Journal of African Law, 65, 3 (2021), 351–375 © The Author(s), 2021. Published by Cambridge University Press on behalf of SOAS University of London.
doi:10.1017/S0021855321000322 First published online 21 September 2021

On Disinformation, Elections and Ethiopian Law

Kinfe Micheal Yilma*
Addis Ababa University, Addis Ababa, Ethiopia
E-mail: kinfe.yilma@aau.edu.et; kinfeyilma@gmail.com

Abstract

Disinformation has become a formidable challenge to the integrity of electoral processes as well as the internal political stability of many countries. This state of affairs has spurred a wave of new regulatory measures in several countries. From stringent rules governing dissemination of political advertisements via social media platforms to media literacy programmes, the past few years saw the introduction of legislative and non-legislative measures in many jurisdictions. Ethiopia is no exception in introducing measures to address the problem. This article examines Ethiopia's policy responses towards addressing the impact of disinformation on the integrity and credibility of elections. It argues that measures taken thus far in Ethiopia appear to address the impact of disinformation on national security and social harmony. As such, Ethiopia has not taken tailored measures to address the impact of disinformation on its democratic aspirations, particularly in holding free, fair and democratic elections.

Keywords

Elections, disinformation, fake news, social media, democracy, Ethiopia

INTRODUCTION

Disinformation has come to be one of the most consequential problems in the digital environment. While not entirely a new phenomenon, the proliferation of misleading information and conspiracy theories has grown exponentially and proven dangerous in the past few years. With increasing access to the internet worldwide and the prominence of social media platforms, disinformation is probably one of the greatest challenges to the global political economy in the 21st century. From Brexit – in which the "leave" campaign allegedly circulated information that misled voters[1] – to the 2016 United

* Assistant Professor of Law, Addis Ababa University Law School, Ethiopia. The author gratefully thanks his colleagues Kokebe Wolde and Halefom Hailu Abraha for comments on the earlier versions of the article. After this article went to press in early May 2021, Ethiopia held highly disputed general elections in most parts of the country on 21 June 2021, however this article has considered developments only up until 10 May 2021.

1 See, e.g., "EU-bashing stories are misleading voters – here are eight of the most toxic tales" (19 May 2016) *The Guardian*, available at: <http://bit.ly/1TgGcXB> (last accessed 20 February 2021).

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

States (US) presidential elections,[2] elections, electoral processes and democratic institutions have, in particular, become targets of disinformation over recent years. To counter the spread of disinformation online as well as offline, the past few years have seen a wave of regulatory responses worldwide. A closer examination of these regulatory responses signals a stark difference in approach between countries, particularly regarding the underlying objectives of regulatory responses. Guarding the integrity of electoral processes and democratic institutions has been the prime concern of disinformation regulation in some countries. This is best illustrated by multi-pronged responses to election disinformation in Australia, Canada, France, India, the US and Sweden,[3] whereas guarding national security and ensuring social harmony has been the prime objective of disinformation regulation in other countries such as Egypt, Uganda and Tanzania.[4]

Ethiopia has not been immune to the scourge of disinformation. Despite the limited level of internet penetration in the country, the spread of disinformation is increasingly becoming common and consequential. The magnitude of the problem has intensified since the public protests in late 2015.[5] Two current developments are, however, bound to further exacerbate the problem in Ethiopia. One key factor relates to the overall liberalization efforts such as the opening of the telecom and media sectors. One objective of the ongoing telecom liberalization is to increase the level of internet use and penetration. More access would bring with it the risk of wider circulation of false rumours and conspiracy theories. A second objective, but more concerning, is the impending national elections and the attendant polarization of politics. While Ethiopia's political environment is typically polarized, it is increasingly becoming more consequential, with social media being a key medium of political mobilization. But the controversial postponement of the elections and extension of the term of the parliament due to the pandemic are likely to precipitate further disinformation. With the elections now slated to be held in June 2021, the problem of disinformation is likely to be greater during the election cycle.

---

2 See generally, "Joint statement from the Department of Homeland Security and Office of the Director of National Intelligence on election security" (2016), available at: <https://bit.ly/32aRJAI> (last accessed 20 February 2021).

3 For a summary of regulatory responses in these nations, see "Government responses to disinformation on social media platforms" (September 2020) *Library of Congress*, available at: <https://www.loc.gov/law/help/social-media-disinformation/> (last accessed 20 February 2021).

4 For a summary of regulatory responses in Egypt, see "Government responses to disinformation on social media platforms: Egypt" (September 2020) *Library of Congress*, available at: <https://www.loc.gov/law/help/social-media-disinformation/egypt.php> (last accessed 20 February 2021).

5 For more on this, see KM Yilma "Fake news and its discontent in Ethiopia" (2017) 5/1 *Mekelle University Law Journal* 98 at 102–5.

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

This article examines the extent to which, and whether, Ethiopia has taken measures to address the risks of disinformation to its fledgling democracy. In particular, it considers the question of whether or not the current Ethiopian legal and policy framework is well equipped to address this problem in light of the impending general elections and referenda for internal self-determination of peoples. It argues that Ethiopia has not taken specific tailored measures to address the risks of disinformation to its democratic aspirations, particularly in holding free, fair and democratic elections. Regulatory measures taken thus far to tackle disinformation generally, such as enactment of disinformation legislation, or commonly taken extra-legal measures, such as internet shutdowns, seek to protect national security and enhance social harmony, as opposed to ensuring the credibility of electoral processes.

For the purposes of this article, the term "disinformation" represents information that is meant to mislead. Therefore, it is meant to embrace all types of deliberately misleading information regardless of truth in its content or whether it is packaged as "news". This is not just for the purpose of semantic accuracy, but also because the idea of falsity or falsehood is too problematic to serve as a basis for any serious regulatory effort or scholarly scrutiny. Falsity – and for that matter truth – has no fixed meaning. A piece of given information may either be entirely false, partially false, visually false, contextually false or even essentially false.[6] Given such fluidity in meaning, competing notions of misinformation and "fake news" are not pertinent to the process of capturing what is worthy of regulation. Another caveat is also in order: unless the context requires otherwise, this article focuses primarily on online or digital disinformation.

REGULATORY RESPONSES TO DISINFORMATION GENERALLY

The Ethiopian government has a notably progressive track record in terms of recognizing the socio-economic benefits of the internet, and in setting out a clear policy path to reap these benefits. Ethiopia adopted its first national policy on Information and Communication Technologies (ICTs) in 2002, which has since been updated in 2009 and 2016. Other related policies have likewise been recently adopted by the government, such as the Information Security Policy of 2011 and the Broadband Strategy of 2016. A more recent addition to the policy repertoire is Digital Ethiopia 2025: Digital Strategy for Ethiopia's Inclusive Prosperity (2020). Some of these policy documents are translated into a number of laws, including several pieces of legislation on e-commerce, e-signature and cybercrime.

Implementing agencies have also been set up to translate the policies and laws into action. But the record so far in developing a coherent and legally defensible approach in dealing with emerging cyber threats is dismal. This

6 See generally, C Wardle "Fake news: It's complicated" (16 February 2017) *First Draft News*, available at: <https://bit.ly/3qzwwdj> (last accessed 20 February 2021).

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

is particularly the case in dealing with the rising rogue web culture in Ethiopia, the proliferation of disinformation being the most recent, but also most dangerous of problematic contents. Ethiopia openly recognized the threats posed by disinformation in a 2016 address to the United Nations General Assembly (UNGA) by the former prime minister. In his address, Hailemariam Desalegn decried the misuse of social media platforms to spread hate, bigotry and misinformation.[7] Since then, the government has taken a number of regulatory measures. Such regulatory measures taken so far may be grouped into two categories: legislative (legal) and non-legislative (extra-legal). What follows examines each type of regulatory measure.

Legislative responses

Legislative or legal regulatory measures concern measures that have a clear legal basis and hence are more transparent. Unlike extra-legal measures, this set of measures is either explicitly mandated in law or is a given piece of legislation that is often invoked to justify the measure. There are two categories of legislative or legal regulatory responses to disinformation in Ethiopia. One is the prosecution of suspects under the newly adopted disinformation legislation.[8] Before the adoption of this relatively tailored law, prosecution of similar offences was carried out under the Criminal Code.[9] The second legislative regulatory measure took the form of an institutional response by which "cyber warriors" would be trained to attend to disinformation, among other hybrid cyber threats, online.[10] Until the institution tasked to train these warriors was abolished in mid-2019, this regulatory measure was duly mandated by law.

Criminal prosecution

For over a decade, the Ethiopian government has prosecuted a number of individuals, including journalists, for disseminating falsehood under a controversial provision in the Criminal Code of 2004. Article 486 of the Code criminalizes two sets of acts: (a) spreading or initiating false rumours,

7 "Ethiopia leader at the UN assembly decries use of social media to spread messages of hate and bigotry" (21 November 2016) *UN News*, available at: <https://bit.ly/2GElK3z?> (last accessed 20 February 2021).

8 Hate Speech and Disinformation Prevention and Suppression Proclamation No 1185/2020, *Federal Negarit Gazeta*.

9 Criminal Code of Ethiopia, Proclamation No 414/2004, *Federal Negarit Gazeta*. Other Ethiopian laws are also relevant to disinformation regulation, one being the Media Proclamation. This law stipulates that any broadcasting content and source of any programme, including news, should be accurate. Further, it requires online media outlets to refrain from the dissemination of disinformation. Violation of this proviso will be punishable with a fine of up to 50,000 ETB. See Media Proclamation No 1238/2021, *Federal Negarit Gazeta*, arts 61(9), 68(2)(b) and art 75(1)(j).

10 Cyber Army Development Institute Establishment Council of Ministers Regulation No 401/2017, *Federal Negait Gazeta*.

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

suspicions or false accusations of the government or public authorities and hence twisting public opinion or creating public disturbance; (b) fomenting dissent, hatred, violence or political, racial or religious disturbance by spreading accusations. This provision had long come under attack from different corners for being used to suppress legitimate dissent and freedom of the press.[11] With the adoption of the new disinformation legislation, namely Proclamation No. 1185/2020, this particular article of the Criminal Code has been repealed.[12] The adoption of this legislation has, however, not been without criticism. Beyond the concerns expressed by human rights advocacy groups that the law could be used to suppress critical voices,[13] 23 parliamentarians voted against the adoption of the law as well.[14] No legislation in Ethiopia's recent past has spurred such opposition in the legislature.

This legislation now constitutes the prime legislative regulatory response to disinformation in Ethiopia. Article 3 of the law provides that its main objective is to ensure "*individuals will not engage in speech that incites violence, is likely to cause public disturbance or promotes hatred and discrimination against a person or an identifiable group*" (emphasis added). This provision suggests Ethiopia's regulatory response focuses on addressing disinformation that presents dangers to national security and social harmony. The national security rationale common in certain jurisdictions is explicitly recognized in this legislation. This further suggests that guarding the integrity of electoral processes and democratic institutions is not a stated legislative goal of Ethiopia's disinformation law.

Of course, one of the stated objectives of the law is to "strengthen democratic governance" in the country, but this objective is not framed in a manner envisaged in the laws of several other countries.[15] That is, the objective is not

11 "Draft hate speech and disinformation prevention and suppression proclamation: informal and preliminary comments of the UN Special Rapporteur on Freedom of Opinion and Expression" (5 December 2019), available at: <https://bit.ly/2ZgKJQL> (last accessed 20 February 2021).

12 Proc No 1185/2020, above at note 8, art 9. Note that this legislation concerns two related problems: hate speech and disinformation, which conceptually exhibit a number of overlaps. For instance, a given information or speech may embody the character of both disinformation and hate speech, and often both may have similar consequences in real life. Nonetheless, this article deals only with the disinformation aspect of this law. Note, though, that while the law appears to regulate "disinformation" alone — thereby excluding other cognate notions such as "fake news" and misinformation, the provision that states its objectives mentions controlling and suppressing "other related false and misleading information" as well as disinformation as one of the three legislative objectives. But substantive parts of the law do not address these notions. See id, art 3(3).

13 "Ethiopia's hate speech and disinformation law: the pros, the cons, and a mystery" (19 May 2020) *Access Now*, available at: <https://cutt.ly/hluQCBF> (last accessed 20 February 2021).

14 "Ethiopia passes controversial law curbing 'hate speech'" (13 February 2020) *Al Jazeera*, available at: <https://bit.ly/2R4HIi8> (last accessed 20 February 2021).

15 Proc No 1185/2020, above at note 8, art 3(2).

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

to foster democracy by curbing the risk of disinformation to democratic processes and institutions, but rather to strengthen democratic governance by criminalizing disinformation (and also hate speech). And it is probable that this objective concerns the hate speech aspect of the law because it seeks to strengthen democracy by "promoting tolerance, civil discourse and dialogue".[16] Further reinforcing Ethiopia's national security approach to disinformation is the Preamble of the law in which its underlying objectives are provided. Paragraph 2 of the Preamble states: "Cognizant of the threat hate speech and disinformation pose to social harmony, political stability, national unity, human dignity, diversity and equality".

A closer examination of the law reveals two key lapses that undermine its effectiveness in tackling disinformation through criminal prosecution.[17] First, the law exhibits a number of substantive shortcomings; in particular, it suffers from a number of ambiguities. The ambiguity in the law starts with the term "disinformation". Article 2(3) of the Proclamation defines "disinformation" as "speech that is *false*, is disseminated by a person who knew or should reasonably have known the falsity of the information and is highly likely to cause public disturbance, riot, violence or conflict" (emphasis added). This definition seems to be based on three incorrect assumptions. The first is that "falsity" has a fixed meaning, but that is not always the case as an information or idea could be only partially false, contextually false or visually false. The second assumption is that only categorically "false" information poses a problem (for example disturbance or violence) and is hence worthy of regulation. But the spread of information that is speculative but hard to verify, or information that is not entirely factually inaccurate but misleading, could be a source of destructive incidents on the ground. Finally, the provision has its sights set only on disinformation that is likely to result in physical consequences in real life: "public disturbance, riot, violence or conflict". As such, it therefore overlooks other less tangible consequences of disinformation, such as misleading voters, swaying the course of elections or casting doubt on the validity of election outcomes. This provides additional evidence that Ethiopia's approach falls largely in the approach to disinformation regulation common in countries where national security is the prime driving factor.

The term "dissemination", which forms a key part of the crime of disinformation, is also ill-defined. It is defined as "spreading or sharing [sic] a speech on any means for many persons [sic] but it does not include like or tag on social media".[18] This provision must be read together with the provision that criminalizes disinformation and article 2(3) that defines the notion of

16 Ibid.

17 But the law drew also sharp criticism from a human rights perspective, particularly in light of its impact on the right to freedom of expression. See, e.g., "Ethiopia: Bill threatens freedom of expression" (19 December 2019) *Human Rights Watch*, available at: <https://bit.ly/3m9GlNw> (last accessed 20 February 2021).

18 Proc No 1185/2020, above at note 8, art 2(7).

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

"disinformation". The crime of disinformation is formulated as follows: "disseminating [sic] any disinformation on public meeting by means of broadcasting, print or social media using text, image, audio or video is a prohibited act".[19] The way in which "disinformation" is defined, as outlined above, suggests that criminal liability would fall solely on the person who disseminated the information while knowing, or who ought to have known, the dire consequences it would cause. This reading of the provision may restrict criminal liability to the person who originally shared the disinformation, but not to those who further share or circulate the content. But the definition of "dissemination" appears to broaden the scope of criminal liability. Except for the specifically mentioned acts of "like or tag", any act of spreading or sharing any disinforming content would therefore attract criminal liability.

One notes at this point that the exceptions are not only exhaustive but also seem to have in mind interfaces in currently popular social media sites such as Facebook. This parochial vision of social networking makes it lack the key principle of technological neutrality in internet policymaking by basing the normative standard on the technology of the time. This principle of internet regulation holds that regulation should be "flexible, time-proof and open to technological change".[20] What would happen when new technological interfaces that facilitate easier spreading of online content emerge? Or does the provision even, for example, exclude retweets on Twitter, a popular social networking site? It is also vital to note that the exceptions do not concern other channels of dissemination such as print or broadcasting. What if a particular television show airs an excerpt with some potentially problematic content? The law leaves such questions open.

Another form of ambiguity is evident in the significant variations between the Amharic and the English versions of the law. This point is worth noting because when such variations occur, the Amharic version would prevail. But still, laws in Ethiopia are often first drafted in English and then translated into Amharic, mainly because most Ethiopian laws are transplanted from elsewhere. While it is not known in what language the law was originally drafted, the divergence might cause the true intent of the lawmakers (and drafters) to be lost in translation. For instance, the Amharic version of the provision defining disinformation – i.e. article 2(3) – embodies a condition not specifically mentioned in the English version. According to the Amharic version, "disinformation" is false speech disseminated by a person who has not taken reasonable steps under the circumstances to ensure the veracity of the information. This is neither patent nor latent in the English version. The implication of such divergence is that if courts were to rely on the Amharic version only, that version would be more protective of free expression than the English version.

19 Id, art 5.

20 R Ali "Technology neutrality" (2009) 14 *Lex Electronica* 1 at 11–12.

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

The law borrows a notion from the 2018 Egyptian media law that equates social media accounts that have more than 5,000 followers to media establishments.[21] But Ethiopian law uses this numeric threshold of followers as an aggravating circumstance, i.e., that when disinformation is spread by print, broadcast media or social media accounts with more than 5,000 followers, the applicable penalties would increase from jail time of maximum one year to maximum three years or fines from 50,000 ETB to 100,00 ETB. Two problems, however, inhere in this proviso: the numeric threshold appears to be arbitrary; it also does not clearly indicate whether the relevant account should relate to those owned by individuals only or also to groups, associations etc. as well. If the latter is the case, it is not clear how this would play out in terms of criminal liability. In particular, the nature of criminal liability, as well as who, when it comes to groups or associations, would be held liable, and in what form, is also far from clear.

What is ironic about the new disinformation law is that not only does it tend to legitimize problematic speech under the name of "exemptions", thereby undermining its legislative objective, but also the exemptions under the law are framed somewhat broadly as well. Article 6 of the Proclamation states that speech would not be considered "disinformation" when it is part of (a) academic study or scientific inquiry; (b) a news report, analysis or political critique; (c) artistic creativity, performance or other form of expression; (d) religious teaching; or (e) where the speech has been made after the speaker took reasonable efforts in the circumstances to check the veracity of the information. While exemptions are definitely required to uphold free speech, the exceptions must be carefully defined and be qualified. This is more so in the current highly polarized and ethnicized political environment in Ethiopia. Otherwise, under the banner of, for instance, academic study or scientific inquiry, deeply problematic speech could easily escape restriction. The other exemptions are also problematic. Dangerous and consequential ideas and information may be conveyed in the name of artistic or journalistic ventures or even religious preaching. For instance, the exception for academic or scientific inquiry must be qualified to allow only potentially disinforming content that is expressed for "purely" academic study or scientific inquiry.

The second lapse is that the law faces implementation challenges partly because of the way in which it envisions institutional roles and the nature of the problem. In some respects, the law appears to envision a co-regulatory solution to the problem of disinformation. First, it generally obliges social media companies to put in place internal rules that govern the notice-and-takedown of problematic speech on their platforms.[22] Secondly, it requires these companies to "endeavour to suppress and prevent

21 Proc No 1185/2020, above at note 8, art 7(4). Cf Law no 180 of Egypt, Al-Jaridah Al-Rasmiyah, vol 34 (bis)(h) (27 August 2018) art 4.

22 Proc No 1185/2020, above at note 8, art 8(3).

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

dissemination" of problematic speech on their platforms.[23] In a way, this proviso further solidifies and legitimizes the enormous power that social media companies wield in content moderation. However, the law does not envision any penalties against those companies failing to comply with those sets of obligations. Should a secondary legislation be later enacted (as envisioned in article 8(7)), it may prove problematic.

On pain of being penalized, these corporations would, more often than not, resort to aggressive content moderation measures, thereby significantly curtailing free speech on their platforms. But, of course, this would most likely apply to future local social media companies – if they come into the picture at some point – and not global giants like Facebook and Twitter. As a poor country, Ethiopia has no meaningful leverage by which to force companies such as these, which generally have a smaller user-base in the country.[24] In the current reality, that undercuts the potential of the proviso in which American-based social media companies like Facebook are the prime spaces for disinformation affecting Ethiopia. Thirdly, it requires these companies to remove impugned content within 24 hours of receiving notification.[25] However the law leaves it open as to who is entitled to submit notification – is it anyone, or is it the police or the other bodies mentioned in the law, i.e. the Ethiopian Human Rights Commission and the Ethiopian Broadcasting Authority (EBA)?

The assignment of institutional roles under the law is also far from clear. The nation's media regulator is tasked to carry out two functions. First, it shall compile and disclose a report detailing the degree to which social media companies comply with the law[26] (and the purpose of this report appears to be simply "notifying" the public). Such a duty of reporting on media regulators, in the context of disinformation regulation, is not new. French misinformation law also requires the media regulator to compile similar reports,[27] but it does not stop there as, based on that report, measures could be taken against delinquent parties. Where the delinquent is a media agency, for example the regulator may revoke its broadcasting licence. In cases where delinquents are other actors, the report provides the basis for action by other regulators. But as the law currently stands, Ethiopia's

23 Id, art 8(1).

24 HH Hailu "The problems with Ethiopia's proposed hate speech and misinformation law" (4 July 2019) *LSE Media Policy Blog*, available at: <https://bit.ly/2R5ZIsA> (last accessed 20 February 2021).

25 Proc No 1185/2020, above at note 8, art 8(2). Note that by virtue of the newly enacted media law, EBA is now renamed as the Ethiopian Media Authority to reflect its regulatory reach beyond the broadcasting sector – and hence covering online media – but its role vis-à-vis disinformation is not provided for in this omnibus legislation. See Proc No 1238/2021, above at note 9, arts 4–6 and arts 2(4), 89.

26 Id, art 8(4).

27 See generally LOI n° 2018–1202 du 22 Décembre 2018 Relative à la Luttecontre la Manipulation de l'information.

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

disinformation law says little regarding the goal of the reporting. The stated goal of "notifying the public" serves little purpose in terms of countering the problem of disinformation.

The second task of the EBA is to run media literacy and public awareness campaigns.[28] While this provision rightly advances a widely accepted strategy in dealing with disinformation, it leaves many questions open. One is that it is not entirely clear why and how the EBA is the pertinent body to raise public awareness. As a regulator of media houses, it is best positioned just to follow the regular regulatory channels in order to tame rogue media organizations. A series of regulatory tools are in place to address media organizations' conduct in the context of disinformation and/or hate speech. When it comes to media literacy, the global approach varies, but an emerging trend is that media literacy should not be delegated to a single institution, but instead to several organs within their sphere of influence. Another growing trend in the long-term approach to media literacy is to make it part of school curricula. The US states of California and Massachusetts have, for instance, taken steps towards introducing media literacy lessons in public schools.[29] Ethiopia's approach towards media literacy should be reoriented along these lines.

The Ethiopian Human Rights Commission also assumes a role under the disinformation legislation as the Commission is tasked to raise public awareness regarding hate speech.[30] Under its founding law, the Commission is charged to raise public awareness about human rights and also conduct human rights education.[31] This suggests that its additional function under the disinformation law is based on the assumption that "hate speech" – as opposed to "disinformation" – is a human rights problem and that the Commission is best placed to raise public awareness. As noted above, the EBA is tasked to raise public awareness regarding disinformation, but disinformation is as much a human rights problem as is hate speech, and disinforming attacks could well be a source of egregious human rights violations similar to hate speech. This regulatory conception of "disinformation" is problematic because it encourages cumbersome responses against acts of online disinformation, thereby burdening human rights, and in particular free expression. But the law also leaves out other pertinent authorities from the purview of the law.

---

28 Proc No 1185/2020, above at note 8, art 8(5).

29 See, e.g., "California joins other states in passing new media literacy law" (23 September 2018) *VOA News*, available at: <https://bit.ly/2ZhXLh8> (last accessed 20 February 2021). This appears to be gaining momentum in other parts of the US as well. According to a recent report, for instance, legislatures in 14 US States have taken measures to include media literacy in school curricula. See "US media literacy policy report 2020: A state-by-state survey of the status of media literacy education laws for K–12 Schools" (2020) *Media Literacy Now*, available at: <https://bit.ly/3dt1GiU> (last accessed 20 February 2021).

30 Proc No 1185/2020, above at note 8, art 8(6).

31 Ethiopian Human Rights Commission Establishment Proclamation No 210/2000 (as amended by Proclamation No 1224/2020) *Federal Negarit Gazeta*, arts 5–6.

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

Entities like the Information Network Security Agency (INSA), which is given key roles in cybercrime investigation and prosecution, should also have been tasked under the law.

So far, the law has been used to prosecute disinformation in only a handful of cases. In a recent alleged "fake news" case, the police reportedly invoked the anti-terrorism legislation – as opposed to the new disinformation law – to prosecute a freelance journalist named Yayesew Shimelis.[32] After some confusion as to whether he was being charged under the anti-terrorism law or the disinformation proclamation, the journalist was charged, but later bailed, under the newly adopted disinformation law.[33] He is the first individual to be charged under the disinformation law for disseminating disinformation relating to Covid-19 through his social media accounts, but the content leading to his charge had been posted days before the new law entered into force on 23 May 2020. Hence, the law in this case has been used retroactively, thereby violating the non-retroactivity of criminal law under the Ethiopian Constitution.[34] Elisabeth Kebede, a volunteer lawyer at the Ethiopian Women's Lawyers Association, has been charged by the Harari Regional State Police under the new law for circulating disinformation regarding Covid-19.[35] The current status of her case is unknown, however in early May she was released from detention on bail. The latest defendant under the disinformation law is Temesgen Desalegn, managing editor of a private magazine, who thus far has been briefly arrested, but not formally charged.[36] As these early cases suggest, the disinformation legislation is being used against journalists and dissidents who voice their criticism, thereby clouding its effectiveness in addressing the real problem of disinformation.

Militarization of social media

Deploying "warriors" on social media platforms is the other regulatory response introduced through legislation. The initial idea of trained personnel who would debunk falsehoods on social media sites was put forward by the

32 "Ethiopian police hold journalist Yayesew Shimelis pending terrorism investigation" (6 April 2020) *Committee to Protect Journalists*, available at: <https://bit.ly/2wMJ5vp> (last accessed 20 February 2021).

33 "Journalist's detention sparks concerns over Ethiopia's new hate speech law" (5 June 2020) *International Press Institute*, available at: <https://bit.ly/3i8KIGc> (last accessed 20 February 2021).

34 Constitution of Ethiopia Proclamation No 1/1995, *Federal Negarit Gazeta*, art 22.

35 "Ethiopia: Free speech at risk amid Covid-19" (6 May 2020) *Human Rights Watch*, available at: <https://bit.ly/335FZid> (last accessed 20 February 2021).

36 "AMDF condemns arrest of Ethiopian journalist Temesgen Desalegn" (20 February 2021) *Africa Media Development Foundation*, available at: <https://bit.ly/2HEzbRR>. While this article was being readied for press, another journalist – Bekalu Alamirew – has been arrested for alleged disinformation, among other offences, but released on bail a few weeks later. See "Six journalists arrested in Ethiopia on trumped-up charges" (12 November 2020) *International Press Institute*, available at: <https://cutt.ly/8hjwPNJ> (last accessed 20 February 2021).

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

then governing party in 2017, the Ethiopian Peoples' Revolutionary Democratic Front (EPRDF).[37] Citing the proliferation of disinformation and hate speech online, particularly targeting the party, the ideological outlet of the Front stressed the imperatives of training and deploying a social media army. Shortly after, the idea took a different direction, and the government introduced legislation that created a "Cyber Army Development Institute" within the nation's cyber command, INSA.[38] The law envisioned the Institute as a government higher education institution that would, among other things, train personnel needed for leading the nation's cyber force.[39] A key objective of the Institute was provided under article 4(1):"To provide regular education to key role players in the development of cyber force and develop disciplined cyber force capable to protect national interest and respond to the needs of the country's cyber warfare".

In a stark departure from the initial idea, the law neither explicitly mentioned a "social media army" nor mentioned problems of hate speech and disinformation. The Council of Ministers, the federal cabinet, recently abolished the Institute, and without any clear rationale,[40] but it is interesting to note that the regulation abolishing the Institute transfers the powers and functions of the Institute to INSA.[41] This suggests that INSA would still retain the role of training personnel for the nation's cyber army that would combat, inter alia, disinformation, however little is known about whether this has been the case in reality. Also unclear is whether the Institute had trained cyber warriors before it was disbanded and whether its graduates are at work, for example within INSA. INSA is empowered under its establishment law to "take all necessary counter-measures to defend any cyber or electronic attacks on information and computer-based infrastructures or systems or on citizens' psychology".[42] One might wonder if such countermeasures, which INSA itself – as shall be noted below – has claimed to have taken to counteract cyber-attacks, have been taken to deal with social media disinformation. What is clear, however, is that the idea of a social media army does not seem to have been abandoned altogether. Reinforcing this point is the fact that shortly before the

37 "EPRDF: Let's play our core role through active participation in the social media space" (11 October 2016) *Addis Ra'e* (Addis Ababa) at 76–96 [Amharic: author's translation].

38 Regulation No 401/2017 above at note 10, art 3(2).

39 Id, art 3(1) and art 4(1).

40 Dissolution of Cyber Army Development Institute Regulation No 458/2019, *Federal Negarit Gazeta*, art 2.

41 Id, art 3.

42 Information Network Security Agency Reestablishment Proclamation No 808/2013, *Federal Negarit Gazeta*, art 6(4). Note that per a secondary legislation meant to further this law, taking "counter-measures" falls under INSA's broad power of launching "cyber operations" to (a) collect digital forensic evidence, (b) prevent cyber and electromagnetic attack against national sovereignty, or (c) prevent cyber action that threatens national security or citizens' security. See Information Network Security Agency Reestablishment Proclamation Execution Council of Ministers Regulation No 320/2014, *Federal Negarit Gazeta*, art 9 and art 2(5).

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

Cyber Army Institute was abandoned, the government tabled a Bill in late 2018 that would create a cyber force as well as naval and space forces.[43] The Bill is yet to be adopted by the legislature, but it signalled that the government had not abandoned the idea of a cyber army, including a social media army. It is still not entirely clear, however, if the envisaged cyber force would have any role in dealing with disinformation, including foreign information influence operations or attacks.

But, the idea of creating a social media army was in itself unlikely to be problematic. That the idea was pursued openly, and with a clear legal basis, was promising. Such transparency would create a sense of certainty, and hopefully accountability. However, the initiative should have been taken at the national level and pursued more vigorously. Such efforts would have allowed the government to look to long-term measures in dealing not just with disinformation but also with all other forms of hybrid threats presented by the internet. Of course, the idea of a social media army has some semblance to the practice in a number of authoritarian countries. Countries like China – known for its fierce online censorship – have been suspected of secretly hiring about two million individuals to weigh in on social media debates on behalf of the government.[44] But these government employees do not appear to engage in constructive debates, but instead infuse social media sites with information that praises the government and its achievements, thereby overwhelming users engaged in other useful debates.[45]

The Ethiopian government must distance itself from such unhelpful engagements as this would further distort the flow of information, burden legitimate speech, and ultimately reinforce fake news. The aim should be to counter falsehood by presenting the public with accurate and timely information based on reliable and verifiable facts, rather than dictate the truth. Had it not been aborted, the idea would have fulfilled some sort of useful purpose in dealing with disinformation, at least in terms of the kind of role Sweden bestowed on its "Psychological Defence Authority".[46] Sweden created this body to counter false and misleading information by presenting factual information to the public. As such, it does not engage in further offensive measures, or what is otherwise called "persistent engagement".

Non-legislative responses

Non-legislative measures are those with no clear legal basis and bereft of any transparency or accountability as well. Internet shutdowns are one such

43 "Draft bill introduces naval, cyber and space force" (1 December 2018) *The Reporter*, available at: <https://bit.ly/37J8J43> (last accessed 20 February 2021).

44 See generally, G King et al "How the Chinese government fabricates social media posts for strategic distraction, not engaged argument (2017) 111 *American Political Science Review* 484.

45 Id at 28–30.

46 "Sweden to create new authority tasked with countering disinformation" (15 January 2018) *The Local*, available at: <https://bit.ly/2FcFqe2> (last accessed 20 February 2021).

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

commonly taken measure against the circulation of disinformation online in Ethiopia. Web filtering, such as blocking websites, is the other form of non-legislative regulatory measure used in Ethiopia, but it has become less common in the past two years.[47] With the apparent regression in political reforms in the country, there are, however, signals of a return to past practices of web filtering. A growing number of websites and apps hosting content critical of the government are now inaccessible in Ethiopia.[48] Internet shutdown is a more recent tool of "informal" content regulation.[49] Since the widespread protest against the government in 2015 – in the orchestration of which social media platforms played a central role, the government resorted to internet shutdowns on a number of occasions. Be it to stop the spread of leaked text of national university entrance examinations or allegations of brutal crackdown on protestors, the internet has been shut down by the government several times in the past few years.

Fighting disinformation is the more recent and persistent rationale invoked by the government when shutting down or throttling internet use in some parts of the country.[50] But the government rarely offered a legal justification for resorting to shutdowns.[51] Often, the government presents unpersuasive

47 A 2016 joint report of Amnesty International and Open Observatory of Network Interference documents that Ethiopia notoriously blocked dozens of websites which, according to the government, disseminate content deemed objectionable for social, political and security reasons. See generally "Ethiopia offline: evidence of social media blocking and internet censorship in Ethiopia" (2016) *Amnesty International and Open Observatory of Network Interference*, available at: <https://cutt.ly/IlppKCi> (last accessed 20 February 2021). Unblocking most of such sites was, however, among measures taken with the reshuffle in government in mid-2018. See "Ethiopia allows access to over 260 websites" (22 June 2018) *Committee to Protect Journalists*, available at: <https://bit.ly/2Fh4bG9> (last accessed 20 February 2021).

48 See, e.g., "Resurgence of internet censorship in Ethiopia: Blocking of WhatsApp, Facebook and African arguments" (14 August 2019) *Open Observatory of Network Interference*, available at: <https://cutt.ly/Ylupzyl> (last accessed on 20 February 2021).

49 Regulatory measures such as internet shutdowns are also referred to as "gateway regulation" as they target the gateway of communication. See, e.g., L Eko "Many spiders, one worldwide web: Towards a typology of internet regulation" (2001) 6 *Communication Law and Policy* 445 at 475–77.

50 Recurrent shutdowns have occurred in Ethiopian in mid-2019 following a series of political assassinations and disturbances. See, e.g., "Ethiopia internet shutdown continues following reported coup attempt" (24 June 2019) *Net Blocks*, available at: <https://bit.ly/35iFPa0> (last accessed 20 February 2021). At the time of writing in late February 2021, internet shutdown is in place in the regional state of Tigray where there is an ongoing war between Tigray Defence Forces (TDF), on the one hand, and, since early November 2020, Ethiopia's National Defence Forces and its domestic and regional allies on the other. See, e.g., "From Myanmar to Ethiopia, internet shutdowns become favoured tool of regimes" (11 February 2021) *CBC*, available at: <https://bit.ly/3tJw5hD> (last accessed 20 February 2021).

51 KM Yilma "Internet shutdowns and the law in Ethiopia" (July 2020) *Medium*, available at: <https://bit.ly/3jyFFif> (last accessed 20 February 2021); see also KM Yilma "Network disruptions and the law in Ethiopia: A legal guide" (Internews, May 2021).

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

defences for its opaque shutdown practices. One may recall here the claim that since the internet is neither water nor air, it may therefore be shut when the government deems there is a threat to national security.[52] But more recently, the Office of the Federal Attorney General, in its formal comments on a report of the UN Special Rapporteur on Freedom of Opinion and Expression that lamented government shutdown practices, coincidentally offered a legal justification of sorts for internet shutdowns.[53] This casual legal justification has two prongs, one of which is that the Office notes that the 2013 law that re-established INSA empowers the Agency to "keep the country safe from any threats against national security and [said] it can take measures when the necessity arises".[54] According to the Office, this law provides a legal basis for internet shutdowns.

A closer look at this law does not, however, support this claim. Nowhere in this law is the Agency's power to cut internet access for national security purposes either explicitly stated or implied. The closest this law comes to stating it is when it empowers INSA to take "countermeasures" for cyber-attacks against the nation's critical infrastructures, like power grids and "citizens' psychology".[55] As the nation's cyber command, this proviso simply empowers INSA to take counter-measures – otherwise called "strike-backs" – against perpetrators of cyber-attacks. Strike-backs, therefore, are a sort of in-kind retaliation by resorting to proportionate cyber-attacks. If the attack was, for instance, in the form of a Distributed Denial of Services (DDoS) attack, the Agency may retaliate with similar DDoS attacks or large-scale spreading of malware. This means two things: first, when cutting internet access, INSA would not be engaging in the lawful strike-backs envisioned in its establishment law. Instead, it would simply be unlawfully restricting the individual right to free expression, including the right to access information online. Second, most trigger factors for internet shutdown in Ethiopia, such as social media disinformation, do not really fall under the rubric of cyber-attacks imagined in the law. Disinformation is a form of hybrid cyber threat, but not quite a cyber-attack warranting lawful strike-backs.[56] Even if it were, how would a state hit back proportionately against coordinated disinformation campaigns of non-state actors? INSA had previously invoked a similar line of reasoning to justify the brief internet blackout in December 2019.[57] At the time, INSA

52 "Twitter backlash after Ethiopia PM's internet 'not water or air' Threat" (3 August 2019) *Africa News*, available at: <https://bit.ly/3bF0ia2> (last accessed 20 February 2021).

53 Report of the UN Special Rapporteur on the Promotion and Protection of Freedom of Opinion and Expression (29 April 2020) paras 51–52.

54 Comments by the State on the Report of the UN Special Rapporteur on the Promotion and Protection of the Freedom of Opinion and Expression on His Visit to Ethiopia (15 April 2020) para 20.

55 Proc No 808/2013, above at note 42, art 6(4).

56 See generally H Gunneriusson and R Ottis "Cyberspace from the hybrid threat perspective" (2013) 12 *Journal of Information Warfare* 67.

57 Report of the UN Special Rapporteur, above at note 53, para 50.

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

claimed the brief shutdown was needed to fight off active cyber-attacks against the nation, but this justification lacks any legal basis. The second part of the Federal Attorney's legal justification is that internet shutdowns are seldom taken with maximum restraint, and in line with international human rights and national constitutional standards of "legality, legitimacy, necessity and proportionality".[58] Not only are internet shutdowns occurring frequently – and, at times, for extended periods – but they also lack clear legal basis, thus failing to meet the requirements of "legality". This makes it immaterial to consider whether the other requirements of necessity and proportionality are fulfilled.

Overall, recurrent episodes of arbitrary internet shutdowns in Ethiopia suggest that the government saw value in internet shutdown as a useful regulatory measure. But it could have grounded such shutdowns on a sound legal basis in the recent cybercrime law.[59] This law potentially offers a defensible legal basis for gateway measures like internet shutdown. Moreover, because the law requires a prior court warrant before such measures are taken, it also envisages safeguards against abuse. The recurrence of network disruptions, and their impact on the enjoyment of human rights, would be mitigated when each request for an internet shutdown had to be considered by the courts in light of national and international human rights standards.

ELECTION DISINFORMATION AND ETHIOPIAN LAW

Elections and democratic institutions have become the main targets of recent disinformation campaigns worldwide.[60] Many of the recent regulatory measures have been taken to bolster the resilience of the integrity and security of electoral processes against online disinformation. Ethiopia is generally categorized as a non-democratic nation – or, per The Economist Intelligence Unit Democracy Index, an "authoritarian" State.[61] Despite having held elections

58 Comments by the State on the Report of the UN Special Rapporteur, above at note 54, para 20.

59 Computer Crime Proclamation No 958/2016, *Federal Negarit Gazeta*, art 32(5). For more on this point, see Yilma, above at note 51. Note also that laws imposing a State of Emergency (SoE) – also called "martial laws" – often provide a legal basis, albeit tentative, for network disruption in Ethiopia. A 2020 SoE law declared in the regional state of Tigray, for instance, empowers the Task Force instituted to oversee the decree to "cause the closure or termination of any means of communication where it is necessary to maintain the Constitution and constitutional order". See State of Emergency for the Protection of the Constitution and Constitutional Order Proclamation No 4/2020, *Federal Negarit Gazeta*, art 4(5) and State of Emergency Proclamation for the Prevention of Constitution and Constitutional Order No 4/2020 Ratification Proclamation No 1228/2020, *Federal Negarit Gazeta*.

60 See generally B Martin-Rozumiłowicz and R Kužel "Social media, disinformation and electoral integrity" (International Foundation for Electoral Systems Working Paper, August 2019), available at: <https://bit.ly/3iR50Xk> (last accessed 20 February 2021).

61 "Democracy Index 2019" (2020) *The Economist Intelligence Unit* (London) at 13.

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

over the past few decades that have failed to credibly meet the democratic bar, the country has, nevertheless, always had a longstanding aspiration to install a democratic order based on free, fair and democratic elections.

After the recent much-lauded but quickly diminishing democratic reforms, holding free, fair and democratic elections has been set as a priority by the current government. But the general elections, originally slated to be held in May 2020, have already been rescheduled twice, and again more recently due to the pandemic. Tigray – one of the ten regional states in Ethiopia – did, of course, hold a controversial election for the region's Council in September 2020, although the rest of the country has postponed its elections indefinitely.[62] And in late 2019 as well, a referendum was held in the Southern Nations, Nationalities and Peoples Region, which ultimately led to the creation of the tenth regional state in Ethiopia.[63] But little is known as to whether disinformation has been a concern during the rather brief election cycle in Tigray or in the Sidama referendum. With general elections now set to be held sometime in 2021 in the rest of the country – and also potentially multiple referenda for regional statehood – the question of whether, and the extent to which, current Ethiopian legal framework is sufficiently well equipped to address the dangers of election disinformation remains. This section considers this question.

Disinformation in the context of elections engages a number of legal regimes, including electoral law, data protection law, media law and pieces of legislation governing telemarketing/spam and advertisements. But a closer look at the current catalogue of relevant Ethiopian laws suggests that no tailored regulatory measure is envisioned to meet the challenges of election disinformation. As shown above, the recent disinformation legislation regulates disinformation more generally and, hence, would cover problematic content during the election season. But, besides its multiple loopholes, it does not even come close to the kind of election-oriented legislative measures taken in other jurisdictions such as in the US, Canada and Australia. Electoral law is the primary means of regulating the use of the media during the election cycle, campaign finance (spending and donations), access to voter records/registration and certification of advertisements.[64] However, the more recent electoral law enacted as part of the broader effort of strengthening the nation's democratic institutions does not seem to envision disinformation as a threat to the credibility of elections. Where the relevant election legislation appears to recognize the problem of election disinformation, it adopts a slightly narrower scope in dealing with the problem.

62 "Ethiopia's Tigray holds regional election in defiance of federal government" (9 September 2020) *Reuters*, available at: <shorturl.at/fTVW6> (last accessed 20 February 2021).

63 "Sidama referendum: Over 98% vote 'YES' for Ethiopia's 10th regional state" (23 November 2019) *Africa News*, available at: <shorturl.at/cfiEJ> (last accessed 20 February 2021).

64 See generally, D Tokaji *Election Law in a Nutshell* (2nd ed, West Publishing, 2016).

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

Electoral law

Ethiopia's omnibus electoral law of 2019 has some provisions that do tend to address election disinformation. For instance, it prohibits engaging in "activities that in any way disrupt, destroy or frustrate the election campaign of other parties or cooperate in such acts".[65] It similarly prohibits dissemination of false information, claiming that the secrecy of the ballot has not been maintained.[66] These prohibitions appear to cover common election-related disinformation. But the scope of the law's overall orientation is directed at duly registered political parties, their candidates, members, supporters and agents.[67] As such, it envisions threats of disinformation only from domestic actors, specifically from registered political actors. This means that it would not ordinarily apply to those who engage in those impugned acts without any political registration or affiliation. Foreign state and non-state actors that engage in those acts would not therefore be regulated by the law. This problem of scope makes this new law slightly outdated in light of modern-day disinformation perpetrated across borders through the help of modern communication technologies.

To an extent, the electoral legislation addresses the key issue of campaign finance. First, it imposes a series of regular reporting, bookkeeping and auditing obligations on political parties regarding their sources of income and donations.[68] Second, it bans donations from certain actors, particularly foreign governments and organizations as well as non-governmental bodies.[69] Such constraints on sources of income help fend off not only influence on political parties but also interference in the electoral process. But these parts of the law overlook a key part of recent electoral laws in the digital age: regulation of political advertisements online. Much of the election-related disinformation in other countries is undertaken through the use of purchased political advertisements by foreign as well as domestic actors. Recent electoral law reforms, for instance in the US and Canada, introduce a series of transparency obligations on social media platforms to disclose the identity of those purchasing political adverts and the attendant price, among other details.[70] Corollary to such duties is a system in some countries by which political

65 Electoral, Political Parties Registration and Election's Code of Conduct Proclamation No 1162/2019, *Federal Negarit Gazeta*, art 129(2).

66 Id, art 130(7) and art 144(3). In addition, there is a more positive duty on political parties to contribute towards the realization of the right to vote and be elected. See id, art 129.

67 Id, art 3(2) and Preamble, para 8.

68 Id, arts 78, 81–82, 111.

69 Id, art 108.

70 See, e.g., A Bill to Enhance Transparency and Accountability for Online Political Advertisements by Requiring Those Who Purchase and Publish Such Ads to Disclose Information about the Advertisements to the Public and for Other Purposes (Honest Ads Bill) [116th Congress, 7 May 2019]; Elections Modernization Act (Bill C-76) [13 December 2018].

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

parties and candidates pre-certify social media adverts by election regulators.[71] This means that major social media sites would not allow adverts that have not been pre-certified by the appropriate electoral body.

In spite of its overall comprehensive scope, Ethiopia's electoral legislation leaves much-needed regulatory details to secondary legislation. It relegates to a series of directives to be adopted by the National Electoral Board of Ethiopia (NEBE) the responsibility to hammer out a number of issues, such as the manner of conducting election campaigns and media code of conduct on election coverage,[72] but no such directive that regulates the issue of social media mediated disinformation has been made public. In light of the law's overall narrow scope in regard to election-related disinformation, it is less likely that upcoming directives would be able to directly address the issue.

A related limitation of recent electoral laws is that they appear to underestimate the role of social media in shaping the course of elections. Although adopted as recently as 2019, the Proclamation has within its purview only legacy media as the prime medium of election-related communications. Nowhere in this law is the role of the new media taken into consideration in regulating election-related information dissemination and communication. Mass media, which primarily concerns print and broadcast media, both of which are within the regulatory reach of the government, appears to be the law's sole focus.[73] It is only remotely that some provisions of the law actually touch on the sort of election disinformation threatening elections. One such provision, for instance, prohibits "abuse of position of power", by which any political party may not use its position of power to influence – which includes "special opportunity or influencing ability" – to bribe or use any other illegal methods to further its interests.[74] This broad framing might capture the use of social media influence. Similarly, article 136 prohibits "corrupt practices", including using any inducement to sway the opinion of voters, but both of these rules apply only to political parties registered under Ethiopian law.

Overall, Ethiopia's electoral law has its sights set on registered political parties, candidates and their supporters. But, importantly, the law generally overlooks the role of technology companies in altering the course of elections, particularly by offering a platform for actors (state or non-state, domestic, regional or international) to manipulate voting outcomes through various

71 See, e.g., Supreme Court Order for Pre-certification of Political Advertisement on Electronic Media, in Letter from Election Commission of India to Chief Secretaries et al (13 September 2018), available at: <https://perma.cc/U2MM-U862> (last accessed 20 February 2021).

72 Proclamation No 1162/2019, above at note 65, arts 43–44.

73 Id, art 44 (dealing with the use of mass media by political parties and candidates as well as coverage of elections by journalists, yet key details are relegated to future secondary/tertiary legislation); see also National Electoral Board of Ethiopia Establishment Proclamation No 1133/2019, *Federal Negarit Gazeta*, art 7(5).

74 Id, art 135.

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

methods, including disinformation. Assisted by the ever-evolving and sophisticated technological environment, the world of digital political campaigning is deeply complex, involving invisible actors and practices. This is further complicated by the transnational nature of the network on which it operates. A layer of technology companies operates in the ecosystem: from data brokers, data analytics firms, campaign platforms to AdTech and social media networks. So, behind the curtain of social media platforms from where user data are harvested and later used to target those users with political adverts, a number of invisible and, hence, unaccountable players exist.

The Cambridge Analytica scandal that plagued Facebook a few years ago is a good case in point.[75] This data analytics company used unlawfully obtained personal data of about 87 million Facebook users in order to engage in disinformation campaigns during the US presidential elections. And, of course, the scandal hit close to home as well when similar allegations of disinformation campaigns occurred during the presidential elections in Kenya (2013, 2017) and Nigeria (2015).[76] Unlike the laws in India, for instance, Ethiopian law does not envision social media platforms as key stakeholders in the fair and peaceful conducting of elections. It does not go beyond imposing a very general "duty to cooperate" on everyone in the proper implementation of its provisos.[77] With increasing use of the internet in Ethiopia, and the rising role of social media in socio-political discourse, there is an urgent need to address the role of social media platforms generally, and during the election cycle in particular.

The NEBE is reportedly drafting a Directive that would partly address the issue of election-related disinformation in the social media environment. This draft Directive reportedly addresses two themes.[78] First, it seeks to regulate the use of social media by political parties and candidates for political campaigning purposes. As such, the object of this Bill seems to be outlining a code of conduct for these political actors when using social media platforms during the election season. Second, it will also set out duties on political parties to provide ethical education to voters, particularly their supporters and constituency. Once adopted, this Directive would partially address the gaping hole in the 2019 Proclamation, which overlooks the role of social media discourse in shaping the course of elections. There is still, however, an issue remaining with the narrow conception of the problem associated with social media platforms.

As highlighted above, dangers to the credibility and integrity of electoral processes come from different corners in the digital age. Social media's use

75 "The Cambridge Analytica story, explained" (2019) *The Wired*, available at: <https://bit.ly/2FuOGdP> (last accessed on 20 February 2021).

76 "Cambridge Analytica in Africa – What do we know?" (10 January 2020) *Democracy in Africa*, available at: <https://bit.ly/3jrSlY4> (last accessed 20 February 2021).

77 Proc No 1162/2019, above at note 65, art 161.

78 Ethical Education and Social Media Use by Political Parties Directive (Draft, October 2020).

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

of practices of registered political parties and candidates – whose conduct is and could be monitored by the NEBE – is unlikely to pose the greatest danger to the credibility of elections. Global actors, be it state or non-state actors, with geo-political or economic interests in the nation could marshal social media platforms to skew the elections. As was the case in other jurisdictions, sophisticated disinformation campaigns, including using sponsored political advertisements, pose serious dangers to the integrity of elections. Besides such foreign actors, Ethiopian political actors other than registered political parties could also use online platforms to influence the outcome. With the significant role of the Ethiopian diaspora in domestic political dynamics, social media platforms would simply offer new ways to reshape the domestic political reality, including election outcomes. The NEBE's regulatory responses thus far do not seem to have such new and sophisticated election-manoeuvring practices in mind. More crucially, no measure seems to be in the offing that would outline the duty or role of major social media platforms, such as Facebook, during the election cycle in Ethiopia.

Criminal law

Criminal law may also apply in some contexts. Title V (Crimes against Public Elections and Voting) of the Ethiopian Criminal Code touches upon an aspect of election disinformation.[79] Article 471 criminalizes "unfair practices", which include two key offences. One is campaign finance violations, for example collecting money or receiving donations contrary to campaign finance rules. The other offence concerns fraudulently securing, abusing or misappropriating votes directly or through an intermediary with (a) the help of false news or rumours circulated through, inter alia, the press, radio or "any media of publicity"; (b) the help of any other fraudulent, irregular or dishonest practices. This provision was drafted at a time when the spread of either election-related information or political adverts had not reached its present level of sophistication, but it specifically uses terms like "false news and rumour", thereby capturing the essence of "disinformation", and its illustrative list of media engaging in unfair electoral practices includes the new media, including social media platforms.

It is vital to note that this provision applies to anyone who engages in those practices and, as such, it is not restricted to political parties and candidates. In comparison, therefore, Ethiopian criminal law contains rules on election-related disinformation that are more progressive. These rules, however, do not provide adequate safeguards; for one thing, they offer remedies after the fact, and once the accused has engaged in the impugned acts, and hence do not preemptively prevent or mitigate the risk of disinformation.

79 Criminal Code, above at note 9, arts 466–76. Note that the more recent criminal piece of legislation, the cybercrime law, criminalizes dissemination of spam but concerns only unsolicited communications of commercial nature. See Proc No 958/2016, above at note 59, art 15.

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

In addition, the transnational nature of the problem and weak institutional capacity to wade through the complexity of digital disinformation further diminishes the criminal law solution to the disinformation problem in Ethiopia, including in the election context.

Data protection law

In regulating the collection, processing and sharing of personal data, data protection law plays a key role in controlling the use of personal data for political purposes. Data protection law would constrain processing of sensitive personal data such as one's political opinion and profiling of data subjects. It would impose a series of transparency obligations on data controllers and processors, such as to clearly state the type of data collected, for how long, and its purposes as well as to whom it may be shared. These duties are embedded in a series of data protection principles and rights. On top of this, this area of law would put in place an oversight mechanism by which compliance is monitored. As the controversy over the 2016 US presidential elections illustrated, exploitation of personal data from social media users was part of the disinformation campaign.[80] In the wake of this debacle, the debate has centred on the role of data protection law in regulating the use of personal data for political campaigning purposes. While Ethiopia does not have data protection legislation, it has recently issued a Bill that provides useful safeguards against exploitation of personal data for political purposes.[81]

This Bill addresses some of the key issues of data protection in the context of elections. First, unlike the laws of many countries, Ethiopia's draft legislation does not exempt processing of personal data for political purposes.[82] This means that any collection, processing or dissemination of personal data by anyone for political purposes must comply with data protection principles and rights as well as the attendant regulatory controls. Second, it also categorizes personal data concerning a data subject's political opinion as "sensitive personal data".[83] And this would mean that while processing of such data is prohibited in principle, it is strictly regulated when certain exceptions warrant processing. Third, the Bill also addresses profiling – i.e. automated processing of personal data – which is a key aspect of current social media political advertisement practices.[84] Profiling is permitted in only exceptional circumstances, but is totally prohibited if the processing of the data involves sensitive personal data. Fourth, the Bill also defines personal data in a manner that captures the state of the art in the world of online political advertisements, where use is mainly made of pseudonymized and anonymized data. The

80 See generally, "Challenging data exploitation in political campaigning" (June 2020) *Privacy International*.
81 Draft Personal Data Protection Proclamation (April 2020).
82 Id, art 63.
83 Id, art 2(28)(e) and arts 18–19.
84 Id, art 2(24) and art 42.

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

definition of personal data includes (pseudonymized or anonymized) data that could allow the identification of a person when read/combined with other data. Fifth, the draft law imposes a series of transparency obligations on data controllers and processors under the principles of "fairness and transparency", "purpose limitation", "data minimization", and data rights such as the "right to be informed" and the "right of access".[85] Sixth, to monitor protection of data privacy, the Bill establishes a Data Protection Commissioner and also mandates the appointment of Data Protection Officers by data controllers. But the virtues of this impending law are constricted; for one thing, it is a mere draft and hence it is not clear when it will be enacted and will enter the statute book, however even after entry into force, its implementation will be impaired by a number of factors, including lack of resources and expertise. As the experience in other African countries suggests, it would be a while before a national data protection authority is up and running, which might mean after several elections and referenda have already been held and potentially marred by disinformation.

Advertisement law

Ethiopia has an advertisement law that regulates all forms of advertising in Ethiopia, including web advertising. Its conception of advertisement is, however, problematic. The definition of advertisement under the law suggests that it concerns only "commercial ads", implying that adverts made for non-profit purposes are not covered,[86] but again, an overall reading of the law suggests that it applies to all forms of adverts, including non-commercial adverts such as personal and political adverts. Adverts "having political goals" are listed among prohibited or restricted types of adverts, however the law carves out an exception for political adverts disseminated during the election season by political parties and individual candidates registered under Ethiopian law.[87] This means that other adverts with certain political goals, but disseminated by actors other than those two groups, are prohibited. Theoretically, this would include sponsored adverts by foreign state and non-state actors, but in light of the law's overall narrow scope in regard to social media-based sponsored adverts, the law offers little in addressing adverse political advertising from overseas. It is also vital to note that the duty of monitoring the implementation of this legislation falls on the EBA. However, the Authority's regulatory remit thus far has been restricted to the regulation of legacy media – i.e. broadcast and print media, and this means that types of political adverts disseminated through social media platforms as tools of disinformation campaigns would not be addressed by Ethiopia's advertisement legislation.

85 Id, caps 3 and 4.
86 Advertisement Proclamation No 759/2012, *Federal Negarit Gazeta*, art 2(1).
87 Id, art 25.

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

CONCLUSION

As shown in this article, regulatory measures taken in Ethiopia are primarily legislative (legal) and, as such, extra-legal measures commonly taken in other jurisdictions are yet to emerge, but whether the challenges to Ethiopia of disinformation, including to the nation's democratic aspirations, can meaningfully be addressed through legislation is in doubt. This is because of two fundamental reasons. One relates to the inherently transnational nature of the problem, involving actors – often less visible – from different jurisdictions. With Ethiopia's limited leverage to regulate the behaviour of transnational actors, legislative measures are unlikely to prove effective. Add to this the fact that conspicuous underestimation or failure to properly realize the problem's gravity and nature, and the disjointed nature of measures, which – as shown above in the context of the nation's electoral legislation – will undercut the effectiveness of legislation.

The second reason concerns regulatory capacity and independence. Regulating complex problems like disinformation in the digital environment requires well-resourced regulatory bodies, particularly in terms of expertise. Election and media regulators must be equipped with personnel competent to investigate and regulate disinformation in the ever-dynamic digital ecosystem. Equally vital as well is institutional independence and autonomy, which is not generally present in Ethiopia. This is all the more so in light of the controversy that most regulatory attempts might trigger among stakeholders. With the NEBE only recently re-established, operating not only in a deeply divided and polarized climate, but also with EBA's weaker institutional capacity and independence of the Office of the Federal Attorney General, it is unlikely that the legislative avenue would bring about meaningful results in terms of curbing disinformation, including during elections.

Disinformation presents a real risk to Ethiopia's democratic aspirations. Episodes of social media disinformation in the past few years in Ethiopia have foreshadowed the risks of disinformation to the democratic aspirations of the country as well as to its internal socio-political stability. To properly address these risks, the article closes with the following policy recommendations. First, Ethiopia should properly recognize the risks of disinformation to its aspirations of holding free, fair, democratic and credible elections, and either take tailored policy measures or adapt the existing policy, legal and institutional framework. Second, Ethiopia should adopt a nuanced, but comprehensive approach that would effectively address the ills of disinformation to Ethiopia's fledgling democracy. Third, Ethiopia should take a multipronged approach to the disinformation problem that combines legal measures such as criminalization, regulation of political advertising and extra-legal measures such as regular as well as occasional media literacy programmes. Fourth, Ethiopia should properly recognize and define the key role of technology companies in addressing the disinformation problem, including by introducing elaborate regulations that outline codes of conduct, working closely with major social media platforms, and, of course,

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press

establishing meaningful international cooperation in order to make legislative measures effective. Fifth, Ethiopia should support independent efforts of third parties in tackling disinformation, including during the election cycle, through funding and other forms of support. Sixth, Ethiopia should strengthen the institutional as well as the legal frameworks in order to make them fit for purpose in the complex world of disinformation, including by instituting dedicated and properly resourced entities.

CONFLICTS OF INTEREST

None

https://doi.org/10.1017/S0021855321000322 Published online by Cambridge University Press