POLICY ACTION NETWORK

PAN TOPICAL GUIDES

AI & DATA SERIES 8

THE POLITICS OF AI & DATA: MEDIA & ELECTIONS IN SOUTH AFRICA

science & innovation
Department:
Science and Innovation
REPUBLIC OF SOUTH AFRICA

HSRC
Human Sciences
Research Council

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

SUMMARY

This Topical Guide serves as an introduction to the relationship between developments in Artificial Intelligence (AI) and electoral integrity, in a South African and an African context. By expanding consideration of both the actions and actors involved in the electoral process, the Guide provides a foundation for key debates within both data governance generally, and AI more specifically, with electoral integrity as the central normative objective.

Though issues of mis- and disinformation are of direct relevance to exploring the potential influence of AI (and big data) on elections, understanding the social and political phenomenon that underscore technologies is of more relevance for designing effective policy interventions.

In South Africa, global conversations about AI and elections are relevant, but so too are the peculiarities of a political environment that is still strongly impacted by political party hegemonies. Understanding AI and data in South Africa as largely a process of extraction helps to frame our understanding for intervention in elections as one which expands individual control across the full spectrum of the process, with law and regulation standing as important instruments for expanding effective accountability in an opaque environment.

ABOUT THE AUTHOR

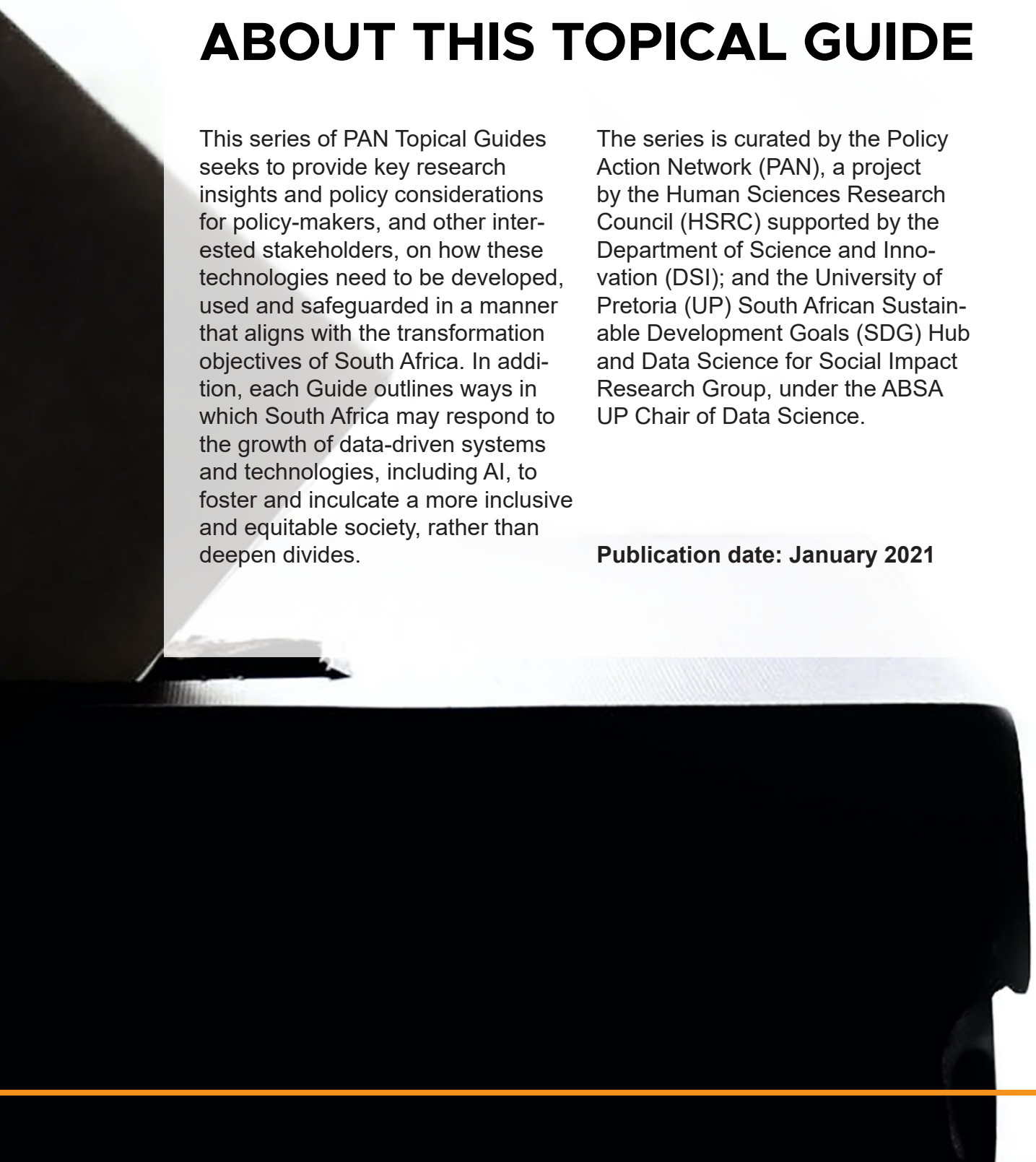
Gabriella Razzano is a Senior Research Fellow at Research ICT Africa, and a Senior Atlantic Fellow in Social and Economic Equality. She is a founding Director of the open data civic tech hub, OpenUp, and is a legal consultant on issues of transparency, open data, privacy, technology and law.

ABOUT THIS TOPICAL GUIDE

This series of PAN Topical Guides seeks to provide key research insights and policy considerations for policy-makers, and other interested stakeholders, on how these technologies need to be developed, used and safeguarded in a manner that aligns with the transformation objectives of South Africa. In addition, each Guide outlines ways in which South Africa may respond to the growth of data-driven systems and technologies, including AI, to foster and inculcate a more inclusive and equitable society, rather than deepen divides.

The series is curated by the Policy Action Network (PAN), a project by the Human Sciences Research Council (HSRC) supported by the Department of Science and Innovation (DSI); and the University of Pretoria (UP) South African Sustainable Development Goals (SDG) Hub and Data Science for Social Impact Research Group, under the ABSA UP Chair of Data Science.

Publication date: January 2021



ELECTIONS, DEMOCRACY AND DIGITAL TECHNOLOGIES IN AFRICA

To participate in a democracy, a citizen votes and the ballot box thus duly stands as the "heart of the…constitutional structure".[1] The South African Constitution notes in its very first provision that the democratic state project is founded on universal suffrage, a national common voters roll, regular elections, and a multi-party system.[2] Elections are prioritised across the globe as the key legitimising political act of democracy.

This primacy has historical roots. The first recorded popular elections saw Spartans voting for the Ephors in 754 B.C. Jump ahead several centuries, however, to new political realities: in 2017 Saudi Arabia gave citizenship to a robot named Sophia[3] and, in the same year, the world's first virtual AI-powered politician was created, called SAM.[4] AI and data-driven applications are now used routinely in election management, and also by political parties to influence voters, from India[5] to Canada.[6]

What does this 'new age' of AI herald for elections in Africa? The conversation about AI and elections has focused primarily on how social media – enhanced by AI-driven mis- and disinformation – might interfere in election results. The truth is that the impact of AI on the political process of elections is potentially far broader, and this breadth needs to be systematically considered in order for effective policy interventions to be designed.

AI as an autonomous system of decision making: AI are computer programmes that mimic human intelligence (human intelligence being understood as reasoning, learning and problem-solving).[7] While AI is the broad encompassing term, machine learning (ML), as an example, is a specific and widely used set of methods that supports this intelligence. AI-driven applications go beyond automated systems that make decisions based on encoded rules and where a certain outcome is assured. Instead, through ML methods, they autonomously adapt their decision-making to new information or data as it is received.[8] In the realm of politics and administrative justice, automated decision-making even in its rules-based (and thus not as autonomous) form is still a technological process of interest – but AI comes with its own particular challenges.

Elections as a system: National (and other) elections can be simply encapsulated by the act of casting a vote for a person to assume a position in political office as a public representative. However, understanding an election as a system can help us to identify the broader spectrum of activities, moments and ways in which AI (as a technology) may intervene in, enhance, or interfere with, that system. Think of elections as a simple narrative whereby: a citizen [stakeholder] makes a decision [action] then casts a vote based on that decision [action], resulting in a vote [asset] being created for a candidate for public office or an official [stakeholder], and this vote is generated [action], stored [action], secured [action] and counted [action]. This vote is verified [action] by the electoral management body (EMB) or others [stakeholder], collated with all votes [action] and then released or published [action]. Of course, this is oversimplified – there may be any number of forms of oversight or verification. What is important to note is that any of those points of action are potential 'leverage points' for AI technologies. They might be used to influence the making of a decision, or enhance storage and counting, or disrupt the nature – integrity – of the asset created. There is a bigger idea at play too: if AI is intelligence, it can theoretically subsume or even assume the role of the stakeholders at any point in the system too. This systems-thinking exercise will help broaden the focus of AI's relationship(s) to elections in Africa, and in South Africa in particular.

AI and data governance: A key relationship is that between AI, data and information broadly, and thus AI's relationship to data governance. For generating intelligence, machine and deep learning rely on massive sets of structured or unstructured data ('big data') to learn from. Data governance considerations related to data quality, provenance, integrity, availability and privacy are then central to both how automated decision-making may influence future electoral processes; but are also relevant to broader information and data questions in this space, such as addressing misinformation. The organising, structuring and presenting of the data into information is a process of influence; and this influence, enhanced by AI, can be the wilful spread of untrue or misleading information (disinformation), or even unintentional falsehoods and untruths (misinformation). Interventions in processing mechanics through data governance frameworks can assist with maintaining the integrity of information in its foundations.

The African electoral context

A re-emerging focus on institutions and structures in the political economy[9] is supporting examinations of elections as a central democratising force in Africa.[10] The role of independent and resourced electoral management bodies (EMBs) as a necessary component of participatory democracy is appropriately emphasised. Yet in spite of growing democratisation across the continent, less than one in six major elections result in a full transfer of power.[11] These outcomes are indications of weaknesses in the 'practice' of elections. Practices which might sway electoral outcomes in Africa, and threaten substantive political legitimacy, include changes to the relevant constitution, weakened electoral oversight mechanisms, intimidation of voters, falsifying of results, or undue challenges to results (amongst others).[12] It is important to note that these challenges are not indications of African exceptionalism (and thus comparative examinations on international discourses on election integrity may be instructive); however, the degree of threats is said to generally be more severe.[13]

At the same time, discussions on electoral integrity are increasingly dominated by questions about the role of social media and threats related to mis- and disinformation. When African EMBs gathered in 2019 to discuss electoral integrity, they did so under the banner of: "Safeguarding Electoral Integrity in the Digital Age: Strategies for Combating Digital Disinformation".[14] African examples of electoral processes potentially impacted by the notorious services of Cambridge Analytica include South Africa, Nigeria and Kenya.[15]

This means that the electoral context is not the only important consideration; so too is the information and communications technology (ICT) and broader digital context for the region. While limited broadband network extension in Africa remains an issue in several countries, coverage is not the only factor determining connectivity and use of the internet. In Lesotho, Rwanda and South Africa, broadband coverage stands at over 98%, and yet significant portions of the population remain unconnected or unable to use the internet in a meaningful way,[16] often because of the unaffordability of services and devices, but also due to low levels of digital literacy.

Internet services are not the only vital component of ICT infrastructure. In many developing countries where electricity supply may be unstable, essential electoral (and other) systems may go offline: the Kenya elections were threatened by the introduction of new electoral systems that struggled with both electricity supply and Internet coverage, meaning a manual back-up voting system had to be relied on.[17]

A final, significant digital challenge is the lack of African-based AI technology developers and governance researchers, which leads to inadequacies in appropriate innovation and digital policy.[18] This reality will become an important focus for contextualising many of the recommendations that follow.

EMERGING POLICY AND PRACTICE

There are law and policy issues of relevance to potential AI-related aspects of elections, but also to data governance issues. EMBs on the African continent have already begun highlighting misinformation and social media as key digital threats to the electoral process.[19] South Africa has also been participating in a collaboration between their EMB, the Independent Electoral Commission (IEC), and the South African civil society organisation Media Monitoring Africa, to maintain a portal[20] for citizen monitoring and reporting of digital disinformation. Nation states have also sought to deal with the disinformation threat more directly through legislation criminalising 'fake news', such as in Ethiopia where a Bill (the Hate Speech and Disinformation Prevention and Suppression Proclamation) on the criminalisation of hate speech and forms of disinformation is being considered.[21]

South Africa has a specific legislative and policy environment in relation to elections and information, more broadly. A central source of electoral information is the voters roll, which has already been the subject of information 'controversy'. The Electoral Act, 1998 in section 16 requires that the voters roll, which includes the personal information of voters, be made accessible on application. While adjudicating on another aspect of the law, in *Electoral Commission v Mhlope*[22] the Constitutional Court considered the role of the voters roll as a public document. In answering the question as to why the collection of addresses in section 16(3) was important, the minority judgement stated "…surely then the availability of addresses on the voters' roll enhances the fairness of elections. The absence of addresses might – not will – result in elections being unfair".[23]

The African Commission Guidelines on Access to Information and Elections,[24] require that an Election Management Body shall proactively provide a:

> *"Voters roll containing information allowing the unique identification of each voter, including the full name, identity number, photograph (where it exists), gender and age of each voter, and any subsequent amendments to this information."*

While the African Commission Guidelines are not binding, it is important to note that the international presumption is toward an open voters roll. Adv. Pansy Tlakula, the current Chairperson of South Africa's data protection authority called the Information Regulator[25] (who was involved in the drafting of the African Commission Guidelines) has begun engagements with the IEC to consider how the balance of data privacy and data access may be implemented in practice.

Outside of this data governance issue, there are specific prohibitions of relevance to disinformation. The Electoral Act, 1998 in s 89(1) states that with respect to certain legally mandated campaign statements, "[n]o person … may make the statement (a) knowing that it is false;

or (b) without believing on reasonable grounds that the statement is true" and in 89 (2), states that "[n]o person may publish any false information with the intention of (a) disrupting or preventing an election; (b) creating hostility or fear in order to influence the conduct or outcome of an election; or (c) influencing the conduct or outcome of an election". The Act also includes an 'Electoral Code of Conduct' to which political parties hoping to contest elections bind themselves; and this Code specifically prohibits parties from publishing false information "in connection with an election in respect of…(i) a party, its candidates, representatives or members; or (ii) a candidate or that candidate's representatives".[26] The Constitutional Court engaged on these sections in *Democratic Alliance v African National Congress and Another*[27] in relation to campaigning messages, and held that a contextual reading of the provision suggested that the kind of false statements prohibited were those that could intrude directly against the practical arrangements and successful operation of an election, not 'information' aimed at influencing its outcome by shaping voters' views about opposing parties. There has been some well-considered criticism that this law is broad, and does not require sufficient mens rea (or criminal intent), considering it is a criminal sanction, for false statements.[28]

Data Governance and AI

Being able to reap the positive benefits of AI presupposes a data governance framework being in place. Lawful data processing frameworks are beginning to emerge in the region, with the European Union General Data Protection Regulations (GDPR) significantly influencing the structure of specific laws (and Bills).[28] South Africa's POPIA, for example, is broadly in keeping with the lawful processing provisions of the GDPR (with two key differences being the creation in POPIA of criminal offences for failures to comply with notices of the Information Regulator, and the extension of data rights to juristic entities).[30]

An important pattern in data protection initiatives in the region is, nevertheless, to fail to empower or properly appoint in due time the independent data protection authority (DPA), the delays in the South African case being demonstrative of this phenomenon.[31] This is an important challenge for enforcement of data processing and protection laws – but is also a particular consideration within the AI context, given the particular role DPAs can play in a challenging technological context: they can offer flexibility and expertise, and also issue regulations that are responsive to sectoral peculiarities, which can help to ease potential compliance burdens on the private sector.

Considering the important role of personal data in both election processes and AI decision-making, cybersecurity is also a fundamental policy area for review. Cybersecurity laws have been adopted in many African countries, such as Malawi, Zambia, and Zimbabwe. In South Africa, the Cybersecurity and Cybercrimes Bill was eventually split, with the Cybercrimes Bill, 2017 currently before the National Assembly for consideration.[31] Yet the Global Cybersecurity Index indicates that only Mauritius, Kenya, Egypt and Rwanda demonstrate a high commitment across all five pillars of their index.[33]

While there are many examples of policy and legislative interventions around the world that deal with aspects of AI, consolidated and comprehensive policy interventions targeted at the technology itself are not common. Some international jurisdictions have explored this option, with Singapore for instance implementing an "AI Governance Framework".[34] These kinds of interventions are typically driven from an economics perspective, particularly considering a digital economy agenda, and therefore provide limited insights into the relationship with governance processes. Nonetheless, emerging policy and practice in a number of regions seeks to mitigate negative aspects of AI and data use in the political sphere as outlined below.

The European Union and the United States on Misinformation

The European Parliament Think Tank summarises[35] a range of actions that the European Union and its member states may adopt in response to the use of personal data for political advertising, including financial sanctions for political parties breaching data protection rules.[36] A special committee for the European Parliament has, for instance, called directly on the larger platforms to take a proactive stance in combatting misinformation, and is under pressure to include sanctions against companies for failures to take adequate action.[37] This approach is underscored by an appreciation of lawful data processing, and the full implementation of the GDPR, as a foundational pillar in regulating the role of AI in elections.[38] Yet beyond the GDPR, there is no European-wide attempt to legislate on mis- and disinformation. A political attitude towards intervention is not matched to a legislative attitude;[39] which relates just as much to the realities of the ability to mandate action, as it does to the broader challenges to regulating in the Internet space. This has not prevented jurisdictions like Germany implementing domestic prohibitions against fake news.[40]

Generally, the United States sees a laissez-faire approach to legislating on issues that may impact free speech; and platforms have been provided with specific forms of limited liability in relation to content moderation in law (limited liability for Internet intermediaries is also replicated in South African law).[41] Whilst there is no country-wide lawful data processing statute, individual states have, however, implemented ad hoc responses to specific technologies.[42] Largely, legislators have sought to exert pressure on platform companies to regulate themselves through content moderation as a salve to misinformation, though political developments under the Trump administration have seen a growing call from both the left and right to institute regulation against platforms as an emerging fora for political contestation.[43]

When we examine patterns in the emerging policy and practice in South Africa in particular, it is noteworthy that there is a tendency to statutorily criminalise ‘undesirable behaviour’, even prior to fully establishing sound data governance frameworks that can extend obligations to creating a sound environment on both public and private sector actors.

Within those statutory forbearances, though, it should be noted that the economic imperatives largely guided by regulation, political imperatives largely driven by policy, and social imperatives largely driven by law, cannot exist in such siloed imaginings with technologies like AI, where the impacts and effects of the technology are so transverse.

RESEARCH PERSPECTIVES

While we have engaged with the existing policy context, the challenges inherent in regulating this environment more broadly will be considered before turning to examine directly the transversal risks (and opportunities) associated with AI in the electoral context.

Challenges in rules and policy

The regulation of emerging technologies is, given their nature, challenging. The Collingridge Paradox notes that efforts to influence or control the further development of technology face a 'double-bind': an information problem (because in emerging technologies the real impacts can't yet be wholly predicted), and a power problem (because control or change is difficult when the technology has become entrenched before regulation or law is in place).[44] This is associated, too, with the law's well-known "pacing problem", which refers to the notion that technological innovation is increasingly outpacing the ability of laws and regulations to keep up.[45] As Larry Downes noted: "technology changes exponentially, but social, economic, and legal systems change incrementally".[46]

These issues are reflected in the AI field, due to the relatively opaque or 'black box' nature of their implementation and recent improvements in hardware enabling rapid increases in data processing. In addition, attempts to regulate AI directly suffer from a fundamental challenge: capability and capacity.[47] The legal and regulatory skill to properly design interventions, coupled with the lack of capability or capacity to monitor once implemented, pose significant inhibitors to meaningful and effective action.

Attempts to then regulate or intervene from a public interest perspective, cognisant of the challenges but unwilling to surrender to techno-determinism, focus strongly on trying to predict potential harms and risks, and engage with those.[48] In considering AI from this perspective, and moving beyond just the underlying data governance challenges, policy questions have considered the impact level of 'decisions' taken by AI for identifying appropriate intervention points (these can be applied more generally to automated decision-making or rules-based systems):

1. Level I decisions will often lead to impacts that are reversible and brief;
2. Level II decisions will often lead to impacts that are likely reversible and short-term;
3. Level III decisions will often lead to impacts that can be difficult to reverse and are ongoing; and
4. Level IV decisions will often lead to impacts that are irreversible and are perpetual.[49]

The focus of policy (and politics) then shifts to examining the most appropriate stage or moment for, and extent of intervention across these levels.

From a legal perspective, Petit suggests that discrete externalities (i.e. impacts) from the effects of AI should be dealt with by merely developing existing legal frameworks.[50] For the kinds of systemic externalities threatened by

AI in the realm of elections, the public interest should drive policy interventions that *ex ante* consider potential impacts, but also *ex post* assess the results of interventions.[51]

Technology, the private sector and power in elections

The role of social media as a mechanism for unduly influencing elections through the spread of mis- and disinformation has now become the popular refrain for understanding technological shifts in political influence.[52] This is, however, an about-turn from the discourse that originally celebrated new media as a mechanism for enhancing democracy (with the oft-cited 'Arab Spring' connections), which built on our more traditional associations between democracy and freedom of expression.[53] The proliferation of information now accessible, whether true or untrue, has started to shift notions on rights such as freedom of expression and access to information, which were based more on concerns about information deficits rather than information gluts. 'Undue influence' by social media in terms of electoral integrity can also be associated with two broader political developments: the rise in the use of soft power as a mechanism for creating change, and the rising centrality of information as power in the digital age.[54]

It is perhaps unsurprising then, with this convergence of digital political attributes, that such significant energy is expended on considering the role of emerging technologies in contributing further to the negative aspects of these two shifts. As an emerging threat, not only does AI expand the capacity of automated algorithms and digital 'bots', amongst others, to influence the feed (i.e. the ready availability) of political mis- and disinformation on social media, but the emergence of 'deep fakes' and 'synthetic media' (i.e. disinformation) facilitated by AI only goes further to undermine social media as a sound and reliable civic space for engaging in political life.[55] People cannot trust what they see, read, or hear.

Yet the drivers of this role in mis- and disinformation for technology do not stem from the technology itself, but the social, political and economic forces at play more broadly. Investigations into media influence in elections has necessarily considered the role of the social media platforms themselves in facilitating this influence.[56] Regulation of social media platforms is a notable challenge for the digital age more broadly, not least because of the massive monopolisation of the digital market by such platforms, and the shifts in political power associated with it.[57] As seen in the European Union and United States examples above, differing attitudes to private sector responsibilities nevertheless seem to result in the same inability to control the influence of the private sector in the field. This has meant significant focus, particularly in Western discussions, on how to regulate (or not regulate) these platforms in a manner that achieves better quality outcomes, i.e. outcomes based on facts. Significant portions of the Kofi Annan Commission Report on "Protecting Electoral Integrity in the Digital Age" focus on the need for platforms themselves to take greater proactive action in combating misinformation and disinformation through enhanced transparency, and initiatives like 'early warning' detection.[58]

The social pressure on platforms to intervene actively in either moderating, or labelling, both mis- and disinformation has grown in recent months.[59] However, approaches by the different tech platforms to content related to elections have been influenced by many things – depending for instance on their own internal political culture, media coverage, and forms of government pressure (consider for instance Trump's particular focus on Twitter's content moderation).[60] Relying on platforms alone to be the 'new governors' of content surrenders these decisions to being largely founded on economic imperatives,[61] which may not be congruent with the broader public interest. When responding to calls on Facebook to take a more active stance in intervening in disinformation, Mark Zuckerberg stated that: "Facebook shouldn't be the arbiter of truth".[62] Yet, when we think about it from the perspective of content 'moderation' the very problem is that platforms do not treat all content as equal, and algorithms and other interventionist mechanisms actively collate and curate content for its consumers. Discerning the truth is becoming more challenging in the information age. A fundamental challenge in the context of misinformation remains the

transparency and accountability of the various actors and outcomes involved - from the algorithms used, to decisions about content.[63]

These attempts at establishing a 'positive obligation' (whether through law or 'ethics') will continue in debates on AI regulation. Private sector AI developers and service providers will have a role to play in the very early detection, and 'equality by design' solutions that may be posited for helping prevent the spread of mis- and disinformation. The shifts in power and impact to the private sector - and greater appreciation of connections between social, political and economic impacts – mean that positive obligations to perform things like social impact studies before AI technologies are introduced within a system, are likely to become established as important, and necessary, interventions.[64] In the context of AI these actions will need to become a lot more pre-emptive and less reactionary, as we have seen in shifting content moderation policy as an example, and as we learn more about the reality of the risks and harms. Directly addressing the social environment and impact prior to and after implementation becomes a necessary expansion of due diligence obligations.[65]

Political realities in South Africa

The political debates that arise from Western media and academia are influenced by two key global political realities. First, is the 'competition' between the United States' laissez-faire approach to regulation, versus the European interventionist approach; and second is the fact that the major digital oligopolies exist in the United States or China (with European markets fighting for space in between the two).[66] While 'data colonialism'[67] is its own data governance challenge of relevance, there is an additional direct contextual concern: the dominant state and political hegemonies which exist as a reality of the African context not necessarily the same as those of the United States, China or Europe. The role of political parties in threatening electoral integrity should not be lost while we focus on this tech-centric debate: in South Africa and Kenya the private sector services of Bell Pottinger and Cambridge Analytica, respectively, in 'influencing' social media feeds were associated with the governing parties.[68]

Responsibilities must be placed directly on to political parties (which should be linked to their ability to contest elections) to not only refrain from mis- and disinformation activities, but also to proactively police the environment.[69] Political parties stand at a significant nexus of power and control in relation to African electoral integrity.

An examination of the power hegemonies in the region also necessitate a constant vigilance, lest an 'unrealistic' focus on the domestic threat of mis- and disinformation is used by states to suppress legitimate dissent, or political and civic discourse.[70] Many of the threats facing electoral integrity in Africa are offline;[71] big data analysis, algorithms and AI are feeding into existing challenges in relation to electoral integrity, which should be the primary focus of interventions.

This caution about an unbalanced focus on digital discourse is echoed when considering the role of the electorate in African societies. In reflecting on the role of mis- and disinformation in elections, which in fact has a historical legacy well preceding the internet, it has been noted that in order to 'activate' any kind of disruption, mis- or disinformation has to: "…hit at pre-existing tendencies and pathologies in society: disaffection, inequality, prejudice, aggression".[72] Yet, thinking about the role of soft power in influencing an electorate, as more and more civic and political activity is conducted online, the particular African context of 'passive' consumption of content, and lower levels of digital literacy, will become increasingly relevant until these characteristics change.[73] How will people fresh to the online space be able to critically engage in the world of deep fakes and synthetic media? How can they 'discern' truth in opaquely curated digital environments? Digital education has become a priority point of intervention. Here, AI itself may be effectively used to clearly identify and delineate the source and provenance of content to help people navigate the online 'infoverse'. This dimension of self-/regulation is a priority challenge because "…the power [of data-driven behavioural economics on platforms] is soft, imperceptible, cheap and ubiquitous, we don't resist it".[74]

The role of AI and data in the electoral system

There are broader challenges that arise in the context of AI, which bear considering when looking to the full breadth of influence that can be exerted across the electoral process. The ability of AI to take decisions and actions 'independently', means that its "…[v]erdicts…land like dictates from the algorithmic gods".[75] Particularly in the context of machine learning, the 'black box' of decision-making (where data goes in and comes out, but we have little oversight of the process in-between) is a considerable concern in AI and data governance conversations.[76] If inclusion of AI within digital voting systems is contemplated, particularly the significant level of impact of a decision in relation to political outcome and legitimacy, it appears completely unjustifiable to ever include anything that is not interpretable or open to scrutiny.[77] Political legitimacy is traditionally founded on transparency and visibility; considering AI within the context of elections puts debates concerning the necessity for transparency and accountability in AI into hyper-drive regardless of where in the process it may be involved.[78]

This decision-making capacity of AI is not just about transparency for appearances' sake, but is also necessary given the risks of exclusion associated with algorithmic decision-making (that extends to AI decisions). The ability to analyse large amounts of data is facilitated by algorithms and formulas – but the opacity of these algorithms presents challenges, both in terms of the outputs of the algorithms (for instance, content limitations on information such as in newsfeeds) and decisions made through them (and their ability to perpetuate bias).[79] Bias can be introduced through the data used, assumptions used, or even within the formula design choices. And the opacity in relation to algorithms can be both technical and proprietary (i.e. restrained due to commercial interests).[80] How these systems then get incorporated within electoral processes, especially given the fundamental importance of notions of suffrage, elections and democracy, mean transparency must be at the forefront of planning – but also that the service providers involved stand as important agents of obligation and responsibility.[81] Even the simple digitalisation of voting machines has led to risks of exclusion from existing elections.[82]

The digitalisation of the electoral process (even as seen in the voting machines) may present another opportunity for AI intervention.[83] It cannot be discounted that AI applications could be taught to make subtle adjustments to vote totals (so subtle that it would be statistically challenging to decipher them).[84] Concerns such as this arise with the emergence of digitalisation (such as voters' identity document scanners in South Africa) even before full AI introduction: and that is the importance and centrality of cybersecurity frameworks, and their concerted implementation, as a prerequisite to the expansion of the role of emerging technologies within our electoral processes. Cybersecurity should be a priority for EMBs as an essential step for ensuring electoral integrity, and the reality of the forms of 'herd immunisation' needed to properly combat cybersecurity threats, means this should be prioritised across the public sector concerned (given its associated information systems), but also at a regional level (to help manage geopolitical forces like cyberwarfare).[85]

A final point to consider when looking not just at the actions within an electoral system, but also at the actors, is the future of AI in politics as something more than just about the action of voting. For example, the ability of AI to examine big data regarding voter sentiment may be an opportunity for politicians to be more responsive to their electorate.[86] What if AI is able to render itself as a political actor, as seen in SAM as an extreme example?[87] AI may also help to base policy decisions more on data and evidence than is currently possible.[88] Ultimately, the opportunity in AI will be its ability to sort through and organise the very gluts of data currently derailing notions of 'political truth'.

RECOMMENDATIONS FOR POLICY AND PRACTICE

A considered reflection of the electoral process provides insights into key learnings in the context of AI. The first is that one cannot separate investigations into the regulation of AI from questions arising from the regulation of data more broadly, even though AI has its own additional peculiarities. This means that data governance emerges as a first-order priority.

In addition, appreciating the potential impact of AI is important for achieving a balanced response to regulation: but in order to do so, the impacts must be considered across the full spectrum of the democratic process. This results in a necessary acknowledgement, when seeking to intervene in the digital space, of both complexity and context.

In South Africa, we are still the subjects rather than creators of AI. When we consider this within the context of 'digital colonialism' (and the removal of data and value for the benefit of foreign companies) alongside the passive consumption of content in our digital economy, it is clear that a phenomenon of extraction is taking place, spurred by dynamics from emerging technologies. A fundamental step for preventing this and other negative impacts of AI is to establish a degree of control. Given the urgency of ensuring equality, privacy and fairness by design, it should be clear that in order to be beneficiaries of AI technologies – and not just 'subject' to their impacts – investing in digital industrial policy that supports the domestic realisation of AI is a necessary progressive step.

Transparency and accountability in relation to algorithmic decision-making and AI become priorities that need to be obliged for both private sector and public sector actors that exert influence within the electoral system. Power is influence, and the challenge of an age of soft power is the opacity of it – AI and algorithms add a further layer of 'detachment' from accountability that we cannot countenance in our elections. We should use law and regulation to explicitly assign accountability, and mandate transparency. Yet what transparency means is perhaps what is being altered the most: in an age of information glut, determining effective transparency may be a key political challenge.

Additionally, future challenges in AI, given the demonstrated complexity, will be resolved only through 'multi-stakeholderism', and regional and global governance approaches being met alongside their domestication. This will require ensuring that African countries are at the table.

AI can be seen as a challenge to democratic practices, but not an insurmountable one.[89] In considering AI and electoral integrity, the following recommendations can be posited:

Recommendations in relation to narrative (applicable across stakeholders):

1 Techno-determinism should be avoided. The introduction of any one technology is not inevitable, nor is the incorporation of their negative impacts. Policy and design can intervene within these systems.

2 Broader social, political and economic forces should be examined to understand the potential impacts of technologies within existing social and institutional arrangements, and also for shaping the priorities for technological intervention itself.

3 Threats to electoral integrity are shaped by existing political hegemonies, which include challenges like political party funding, and institutional capacity and oversight.

Recommendations for policymakers:

1 In determining priorities for managing potential AI impacts, the focus should be on laying the foundations for sound data governance broadly.

2 This data governance should include data processing, data access (and transparency), and cybersecurity imperatives.

3 In South Africa, the Office of the Information Regulator stands as a central agency for building effective and capacitated interventions on AI in elections. A priority should be the development of guidance notes alongside the IEC, ahead of the municipal elections. These guidance notes should cover the full range of data and AI issues for elections.

4 In considering the regulation of AI, the potential level of impact should inform strategies that have both ex ante and ex post policy responses.

5 AI regulation must include establishing the conditions for the domestic emergence of AI technologies and solutions to combat many of the inherent inadequacies in adopted technologies that result in the extraction of both value and agency (a fundamental component of civic action).

6 African policymakers should engage in associated global governance processes, while constructing policy responsive to regional and local contexts.

Recommendations for lawmakers:

1 As challenging as emerging technologies can be for lawmakers, existing frameworks should be leveraged that incorporate consideration of social, political and economic impacts (which is why human rights standards serve as such a powerful tool for guiding law-making in this area).

2 South Africa's emphasis on criminalisation should shift instead to focusing on supporting the principle-based regulation of its nascent lawful data processing regime, which includes capacity for the Office of the Information Regulator, given the realities of our social and political context for elections.

3 Regulation of AI should be pursued to help achieve a balance between constraint and innovation, whilst also addressing capacity and capability.

4 Given the central role of elections in establishing state legitimacy and government accountability, and the potential impacts of AI, a high priority must be placed on transparency within the technologies adopted or adapted, which extends to the creation of obligations for it.

5 Given this role of elections, and the potential impacts of AI, a high priority must be placed on creating appropriate obligations on the full range of actors involved across the electoral-technology process.

Recommendations for electoral implementers (including the IEC):

1 An immediate focus should be placed on ensuring the security of the full electoral process both offline and online. Electoral integrity requires institutional preparedness.

2 Political actors must be prioritised as a site of intervention given their role in helping to ensure electoral integrity.

3 A realistic consideration of the digital environment should inform the decision of what technologies to adopt and adapt within the electoral process.

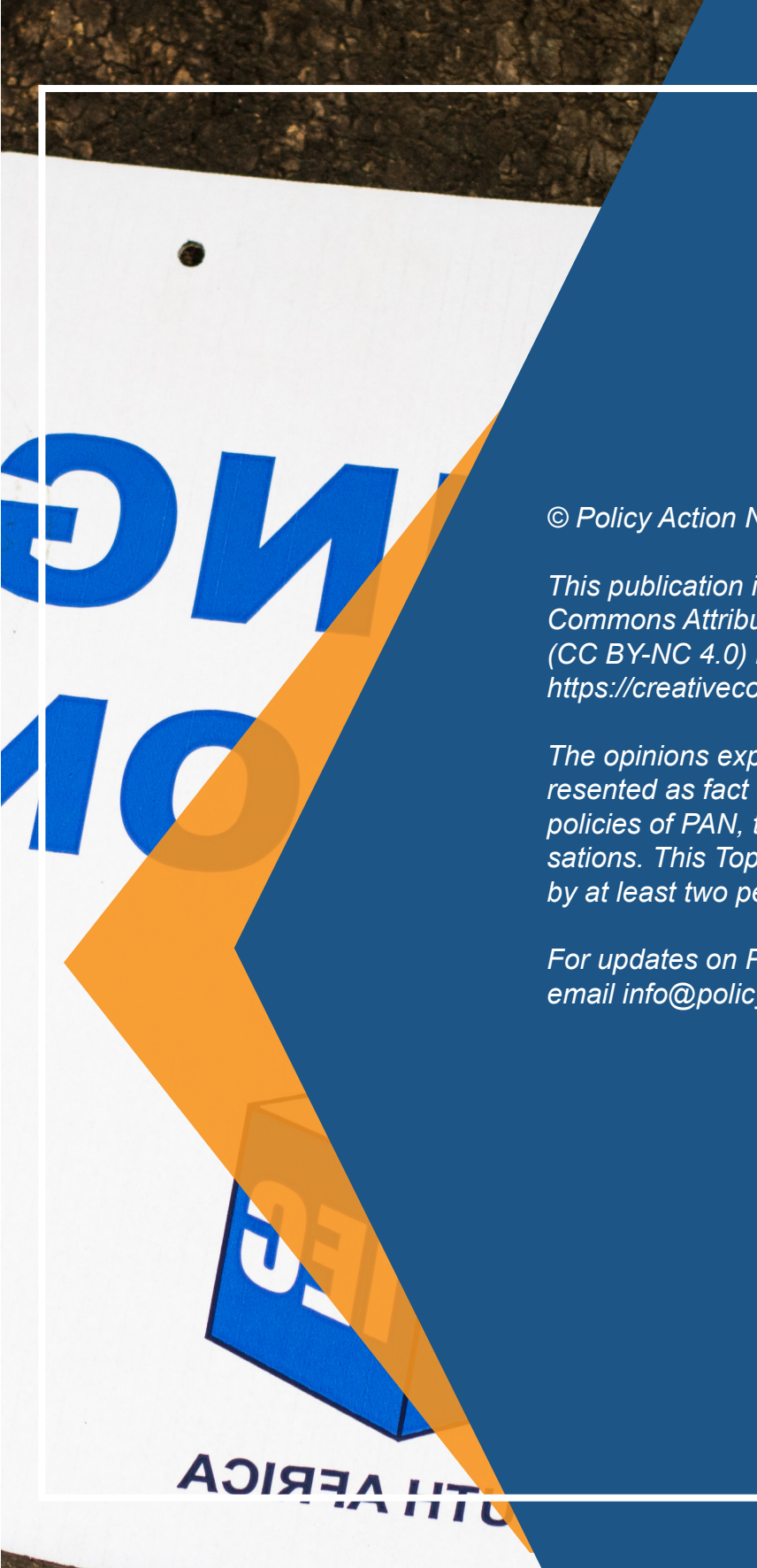
4 The role of EMBs in ensuring adequate civic education, which necessarily includes digital literacy components, is central, and in South Africa would mean expanding the existing Real411 programme, amongst others.

REFERENCES

[1] Harvard Law Review. 2018. Of Ballot Boxes and Bank Accounts: Rationalizing the Jurisprudence of Political Participation and Democratic Integrity. Harvard Law Review, 131: 1443–64.
[2] Constitution of the Republic of South Africa, 1996, Section 1.
[3] Reynolds, E. 2018. The agony of Sophia, the world's first robot citizen condemned to a lifeless career in marketing. Wired. June 1. https://www.wired.co.uk/article/sophia-robot-citizen-womens-rights-detriot-become-human-hanson-robotics
[4] Sarmah, H. 2019. World's First AI-powered Virtual Politician SAM Joins The Electoral Race In New Zealand. Analytics India Magazine. January 28. https://analyticsindiamag.com/worlds-first-ai-powered-virtual-politician-sam-joins-the-electoral-race-in-new-zealand/. As an introduction to the technology, SAM is an AI-powered chatbot – connected to social media - used to gather data (and desires) from citizens, which data is hoped can directly feed into policy positions taken.
[5] For example, see Dasgupta, B. 2020. BJP's deepfake videos trigger new worry over AI use in political campaigns. Hindustan Times. September 21. https://www.hindustantimes.com/india-news/bjp-s-deepfake-videos-trigger-new-worry-over-ai-use-in-political-campaigns/story-6WPlFtMAOaepkwdybm8b1O.html and Srivastava, S. 2019. Indian General Election 2019: How Big Data Is Influencing Voters' Psychology. Analytics Insight. April 16. https://www.analyticsinsight.net/indian-general-election-2019-how-big-data-is-influencing-voters-psychology/
[6] Pinkerton, C. 2018. Elections Canada will use AI to fight disinformation on social media. iPolitics. November 2. https://ipolitics.ca/2018/11/02/elections-canada-will-use-ai-to-fight-disinformation-on-social-media/
[7] PricewaterhouseCoopers. 2017. Bot.Me: A revolutionary partnership. Consumer Intelligence Series. http://www.pwc.in/assets/pdfs/consulting/digital-enablement-advisory1/pwc-botme-booklet.pdf.
[8] Hong Chang, M. and Kuen, H. C. 2019. Towards a Digital Government: Reflections on Automated Decision-Making and the Principles of Administrative Justice. Singapore Academy of Law Journal, 31 (2): 875–906.
[9] See for instance Acemoglu, D. and Robinson, J. A. 2012. Why Nations Fail. Crown Publishing Group: United States.
[10] Southall, R. 2018. Electoral Systems and Democratization. In Daniel, J. and Southall, R. (eds.), Voting for Democracy: Watershed Elections in Contemporary Anglophone Africa. Routledge: New York.
[11] Ronceray, M. and Byiers, B. 2019. Elections in Africa – Playing the game or bending the rules? ECDPM, Discussion Paper No. 261 https://ecdpm.org/wp-content/uploads/Elections-Africa-Playing-Game-Bending-Rules-ECDPM-Discussion-Paper-261.pdf.
[12] See above: Ronceray, M. and Byiers, B. 2019.
[13] Groemping, M. and Martinez i Coma, F. 2015. Electoral Integrity in Africa. Electoral Integrity Project. https://www.electoralintegrityproject.com/electoral-integrity-in-africa.
[14] Gibaja, A. 2020. Are Elections and Politics in Africa Ready to Cope with the Influence of Social Media? International IDEA. March 11. https://www.idea.int/news-media/news/are-elections-and-politics-africa-ready-cope-influence-social-media
[15] Solomon, S. 2018. Cambridge Analytica Played Roles in Multiple African Elections. Voice of America - English https://www.voanews.com/africa/cambridge-analytica-played-roles-multiple-african-elections.
[16] Gillwald, A. and Mothobi, O. 2019. A Demand-Side View Of Mobile Internet From 10 African Countries. Policy Paper, Series 5: After Access - Assessing Digital Inequality in Africa (Research ICT Africa, April 2019), https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf
[17] Privacy International. 2013. Biometrics: Friend or Foe of Privacy? https://privacyinternational.org/news-analysis/1409/biometrics-friend-or-foe-privacy
[18] Bradshaw, N. 2020. Artificial Intelligence in Africa - Will 2020 Be a Tipping Point for African AI ? AI Expo Africa - Africa's Largest B2B Trade Focused AI Event (blog). http://aiexpoafrica.com/2020/01/06/artificial-intelligence-africa-will-2020-tipping-point-african-ai/
[19] See above: Gibaja, 2020.
[20] Real411. Keeping it real in digital media. https://elections.real411.org.za/learn.
[21] Meseret, E. 2020. Hate Speech and Disinformation Concerns Escalate in Ethiopia. Devex. May 6. https://www.devex.com/news/sponsored/hate-speech-and-disinformation-concerns-escalate-in-ethiopia-97095
[22] Electoral Commission v Mhlope and Others (CCT55/16). 2016. ZACC 15; 2016 (8) BCLR 987 (CC); 2016 (5) SA 1 (CC). June 14. http://www.saflii.org/za/cases/ZACC/2016/15.html
[23] See above: Electoral Commission v Mhlope and Others. 2016 at para 19.

[24] See p.17 in African Commission on Human and Peoples' Rights. 2015. Guidelines on Access to Information and Elections. https://www.achpr.org/public/Document/file/English/guidelines_on_access_to_information_and_elections_in_africa_eng.pdf
[25] Razzano, G., van der Spuy, A. and Rens, A. 2020. Waiting for POPIA. Research ICT Africa (blog). June 24. https://researchictafrica.net/2020/06/24/waiting-for-popia/. The Office of the Information Regulator was established by the Protection of Personal Information Act, 2013 (POPIA) to oversee data privacy and information access in South Africa. However, though the Chairperson was appointed in 2017, the Act has only become fully effective from 1 July 2020.
[26] Electoral Act, 1998, Schedule 2, section 9 (2).
[27] Democratic Alliance v African National Congress and Another (CCT 76/14). 2015. ZACC 1; 2015 (2) SA 232 (CC); 2015 (3) BCLR 298 (CC). January 19. http://www.saflii.org/za/cases/ZACC/2015/1.html
[28] Stephanopoulos, N. 2016. Liable Lies. Constitutional Court Review 8. https://journals.co.za/content/journal/10520/EJC-108572b67e?crawler=true&mimeType=application%2Fpdf
[29] There is a useful civil society project tracking the state of domestic data protection frameworks here: https://dataprotection.africa/
[30] Giles, J. 2020. GDPR vs POPIA | Compare the GDPR with the POPI Act? Michalsons (blog), February 13. https://www.michalsons.com/blog/gdpr-mean-popi-act/19959
[31] Greenleaf, G. 2011. Independence of Data Privacy Authorities: International Standards and Asia-Pacific Experience. Computer Law & Security Review. U. of Edinburgh School of Law Working Paper, 18, no. 1 & 2
[32] Moyo, A. 2018. Fake News Too Hot to Handle for Cyber Crimes Bill. ITWeb. November 1. https://www.itweb.co.za/content/P3gQ2MGXQ4dqnRD1. Initial attempts within the draft to broadly criminalise 'fake news' have been partially backtracked on.
[33] ITU. 2018. Global Cybersecurity Index. https://www.itu.int/pub/D-STR-GCI.01-2018
[34] See above: Hong Chang, M. and Kuen, H. C. 2019.
[35] European Parliament Think Tank. 2019. Artificial intelligence, data protection and elections https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2019)637952
[36] European Commission. 2018. State of the Union 2018: European Commission proposes measures for securing free and fair European elections https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5681
[37] DW. 2020. EU Takes Action against Fake News. DW. September. https://www.dw.com/en/eu-takes-action-against-fake-news/a-55056541
[38] See above: European Parliament Think Tank. 2019.
[39] Scott, M. 2019. Europe's Failure on "Fake News". Politico. May 23. https://www.politico.eu/article/europe-elections-fake-news-facebook-russia-disinformation-twitter-hate-speech/
[40] Gesley, J. 2019. Germany: Facebook Found in Violation of "Anti-Fake News" Law. Global Legal Monitor. August 20. www.loc.gov/law/foreign-news/article/germany-facebook-found-in-violation-of-anti-fake-news-law/
[41] Wiener, A. 2020. Trump, Twitter, Facebook, and the Future of Online Speech. The New Yorker. July 6. https://www.newyorker.com/news/letter-from-silicon-valley/trump-twitter-facebook-and-the-future-of-online-speech
[42] Toto, C. S. and Keating, T. 2020. Protecting Elections: Regulating Deepfakes in Politics. Pillsbury. August 6. https://www.internetandtechnologylaw.com/elections-deepfakes-politics-regulation/
[43] Thierer, A. 2018. The Pacing Problem, the Collingridge Dilemma & Technological Determinism. Technology Liberation Front, August 16. https://techliberation.com/2018/08/16/the-pacing-problem-the-collingridge-dilemma-technological-determinism/
[44] Petit, N. 2017. Law and Regulation of Artificial Intelligence and Robots - Conceptual Framework and Normative Implications. SSRN Scholarly Paper https://doi.org/10.2139/ssrn.2931339
[45] Future Today Institute. 2020. Tech Trends Report 2020. http://futuretodayinstitute.com/2020-tech-trends/
[46] See above: Thierer, A. 2018.
[47] Spencer. M. 2019. Artificial Intelligence Regulation May Be Impossible. March 02. https://www.forbes.com/sites/cognitiveworld/2019/03/02/artificial-intelligence-regulation-will-be-impossible/#4814b3b011ed.
[48] See above: Petit, N. 2017.
[49] See above: Hong Chang, M. and Kuen, H. C. 2019.
[50] See above: Petit, N. 2017. In particular, through rules in relation to property & liability, contract laws and the court system.
[51] See above: Petit, N. 2017.
[52] Kamarck, E. 2018. Malevolent Soft Power, AI, and the Threat to Democracy. Brookings (blog). November 29. https://www.brookings.edu/research/malevolent-soft-power-ai-and-the-threat-to-democracy/
[53] See above: Kamarck, E. 2018.
[54] Satell, G. How Technology Is Creating New Sources Of Power. Forbes. October 19. https://www.forbes.com/sites/gregsatell/2014/10/19/how-technology-is-creating-new-sources-of-power/#2b6a124324ed
[55] See above: Future Today Institute. 2020.
[56] Kofi Annan Commission. 2020. Protecting Electoral Integrity in the Digital Age. The Report of the Kofi

Annan Commission on Elections and Democracy in the Digital Age. January. https://www.kofiannanfoundation.org/app/uploads/2020/01/f035dd8e-kaf_kacedda_report_2019_web.pdf
[57] Thieulin, B. 2019. Towards a European Digital Sovereignty Policy. Economic, Social and Environmental Council. March. https://www.lecese.fr/en/publications/towards-european-digital-sovereignty-policy
[58] See above: Kofi Annan Commission. 2020.
[59] See above: Wiener, A. 2020.
[60] Klonick, K. 2018. The New Governors: The People, Rules, and Processes Governing Online Speech. Harv. L. Rev. 131: 1598.
[61] See above: Wiener, A. 2020.
[62] Filloux, F. 2020. The Strange Notion of "Arbiter of Truth". Monday Note. June 7. https://mondaynote.com/the-strange-notion-of-arbiter-of-truth-45d9f50bae72
[63] See above: Klonick, K. 2018.
[64] Crawford, K. and Calo, R. 2016. There Is a Blind Spot in AI Research. Nature News 538 (7625): 311
[65] Kolabhai, R. 2020. Human Rights Obligations and South African Companies: A Transformative Approach. https://scholar.sun.ac.za/handle/10019.1/108152.
[66] See above: Thieulin, B. 2019.
[67] Couldry, N. and Mejias, U. 2018. Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. SAGE Publications. https://eprints.lse.ac.uk/89511/1/Couldry_Data-colonialism_Accepted.pdf; van der Spuy, A. 2020. Colonising Ourselves? An Introduction to Data Colonialism. March 23. https://researchictafrica.net/2020/03/23/colonising-ourselves-an-introduction-to-data-colonialism/
[68] Warah, R. 2019. Cambridge Analytica and the 2017 Elections: Why Has the Kenyan Media Remained Silent?The Elephant (blog). August 9. https://www.theelephant.info/features/2019/08/09/cambridge-analytica-and-the-2017-elections-why-has-the-kenyan-media-remained-silent/; Shoba, S. Bell Pottinger Exposed: Influence unpacks the evils of disinformation. Daily Maverick. August 21. https://www.dailymaverick.co.za/article/2020-08-21-bell-pottinger-exposed-influence-unpacks-the-evils-of-disinformation/
[69] See above: Kofi Annan Commission. 2020.
[70] See above: Meseret, E. 2020.
[71] See above: Groemping, M. and Martinez i Coma, F. 2015
[72] Yaffa, J. 2020. Is Russian Meddling as Dangerous as We Think? The New Yorker. https://www.newyorker.com/magazine/2020/09/14/is-russian-meddling-as-dangerous-as-we-think
[73] See above: Gillwald, A. and Mothobi, O. 2019
[74] Boyte, H. 2017. John Dewey and Citizen Politics: How Democracy Can Survive Artificial Intelligence and the Credo of Efficiency. Education & Culture 33 (2): 13–47.
[75] Cathy O'Neill, quoted in: Boyte, H. 2017.
[76] Pasquale, F. 2015.The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press. https://www.jstor.org/stable/j.ctt13x0hch
[77] Rudin, C. Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead. ArXiv:1811.10154 [Cs, Stat] http://arxiv.org/abs/1811.10154
[78] Wachter, S. and Mittelstadt, B.D. 2018. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. Columbia Business Law Review.
[79] Comninos, A. and Konzett, M. 2018. FABRICS: Emerging Artificial Intelligence Readiness. Martin Konzett KG: Zell am Moos. https://vous.ai/FABRICS-Emerging-AI-Readiness-Comninos-Konzett-First-Edition-2018-LQ.pdf
[80] See above: Comninos, A. and Konzett, M. 2018.
[81] Oliver, J. 2019. Voting Machines. Last Week Tonight with John Oliver. HBO. https://www.youtube.com/watch?v=svEuG_ekNT0; See above: Kofi Annan Commission, 2020.
[82] See above: Oliver, J. 2019.
[83] See above: Oliver, J. 2019.
[84] See above: Kamarck, E. 2018.
[85] Calandro, E. and Berglund, N. 2019. Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: The SADC Case. Internet Governance Forum, Berlin, Germany, November 25; Dawson, F. Herd Immunisation in Cyber Security. KDC Resource. March 21. https://www.kdcresource.com/blog/2019/03/herd-immunisation-in-cyber-security
[86] Niyazov, S. 2020. A.I. Will Mark A Turning Point in the History of Politics. Towards Data Science. February 11. https://towardsdatascience.com/a-i-will-mark-a-turning-point-in-the-history-of-politics-e78e-4a961e69
[87] See above: Sarmah, H. 2019
[88] See above: Niyazov, S. 2020.
[89] See above: Boyte, H. 2017.



For updates on PAN, please follow @PolicyActionZA or email info@policyaction.org.za.