

**SAFEGUARDING ELECTORAL
INTEGRITY IN THE DIGITAL AGE.
STRATEGIES FOR COMBATING
DIGITAL MISINFORMATION – AN
AFRICAN CONFERENCE**

ADV. PANSY TLAKULA
CAPE TOWN, SOUTH AFRICA
2-5 MARCH 2020



**INFORMATION
REGULATOR
(SOUTH AFRICA)**

Resolving protection of your personal information
and efficient access to information

Introduction

- The right to freedom of expression and access to information are important to the conduct of free, fair and credible elections. The importance of the right of access to information in the exercise of the right to vote was underscored by our court in the case of My Vote Counts NPO v President of South Africa and others.
- The role which social media plays in advancing the right to freedom of expression and the right of access to information in the electoral process cannot be over emphasised.

Cont.

- Social media has been used to disseminate information which the incumbent government wants to keep away from the electorate, especially during campaigning. It provides information in real time and a lightening speed.
- Unlike traditional media, which can be subjected to closure, harassment, intimidation and even arbitrary arrest or murder of journalists, social media cannot be subjected to this treatment.

Cont.

- A writer called John Perry Barlow aptly puts it in an article called Declaration of the Independence of Cyberspace -8 February 1996
“Internet would usher in a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced with silence or conformity”.

Cont.

- This explains the reason why in the past governments of countries such as Cameroon, Ethiopia, Gambia and Uganda resorted to the arbitrary shut down of the internet in the run up to and during elections under the guise of the protection of national security or the prevention of election related violence.

Cont.

- In as much as social media promotes access to information, it can also be a dangerous tool against free, fair, credible and peaceful elections. In the run up to an election, social media can be used to spread fake news, misinformation and disinformation which does not only confuse the electorate, but can also influence the way people vote. Fake news and misinformation can incite political violence and sabotage an election. The Cambridge Analytica debacle and the Russian interference in the 2016 elections of United States of America have given impetus to calls of regulation of social media. Moreover, the jury is still out on the effectiveness of the third party fact checking programme.

Cont.

- Unlike mainstream journalism which is regulated by a Code of Ethics which requires journalists to report truthfully and objectively, to verify their sources and afford a person a right of reply, these do not apply to social media. It is for this reason that calls for the regulation of social media are gaining traction.

To regulate or not to regulate

- A number of lessons can be learnt from state regulation of the traditional media. Free expression and human rights activists the world over have always advocated for self regulation of traditional media. In countries where state regulation applies, laws such as criminal defamation, publication of false news, insult laws (which make it a criminal offence to 'insult' a head of state, elected public representatives and in some countries, even senior government officials),

Cont.

- and sedition are often used to arrest and prosecute journalists, members of the opposition parties and even representatives of Non Governmental Organisations who are perceived to be critical to the incumbent government, particularly in the run up to an election.
- There is convergence that illegal content such as child pornography, content which incite violence on the basis of race, ethnicity, religion (hate speech) on social media platforms should be regulated. Unlawful processing of personal information of data subjects is also regulated through data protection laws.

Cont.

- A number of countries have adopted laws which regulate social media. To give examples:

Cont

Country	How Social Media is Regulated
Germany	<p>Germany's NetzDG law came into effect at the beginning of 2018, applying to companies with more than two million registered users in the country.</p> <p>These companies are required to set up procedures to review complaints about content they were hosting, remove anything that was clearly illegal within 24 hours and publish updates every six months about how they were doing.</p> <p>Individuals may be fined up to €5m (\$5.6m; £4.4m) and companies up to €50m for failing to comply with these requirements.</p> <p>The government issued its first fine under the new law to Facebook in July 2019. The company had to pay €2m (£1.7m) for under-reporting illegal activity on its platforms in Germany, although the company complained that the new law had lacked clarity.</p>

Cont.

Country	How Social Media is Regulated
European Union	<p>The EU is considering a clampdown, specifically on terror videos. Social media platforms face fines <u>if they do not delete extremist content within an hour.</u></p> <p>The EU also introduced the General Data Protection Regulation (GDPR) which set rules on how companies, including social media platforms, store and use people's data. It has also taken action on copyright. <u>Its copyright directive puts the responsibility on platforms</u> to make sure that copyright infringing content is not hosted on their sites.</p> <p>Previous legislation only required the platforms to take down such content if it was pointed out to them.</p> <p>Member States have until 2021 to implement the directive into their domestic law.</p>

Cont.

Country	How Social Media Is Regulated
Australia	<p>Australia passed the Sharing of Abhorrent Violent Material Act in 2019, introducing criminal penalties for social media companies, possible jail sentences for tech executives for up to three years and financial penalties worth up to 10% of a company's global turnover.</p> <p>It followed the live-streaming of the New Zealand shootings on Facebook.</p> <p>In 2015, the Enhancing Online Safety Act created an eSafety Commissioner with the power to demand that social media companies take down harassing or abusive posts. In 2018, the powers were expanded to include revenge porn.</p> <p>The eSafety Commissioner's office can issue companies with 48-hour "takedown notices", and fines of up to 525,000 Australian dollars (£285,000). But it can also fine individuals up to A\$105,000 for posting the content.</p> <p>The legislation was introduced after the death of Charlotte Dawson, a TV presenter and a judge on Australia's Next Top Model, who killed herself in 2014 following a campaign of cyber-bullying against her on Twitter. She had a long history of depression.</p>

Cont.

Country	How Social Media is Regulated
Russia	<p><u>A law came into force in Russia in November</u> giving regulators the power to switch off connections to the worldwide web "in an emergency" although it is not yet clear how effectively they would be able to do this.</p> <p>Russia's data laws from 2015 required social media companies to store any data about Russians on servers within the country.</p> <p>Its communications watchdog <u>blocked LinkedIn</u> and fined Facebook and Twitter for not being clear about how they planned to comply with this.</p>

Cont.

Country	How Social Media is Regulated
China	<p>Sites such as Twitter, Google and WhatsApp are blocked in China. Their services are provided instead by Chinese providers such as Weibo, Baidu and WeChat.</p> <p>Chinese authorities have also had some success in restricting access to the virtual private networks that some users have employed to bypass the blocks on sites.</p> <p>The Cyberspace Administration of China announced at the end of January 2019 that in the previous six months it had closed 733 websites and "cleaned up" 9,382 mobile apps, although those are more likely to be illegal gambling apps or copies of existing apps being used for illegal purposes than social media.</p> <p>China has hundreds of thousands of cyber-police, who monitor social media platforms and screen messages that are deemed to be politically sensitive.</p> <p>Some keywords are automatically censored outright, such as references to the 1989 Tiananmen Square incident.</p> <p>New words that are seen as being sensitive are added to a long list of censored words and are either temporarily banned, or are filtered out from social platforms.</p> <p>(source: BBC News (12 February 2020) Social Media: How do other governments regulate it</p> <p>https://www.bbc.com/news/technology-47135058</p>

Cont.

Country	How Social Media is Regulated
South Africa	<p>Film and Publications Amendment Bill:</p> <p>any person who distributes revenge porn will, upon conviction, be liable for payment of a fine of up to R300 000. They may also go to prison for up to four years.</p> <p>Those who make themselves guilty of distributing hate speech may be fined up to R150 000. They may also end up in prison for no more than two years.</p> <p>The bill also requires internet service providers to remove content that amounts to child pornography, hate speech, propaganda for war or incitement of imminent violence. This removal must happen as soon as possible after the service provider becomes aware of it.</p>

Cont. South Africa

Country	How Social Media is Regulated
	<p>Cybercrimes Bill:</p> <p>It criminalises certain electronic data messages which may take the form of SMS, e-mail or social media correspondence. It will be a criminal act to incite violence or damage to property in an electronic data message. This includes messages sent via WhatsApp, Facebook, e-mail, SMS or any similar communications platform.</p> <p>It will criminalise data messages that threaten others with violence or damage to property against individuals or groups. Groups may be characterised according to factors like race, gender, marital status, gender, ethnic or social orientation and belief.</p> <p>It will also make it criminally culpable to make an intimate image of someone available in an unlawful and intentional way.</p>

Cont. South Africa

Protection of Personal Information Act 4 of 2013 (POPIA)

The Act regulates the processing of Personal Information by public and private bodies. It also establishes the Information Regulator (Regulator), which monitors compliance with the Act. The Regulator has extensive enforcement powers.

Cont.

- In Nigeria, the Protection of Internet Falsehood and Manipulation Bill of 2019 is still before the legislature. The Bill has been criticised for being too wide ranging and as a threat to free speech and legitimate political debate.

Cont.

- The Tanzanian Cybercrime Act of 2015 criminalizes fake news.
- There is a view by one proponent of social media regulation (Alan O Rourke) who opines that digital infrastructure must be regulated in the same way as telecoms, railway and energy companies are regulated. He says that even banks, which are private entities, are highly regulated. Other proponents of regulation are of the view that social media enjoys complete freedom of speech and should be regulated in the same way as traditional media.

Cont.

- Their view is that similar to traditional media, social media companies should be held accountable for what is published on their platforms. They feel that the laws which protect intermediaries against liability (such as section 230 of the US Communications Decency Act) have outlived their utility.
- Those who are against state regulation of social media are of the view that social media companies must fix the problems that they have created. They are in complete agreement with the view that illegal content such as child pornography and videos of extreme violence should be regulated.

Cont.

- They prefer self regulation. They have a problem with the regulation of fake news and disinformation by the state. Their reason for this is who decides what is fake news and what is not? If content is found to be fake, is it satire or is it intended to cause harm? Even if it causes harm, who decides whether it is freedom of expression or prohibited expression and what rules or criterion is used to make such a determination? The apprehension of the anti regulation group is that regulation may stifle freedom of expression and suppress dissent or critical speech. Moreover, governments may not have the required resources to regulate social media companies.

Cont.

- In their view, instead of regulating social media, the government should establish independent regulatory bodies which monitor whether social media companies comply with their self regulation policies or not. These bodies should be given effective enforcement powers.

Conclusion

- Lack of adequate and effective data privacy policies in social media companies can compromise the personal information of the electorate. This may results in their personal information being unlawfully processed and used to spread fake news, disinformation or misinformation. The personal information of voters can also be unlawfully processed by political parties to bombard voters with unsolicited campaign messages. It can also be used by data analytics companies to micro target certain groups or individuals so as to influence the outcome of an election and thereby affect its freeness, fairness and credibility.

Cont.

- In my opinion, the proper response to deal with this problem is for the state to establish independent data protection authorities which must be given effective enforcement powers.
- Electoral Management Bodies (EMBs) should also bring their laws in line with the data protection legislation and adopt policies which will ensure the protection of the huge amount of personal information of voters that they keep. Failure to do so might expose them to sanctions in terms of data protection laws.

Cont.

- EMBs might also consider adopting codes of conduct on the use of personal information of voters by political parties.
- Social media companies must ensure that their policies are in compliant with national electoral laws which deal with prohibited conduct and ensure that they remove content which violates these laws. In general, they must use a rights based approach to their policies which must be based on the respect for human dignity, the right to equality, the right to non discrimination, freedom of expression, the right of access to information and the right to privacy.

Cont.

- The management of elections in a digital age requires a complete paradigm shift. Some electoral laws are no longer fit for purpose because they were adopted before the proliferation of social media.

Cont.

- The management of elections in the digital era requires a multi disciplinary approach. It needs collaboration between EMBs and Data Protection Authorities on issues of the impact of fake news and disinformation of the freeness and fairness of elections. Ideally, EMBs should be give enough resources acquire technology which monitors the origins of bad bots which spread fake news and misinformation so that they can take appropriate action.

Cont.

- Finally, an election is a contest for political power, robust speech should be allowed during campaigning. The only speech that should be proscribed is speech which violates standards prescribed in regional and international human rights instruments.
- Introducing new standards for speech in social media platforms might violate long established regional and international human rights standards on freedom of expression and access to information.



www.shutterstock.com - 584483197

Q AND A