

Fake news – The three sisters: Mis, Dis and Mal.

3 August 2022 9 min read

by Ahmore Burger-Smidt, Head of Data Privacy and Cybercrime Practice, and Siyabonga Galela, Candidate Attorney

Fake news Introduction

The Fourth Industrial Revolution (colloquially referred to as “4IR”) has given individuals around the globe almost-continuous access to near real-time conversations about both important and trivial matters,[1] thus exposing people to voluminous amounts of unfiltered information and creating the mammoth task of distinguishing between trustworthy sources, misinformation and so-called ‘fake news’, while ensuring that the constitutional right to freedom of expression is respected.

4IR can be described as the current and continuously developing environment in which disruptive technologies and trends are transforming the way in which our society functions.[2] Trends in advanced monitoring technologies and infinite virtual connectivity have increased online activity and interconnectivity, making it possible for stories and opinions to gain exposure and traction at unprecedented speed.[3]

In recent years, the South African media has been awash with stories of incidents of cyberbullying,[4] with victims reporting a range of forms of psychological harm stemming from cyberbullying.[5] This article discusses the Cybercrimes Act 19 of 2020 and the common law of defamation in the context of the 4IR world, social media activity and so-called ‘fake news’.

What’s in a name?

Use of the term ‘**fake news**’ has gained traction in recent years, and is generally used to refer to some kind of false information or news reporting. What is generally overlooked, however, is that the term encompasses various forms of false information whose characterisation is linked, *inter alia*, to the intention that underpins the dissemination of such information.

For example, ‘disinformation’ refers to the intentional spread of inaccurate information with the intent to deceive;[6] and encompasses false or manipulated information that is knowingly shared to cause harm, or is made with reckless disregard for likely harm.[7]

One such example is how during the COVID-19 pandemic, a number of myths (presented as truth) regarding the origin and nature of the COVID-19 virus, as well as the manner in which it can be transmitted, made headlines across the world.[8]

Conversely, ‘misinformation’ refers to the unintentional dissemination of false, inaccurate or misleading information.[9] ‘Mal-information’ on the other hand, refers to truthful information that is presented deceptively in an attempt to mislead.[10]

All the aforementioned categories of ‘fake news’ generally contain content that can harm public discourse by influencing individuals to make misinformed decisions when it comes to politics, the State or their personal well-being.[11]

Legal Framework

Social media platforms have emerged as one of the primary vehicles via which disinformation, misinformation and/or mal-information is disseminated. However, it is important for social media users to remember that there are limits to free speech, and that the right to freedom of expression is not absolute.[12]

In other words, social media platforms are not necessarily the place for users to say and do as they please, particularly because engaging in such conduct could lead to serious legal consequences.[13]

In South Africa, social media platforms are regulated via either of two vehicles. The first vehicle is the common law and the second vehicle is legislation. In terms of common law, our courts adjudicate disputes on the basis of evaluating whether or not the complainant suffered reputational harm as a result of the publication of the information causing the dispute.[14]

Conversely, legislative regulation canvasses a wider spectrum of issues, including the protection of personal information (Protection of Personal Information Act, 2013) and prohibition of malicious communications, as provided in the Cybercrimes Act, 2020.

Cybercrimes

The Cybercrimes Act 19 of 2020 (“**Act**”) posits cybercrimes as new criminal offences in South Africa, including the criminalisation of certain categories of speech online.[15] For example, the Act criminalises the disclosure, by means of an electronic communications service, of a data message that causes damage to property or violence (i.e. bodily harm) against a person or group of persons.

The aforementioned conduct is criminalised not only on the basis of one’s *intention* to incite the causing of such damage or violence,[16] but also on the basis of one’s threat to cause such damage or violence;[17] or one’s unlawful and intentional conduct in attempting or conspiring to aid, instigate or instruct another person to commit an offence in terms of the Act.[18]

Furthermore, section 16 of the Act criminalises the unlawful and intentional disclosure of a data message of an intimate image of a person without their consent[19] (i.e. including so-called ‘revenge-porn’).

What is of note is that the malicious communication offences created by the Act are premised on *intention*. So in the context of fake news, it is the disclosure of *disinformation* that is criminalised by the Act; thus exposing one to liability for a fine, imprisonment or both.[20]

Although welcoming, it is clear that the criminalisation of malicious communications does not compensate those who have been wrongfully harmed by, *inter alia*, the culpable conduct of others. Fortunately the civil remedy of delict offers such relief.[21]

Defamation

Defamation is a form of delict based on the wrongful, intentional publication of words or behaviour relating to any other person that injures or demeans such a person’s status, good name, character and/or reputation.[22] In the context of fake news and social media, a victim can claim compensation for injury and harm sustained so long as he/she can demonstrate that the published content was wrongful, intentional, and contained defamatory material that refers to the victim.[23]

In *Heroldt v Wills* 2013 (2) 530 SA GSJ, the first South African case involving defamation via social media, the South Gauteng High Court held that the assessment for determining if the content posted has a defamatory meaning is whether a reasonable person of ordinary intelligence might reasonably understand the post concerned to convey a meaning that is defamatory.[24]

In *Heroldt v Wills*, Ms Wills – who was ordered by the court to remove all impugned postings from her Facebook and any other social media sites referred to by the applicant – was the creator of the defamatory post.

However, it is important to note that one does not necessarily have to be the person who creates a potentially abusive post to be held liable for such a post.[25] For example, in *Isparta v Richter and Another* 2013 (6) 529 (GNP), the court confirmed that if one is aware of the fact that he/she is tagged in a potentially defamatory post, and that person makes no effort to disassociate from such a post, then that person may be held as equally liable as the person who created the post.

In the context of fake news, this means anyone found to have contributed to false or defamatory content (including the dissemination of such content) may be held civilly liable for defamation, even if such content constitutes mal-information or misinformation.

Fake News Conclusion

Indeed, people, cultures and communities sometimes have differing views, interpretations and understandings of certain events.[26] However, the 4IR world has demonstrated that these differences have the potential of being manipulated in a manner that infringes on the

fundamental right to freedom of expression and the right to privacy.

There can be no question that the regulation of the dissemination, *inter alia*, of malicious information is a necessary and worthwhile exercise.

However, what needs to be interrogated is the palatability of the scope of such regulation, particularly from a fundamental-rights point-of-view; and the extent to which it strikes the necessary balance between those fundamental rights (i.e. the protection of free speech on one hand and the protection of the right to privacy on the other).

For example, legislative regulations of social media platforms have been criticised for not going far enough to the extent that media platforms are still able to unilaterally regulate the types of content that can be shared on their platform(s); and can streamline and manipulate content in a manner that exposes users to information at the expense of transparency and accountability.

While the operational requirements of media platforms, insofar as they operate as a business, are understandable, they can never be an excuse to facilitate the dissemination of mis/dis/mal-information.

The Cybercrimes Act specifically deals with malicious communications, and we have to understand the impact of this Act on misinformation, disinformation and mal-information.

In the same breath, it should always be borne in mind that governments are not the arbiters of truth; and that the regulation of free speech (whether online or otherwise) must align with, and balance, fundamental constitutional rights.[27]

Be that as it may, there is no denying that the Cybercrimes Act is a positive step in the right direction insofar as our 4IR world is concerned. After all, the ‘fake news’ phenomena is one of but many examples of the need for rules that regulate conduct and standards of behaviour when it comes to use of the internet.

Footnotes

[1] [“Fighting Fake News on Social Media”](#) 22 June 2022, at 1

[2] M Kalinda [“The Role of Media Technology in 4IR”](#) 12 April 2021

[3] [“Fighting Fake News on Social Media”](#) 22 June 2022, at 1

[4] F Khan [“Cyberbullying: a delictual claim for emotional harm?”](#) 1 May 2022

[6] [“Fighting Fake News on Social Media”](#) 22 June 2022, at 1

[7] International Center for Not-For-Profit Law [“Disinformation and Freedom of Opinion and Expression”](#)

[8] [“Fighting Fake News on Social Media”](#) 22 June 2022, at 2

[9] [“Fighting Fake News on Social Media”](#) 22 June 2022, at 2

[10] International Center for Not-For-Profit Law [“Disinformation and Freedom of Opinion and Expression”](#) at 1

[11] [“Fighting Fake News on Social Media”](#) 22 June 2022, at 2

[12] The Constitution of the Republic of South Africa 1996, section 16

[13] “Think before you “Share”” at 2

[14] D Iyer [“An analytical look into the concept of online defamation in South Africa”](#) *Speculum Juris* at 126

[15] International Center for Not-For-Profit Law [“Disinformation and Freedom of Opinion and Expression”](#) at 1

[16] Cybercrimes Act 19 of 2020, section 14

[17] Cybercrimes Act 19 of 2020, section 15

[18] Cybercrimes Act 19 of 2020, section 17

[19] Cybercrimes Act 19 of 2020, section 16

[20] Cybercrimes Act 19 of 2020, section 19

[21] F Khan [“Cyberbullying: a delictual claim for emotional harm?”](#) 1 May 2022

[22] “Think before you “Share”” at 2

[23] F Khan [“Cyberbullying: a delictual claim for emotional harm?”](#) 1 May 2022

[24] *Heroldt v Wills* 2013 (2) SA 530 (GSJ)

[25] Think before you Share at 2

[26] S Grootes “[Divided we tweet: A flood of lies this way comes and will tear us apart](#)” 6 June 2022

[27] International Center for Not-For-Profit Law “[Disinformation and Freedom of Opinion and Expression](#)” at 1



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)