTA*) not providing adequate protection to third parties, it would appear that it does not provide an adequate balance between the accountability of ISP and the interests of all the users of the internet. [191] This system could be open to abuse

[186] Dan M., 'The Marketplace of Ideas is a Failed Market' (*The Medium*, 14 February 2017) <https://medium.com/@danmcgee/the-marketplace-of-ideas-is-a-failed-market-5d1a7c106fb8> accessed 28 March 2021.

[187] 'No.25 of 2002: Electronic Communications and Transactions Act, 2002' (Aug 2002) 446(2) Government Gazette <https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf> accessed 27 March 2021.

[188]See further Alex Comninos, 'Intermediary liability in South Africa' (2012) (accessible at https://www.apc.org/sites/default/files/Intermediary_Liability_in_South_Africa-Comninos_06.12.12.pdf). See also Rens, 'Failure of Due Process in ISP Liability and Takedown Procedures' in Global Censorship, Shifting Modes, Persisting Paradigms (2015) <https://law.yale.edu/sites/default/files/area/center/isp/documents/a2k_global-censorship_2.pdf> accessed 27 March 2021

[189] Natasha Primo and Libby Lloyd, 'South Africa, in Media Piracy in Emerging Economies ed. Joe Karagianis' (*Social Science Research Council*, 2001) <http://piracy.src.org> accessed 4 April 2021 105, 117.

[190]Department of Trade and Industry, Copyright Review Commission Report (2011) <http://www.info.gov.za/view/DownloadFileAction?id=173384> accessed 29 March 2021 35.

[191] N.D. O'Brien, The Liability of Internet Service Providers for Unlawful Content Posted by Third Parties, Masters Thesis, Faculty of Law at the Nelson Mandela Metropolitan University, January 2010, <http://dspace.nmmu.ac.za:8080/jspui/bitstream/10948/1149/1/NDOBRIEN.pdf> p. 144.

by corporations or individuals seeking to get rid of content from the internet for purposes other than concerns in good faith over unlawful content.[192]

7. How does the global intermediary ecosystem shift from a post-hoc, harm-prevention lens to a proactive approach towards understanding and regulating technology?

With the use of technology rising exponentially, the tussle over internet governance continues. On one end are the states led by the U.S. and its associates supporting a global, open and free model of the internet called the 'Western model.' On the other end are a group of states led by Russia and China, supporting a controlled and sovereign version of the internet, a 'Leviathan model.'[193] Although the idea of an internet embodying the principles of openness, equality, and multi-stakeholderism poses a challenge to this model, making it difficult, if not impossible, to prefer one model over the other.

While the internet has enormous potential to aid the development of states on many fronts, it can also be used for illicit purposes. Cybercrime is one of the unnerving challenges of the internet era.[194] Technological advancements that permit unique features like anonymity in cyberspace make cybercrimes less risky with the potential to deliver high returns, making it all the more tempting to various actors. The conference on Cybercrime of the Council of Europe, referred to as the Budapest conference, is the only global tool presently in the vicinity that addresses cyber-crime.[195] Spotting the paramount need for combating crimes, it criminalizes conduct that influences the "confidentiality, integrity, and availability of networks, computer systems, and computer data."

Furthermore, tackling a complicated problem like cyber-crime including questions of laws, technicalities, and human rights, requires concerted efforts from numerous stakeholders that include the private sector and civil society. It is only through such multi stakeholder efforts that we can check the use of ICTs for criminal purposes without clogging human rights.

8. Do the guidelines/policies of online platforms account for fallibility of the algorithm and the human content moderators, and if so, to what extent?

Filtration of content through content moderation allows the online platforms to ease the digital experience for their users as it removes inappropriate content and consequently, simplifies the navigation through the abundance of information available online.[196]

If we take South Africa in perspective, the most used 'social' platforms are WhatsApp, Facebook and YouTube.[197] Therefore, the fallibilities of the algorithm and human content moderation, content moderation in these three platforms shall be looked into.

WhatsApp has opened up challenges for not just content moderation but also for government regulations. In order to repair the problem of information disorder and to prevent third-party access, an end-to-end encryption service was introduced.[198] Since encryption is not available for backup storage or cloud services, encrypted messages can easily be accessed by investigative agencies through cloning.[199] But despite that, the content of WhatsApp is being moderated both at the content and at the account level. While algorithmic moderation is deployed at the account level, at the content level, it implements measures, such as encryption,

[192] Comnios (n 152).
[193] ibid.
[194] Allison Peters, 'Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime' (*Thirdway*, 2 October 2019) <https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime> accessed 31 March 2021.
[195] ETS No. 185, Council of Europe, Explanatory Report to the Convention on Cybercrime. 23. XI. (2001) ETS – No.185. Budapest.
[196] Barrie Sander, 'Freedom of Expression in the Age of online platforms' (2020) 43(4) Fordham International Law Journal <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2787&context=ilj> accessed 28 March 2021.
[197] Simona Varrella, 'Penetration rate of social media in South Africa 2020' (*Statista*, 23 March 2021) <https://www.statista.com/statistics/1189958/penetration-rate-of-social-media-in-south-africa> accessed March 28, 2021.
[198] The Quint, 'Is WhatsApp Really End-to-End Encrypted? Are My Chats Secure? (*The Quint* 28 September 2020) <https://www.thequint.com/tech-and-auto/whatsapp-end-to-end-encryption-chat-leak-security#read-more> accessed 4July 2021.
[199] ibid

groups of up to 256 people, and the forward function, to curb the vitality of problematic messages.[200] Apart from this, recently the issue of WhatsApp backdoor was reported which could be a grave threat to privacy in the Indian context.[201] Despite the two-level screening, the cases of fake news on WhatsApp are growing and since the stories are of a really emotive nature, they receive an immediate reaction from the public. WhatsApp community guidelines list down the code of conduct and best practices for use of WhatsApp, though it does not specifically mention the details of content moderation anywhere.

YouTube has been recently brought into the limelight due to its offensive or violent videos, which might not be suitable for children. It has re-launched its hate speech policy but the content moderation on the platforms has been reported to be very haphazard and inconsistent.[202]

Most platforms use automated content moderation to ensure efficiency, however, there are limits regarding their accuracy. Therefore, moderation must also be accompanied by pre/post human moderation to account for fallibility of automated moderation. Human moderation also allows for the application of greater degree of context regarding local culture, politics etc and common sense.[203]

9. What role should community guidelines drafted by online platforms play in the governance of user-generated content? How should the terrain of conflict between community guidelines, public policy domestic contexts, and international human rights be negotiated upon?

Out of the User Generated Content Statistics so revealed, the biggest social media platforms in terms of their ranking are — Facebook, Instagram, Twitter and YouTube.[204] These online platforms depend upon Terms of Service/Use or Community Guidelines/Standards to govern the 'content and conduct' of its users. It includes specific guidelines about the rights, license, copyrights, duration and removal of content uploaded by users.[205] To identify illegal content, online platforms deploy tools such as 'notice and takedown', 'flagging by users' and machine learning models.[206] In South Africa, *Section 77 of the Electronic Communications and Transactions Act* delineates the requirement of 'notification of unlawful activity'. In the same *Act*, notice and takedown provision are laid down along with sections on caching, mere conduit etc.[207] The South African parliament recently passed *the Films and Publications Amendment Act, 1996* which broadened the definition of 'film' to include user-generated content. However, this move has been in criticism due to the vague terms and inconsistent application.[208]

When community guidelines conflict with domestic public policy contexts, the latter shall prevail. They vary from country to country and are more stringent in identifying illegal content than national laws. The community standards of online platforms are designed so as to ensure a safer environment for its users. This largely comes under the self-governance mechanism of these platforms.[209] For instance, recently in a defamation case about an Austrian politician, the EU's highest court ordered Facebook and other apps to take

---

[200] Gillespie and others, 'Expanding the debate about content moderation' (2020) 9(4) Internet Policy Review <https://policyreview.info/pdf/policyreview-2020-4-1512.pdf> accessed 28 March 2021.

[201] Malcolm Owen, 'WhatsApp backdoor defeats end-to-end encryption, potentially allows Facebook to read messages' (*Appleinsider* 13 January 2017) <https://appleinsider.com/articles/17/01/13/whatsapp-backdoor-defeats-end-to-end-encryption-potentially-allows-facebook-to-read-messages> accessed 29 March 2021.

[202] Louisa Matsakis, 'YouTube Doesn't Know where its own line is' (*Wired* 03rd February 2018) <https://www.wired.com/story/youtube-content-moderation-inconsistent/> accessed 27 March 2021.

[203] Alexendre De Streel and others, 'Online Platforms' Moderation of Illegal Content' (European Parliament, June 2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf> accessed 4 July 2021

[204] Staff Writer, 'The biggest and most popular social media platforms in South Africa, including TikTok' (*Business Insider* 1st July 2021) <https://businesstech.co.za/news/internet/502583/the-biggest-and-most-popular-social-media-platforms-in-south-africa-including-tiktok/> accessed 4 July 2021.

[205] 'Terms of Service' (*YouTube*, 2021) <https://www.youtube.com/static?gl=GB&template=terms> accessed 28 March 2021

[206] De Streel (n 203).

[207] Ashley Johnson and Daniel Castro, 'How other countries have dealt with Intermediary Liability' (*Information Technology and Innovation Foundation*, 22 February 2021) <https://itif.org/publications/2021/02/22/how-other-countries-have-dealt-intermediary-liability> accessed 4 July 2021.

[208] Kevin Hoole, 'Film and Publications Bill – Internet Censorship?' (*Michalsons*, 13 March 2018) <https://www.michalsons.com/blog/film-and-publications-bill/33423> accessed 4 July 2021.

[209] Reality Check, 'Social media: how do other governments regulate it' (*BBC News*, 12 February 2020) <https://www.bbc.com/news/technology-47135058> accessed 30 March 2021.

down all illegal posts from their websites.[210] The need for regulation by the government arises because it is very difficult to design the community guidelines to be applicable to the whole world, with a wide variety and diverse global community. Online platforms try to stay on a safe side by removing more illegal content than what is required by national law because they are not equipped with the same resources which are at court's disposal.[211] For instance, in some countries, it is illegal to share things that are considered to be blasphemous, though this is not particularly in violation of any community guidelines.[212] Thus, these social media platforms such as Facebook do keep in mind the local law and often the national government requests the platforms to take down the content if it believes the content to be violative of the local law.[213] Often the government requests the social media platform to take down content citing various reasons, such as copyright infringement, defamation, national security, etc. For instance, the South African government has made 31 removal requests since 2009, due to which 128 items have been removed from Google and YouTube.[214]

Political Advertising

10. Should the advertisement policies and sponsored content of online platforms adhere to certain standards (e.g. of whether they interfere with the political opinions and elections in a democracy)? If so, who should frame these policies, and who should be the final arbiter?

The increasing reliance on digital advertising has mandated the standardisation of ad formats. Such standardisation helps in resolving the issue of coordination between the publishers and advertisers.[215]

All over the world, there are certain basic principles that are recognised as standards for advertisement. As per these, the ads should be decent, legal, honest, and truthful. Alongside these standards, the advertisement shall also follow the norms and principles of fair competition as are generally accepted in the business.[216] Similar standards are also present in *Code of Advertising Practice*, a self-regulation code for advertisement regulation in South Africa. *Section 1.1 of the Preamble* states indeed that "All advertisements should be legal, decent, honest and truthful".[217]

Recently, many online platforms such as Facebook and Google have come into the limelight due to their unregulated political advertisement. For instance, in the 2014 national election in South Africa an advertisement that was published on YouTube, and which depicted the governing political party in a negative light with serious alleged corruption charges, was banned by the South African Public Broadcasting Corporation.[218]

These political ads can often lead to a tidal wave of misinformation which, in turn, could impact the ideal of 'free and fair election'. A blanket ban on a political advertisement would not solve the problem, instead, online platforms shall take greater responsibility for the content that is being published on their websites. These companies shall look up to the advertising standards of "truthful and honest" advertising and thus, should review the content moderation to reduce the spread of misinformation. In this way, freedom of speech

---

[210] Chris Fox. 'Facebook can be ordered to remove posts worldwide' (*BBC News*, 3 October 2019) <https://www.bbc.com/news/technology-49919329> accessed 29 March 2021.

[211] De Streel (n 203).

[212] Archit Lohani, 'Countering Disinformation and Hate Speech Online: Regulation and User Behavioural Change' (ORF Occasional Paper No. 296, January 2021, Observer Research Foundation.) <https://www.orfonline.org/research/countering-disinformation-and-hate-speech-online/> accessed March 28th, 2021.

[213] Facebook, 'Explaining Our Community Standards and Approach to Government Requests' (*Facebook*, 15 March 2015) <https://about.fb.com/news/2015/03/explaining-our-community-standards-and-approach-to-government-requests/> accessed 29 March 2021.

[214] Google Transparency Reports (*Google*, 2020) <https://transparencyreport.google.com/government-removals/overview?request_country=period:;authority:;p:2&lu=request_country> accessed 28 March 2021.

[215] Avi Goldfarb and Catherine Tucker, 'How do advertising standards affect online advertising?' 2011 SSRN Online Journal <https://www.researchgate.net/publication/228472974_How_do_advertising_standards_affect_online_advertising> accessed 29 March 2021.

[216] 'Codes and Standards' (*International Council for Ad Self Regulation)* <https://icas.global/standards/> accessed 29 March 2021.

[217]Preamble, Code of Advertising Practice v 2021.1, Advertising regulatory Board.

[218] Siyasanga M Tyali and Rofhiwa Felicia Mukhudwana, 'Discourses on Political Advertising in South Africa: A social media reception analysis' in *Social Media and Elections in Africa* (Springer 2020).

could be reconciled with the safety against misinformation.[219]

The *ICC Advertising and Marketing Communications Code* is regarded as the global benchmark of Advertising Self-Regulation. Though this is a global standard, the advertisement standard shall be tailored to national specificities, similar to the advertisement itself.[220] Presently, two forms of advertising regulation exist, which are, self-regulation and statutory regulation.[221]

In a self-regulatory model, an impartial administrator, who is independent of government as well as of the marketplace, acts as a regulator. This model acts as a middle ground between total surveillance and total exemption of rules.[222] Such an independent body, in the case of South Africa, is the South African Advertising Regulatory Board. This body administers the *Code of Advertising Practice* and ensures that the requirements of the Code are being satisfied by the advertising industry.[223]

On the other hand, statutory regulation involves the body which is created under the legislation, or legislation that governs the content of the advertising.[224] The South African advertising code has been recognised as the accepted standard under the *Electronic Communications Act*, *2005*.[225] In South Africa, there is no comprehensive legislation that governs the regulation of advertisement, however, there is a body of fragmented legislation that *inter alia* prohibit misleading statements, deal with intellectual property and control of specific products. Similarly, there are censorship legislations such as *Films and Publications Act*, that control racism and hate speech, and can ensure the regulation of offensive advertising.[226]

[219] Mark Scott, 'Why banning political ads on social media misses the point' (*Politico*, 21 November 2019) <https://www.politico.eu/article/facebook-twitter-google-political-ad-ban/> accessed 29 March 2021.
[220] 'Codes' (n 216).
[221] Stefan W Vos, *Regulating offensive advertising in a democratic South Africa*, (University of Pretoria, 2011).
[222] ibid.
[223] Advertising Regulatory Board (*KISCH)* <https://www.kisch-ip.com/advertising-regulatory-board > accessed 31 March 2021.
[224] Vos (n 221).
[225] Electronic Communications Act 36 of 2005.
[226] Vos (n 221).

ANNEXURE

Questionnaire | Project Aristotle

a. Digital Constitutionalism and Internet Governance

1. What factors can be considered important to ground Digital Constitutionalism in traditional constitutional concepts?
2. How can we define Digital Constitutionalism?
3. What should be the core tenets of a Digital Constitution?
4. How can Digital Constitutionalism present a constitutional model for the people, by the people, and of the people?
5. How can online platforms be made more inclusive, representative, and equal?
6. What role should open-source intelligence (=OSINT: the discipline of assembling and analyzing publicly available information) play in the future of our society?
7. Should the Digital Constitution be an integrative model, which draws upon and comprehensively presents standards for specific laws (e.g. antitrust, evidentiary standards etc.) as opposed to grounding ideals? If so, how should it fulfil the responsibilities of a pluralistic enterprise such as this as well as the specific needs of a pluralistic global society?
8. How can competition and antitrust laws of different jurisdictions protect the global market from big-tech domination, and is there a need to?
9. What is the role of regional/grassroots actors as well as inter-judicial cooperation/coordination in the digital ecosystem? Which other mechanism(s) might be more helpful?
10. Can the Digital Constitution present an anchor for the governance of the virtual world similar to a traditional constitutional model or will it always be in flux? Is there a need for constitutional innovation, and if so, in which areas (e.g. the right to be forgotten as a novel right)?
11. How is it possible to harmonise diverse national frameworks in order to achieve a global Digital Constitution?

b. Human and Constitutionally Guaranteed Rights:

1. Which human and constitutionally guaranteed rights do online platforms affect, and how?
2. Who can be defined as a netizen?
3. Who can be classified as a 'bad actor', and can 'bad actors' be netizens?
4. How can we embed within the digital ecosystem approaches which are responsive to the needs of minorities (e.g. ethnic minorities, racial minorities, gender minorities, religious minorities)?
5. How should the digital age of consent be arrived at and what should it be? In pursuance of which child rights should such an age be identified?
6. How should public order be defined for the digital space? Should situations of disorder in the offline world influence the definition and management of public order online, and if so why and when?
7. Should the state be allowed to impose internet shutdowns, slowdowns and communication throttles? What socio-legal rationale could be adopted by states in order to do so?
8. Could the Social Media Councils (SCMs) model, as introduced by Article 19, be reinterpreted on a larger scale, with the purpose of monitoring human rights, within the context of Digital Constitutionalism?

c. Privacy, Information Security, and Personal Data:

1. How do we define personal and non-personal data?
2. What should be the ethical, economic, and social considerations when regulating non-personal data?
3. Should there be a backdoor to end-to-end encryption/Should traceability be enabled to prevent and mitigate instances of online harms? What would the benefits and detriments of the same be?

4. How important is compliance with complex/technical/lengthy data protection and privacy statutes in events of crises (e.g. such as during pandemics, where time is essential)? In that regard, is there a need to provide regulatory sandboxes, and if so what could be the grounding philosophy to shape the rules of control for such ecosystems?
5. According to which principles and regulations should intelligence agencies operate online?

d. Intermediary Regulation:

1. How do we define online harms?
2. How should community guidelines for online platforms be drafted, disseminated, and enforced?
3. To what legal standards of accountability and transparency should online platforms be held, and in what capacity? Can you suggest any mechanisms (judicial, or otherwise) which might be capable of ensuring such a check on the functioning of these platforms?
4. Should online platforms be immune from liability from third-party, user generated content [refer to intermediary liability laws]?
5. What should the parameters to define problematic user-generated content be?
6. Should online platforms moderate 'fake news', and if so, why?
7. Should safe-harbour protections be offered to online platforms, given that the grant of such a protection will come at the cost of fundamental rights (e.g. privacy) of citizens? If affirmative, how should this balance be achieved? [Read with Questions in Part B.]
8. How does the global intermediary ecosystem shift from a post-hoc, harm-prevention lens to a proactive approach towards understanding and regulating technology?
9. Do the guidelines/policies of online platforms account for fallibility of the algorithm and the human content moderators, and if so, to what extent?
10. What role should community guidelines drafted by online platforms play in the governance of user-generated content? How should the terrain of conflict between community guidelines, public policy domestic contexts, and international human rights be negotiated upon?
11. Should the advertisement policies and sponsored content of online platforms adhere to certain standards (e.g. of whether they interfere with the political opinions and elections in a democracy)? If so, who should frame these policies, and who should be the final arbiter?

Institute
for Internet &
the Just Society