PERSPECTIVES ON MISINFORMATION AND RELATED CYBER LAWS

Hezron Wangi Jnr*

Introduction

In war, truth is the first casualty,[1] in a bio-crisis like the recent novel corona virus, the same adage also applies. At the outbreak of the pandemic, the world took to the internet to express their views. Speculations such as, a laboratory experiment gone wrong, a weaponized bio threat released from Wuhan, the viral effect of 5G internet, anti-Sino slurs and other trending topics on blogs, vlogs and posts flooded the net.

The pandemic has shown the vital need for the provision of authentic information to assist first responders in their timely response in curbing the spread of the virus. In times of crisis, the press and the government also have an increased responsibility in providing reliable information to the public for purposes of awareness, and at times, to serve as a warning.[2] Good comprehension by the general public of a country's state of affairs reduces the risk for panic and fosters people's understanding and compliance to necessary restrictions.[3]

Traditionally, the press has been the main medium in reporting and disseminating information. However, the internet has paved way for ease of convenience in communicating online. This in turn has made it convenient for individuals to readily exercise their freedom of speech and expression online, and in so doing, provides a challenge to the conventional role of the media in society.

The internet has made it easy for individuals to readily express their views without restraint. The anonymity provided by the internet means that a user could publish content without verification or credibility. The excessive use of the internet to publicize, share and manipulate information without any attribution to credible authorities is causing, what is known as, information pollution.

It comes with no surprise that internet users are susceptible to false information spread by the internet, especially on social media. Although seemingly harmless, more issues arise daily because of the misuse and abuse of social media. At times, fake news or information, has a malicious effect if relied upon by the general public. Various questions may arise as to how our legal system captures that concern? Is there sufficient legislation in place to address false information online? And would the presence of these pieces of legislation stifle free speech? These questions will be discussed as this paper.

The Laws on Information

The Freedom to Disseminate and Freedom for Information

Section 46 of the *Constitution* operates to accommodate free speech in Papua New Guinea (PNG). The *Constitutional Planning Committee* (CPC) Report also makes it clear that free speech is a right that must be upheld and protected. However, the exercise of this right may be restricted or regulated by law.[4]

With regards to access to information, section 51 of the *Constitution* provides that every citizen has the right to information, insofar as, it is guided by section 38 of the *Constitution*.[5] The critical

---

* Senior Legal Officer with Office of Solicitor General, Department of Justice and Attorney General.

1 *Aeschylus*, Agamemnon, (reprinted) November 6th 2003, Cambridge University Press, U.K.

2 *Freedom of Expression and Information in Times of Crisis,* Council of Europe Portal, <https://www.coe.int/en/web/freedom-expression/freedom-of-expression-and-information-in-times-of-crisis (accessed on 28/5/2020).

3 Ibid.

4 See section 38 of the *Constitution*.

5 General qualifications on qualified rights may restrict or regulate the right guaranteed by this section.

component of this provision is that it confers the right of reasonable access to official government documents only.[6]

Section 38 of the *Constitution* provides that qualified rights such as the right to freedom of and to disseminate information may be regulated or limited. The regulation and restriction of these rights is deemed necessary when national security is concerned with regards to public interest in defense, public safety, public order, public welfare, public health, the protection of children etc.

The restriction of such rights must be in a manner that is reasonably justifiable in a democratic society so as not to derogate the substance of the rights conferred to citizens. Section 38 provides that for a law or an act to be reasonably justifiable in a democratic society, it must have proper regard to the rights and dignity of mankind determinable in the circumstances obtaining at the time when the decision on the question is made.[7]

With regards to internet use, section 46 of the *Constitution* (on the freedom of expression) by extension, enables freedom of press and freedom of expression by people and news agencies online. This is in terms of publication or creation of audio-visual material in conveying their idea, message or expression.

Information Technology law does not consist of an entirely new branch of law on its own, it includes aspects of other laws such as intellectual property law, privacy law, contract law and other areas of law stemming from different acts and transactions facilitated by computers. The focus of this paper will only be on free speech and the dissemination of information online.

Freedom of Expression and Free Speech Online Is Challenging the Traditional Role of the Press and Credible Agencies

The freedom of expression under section 46 of the *Constitution* provides the foundational basis for press freedom in PNG. However, broadcast or print media in our society must adhere to stringent protocols to ensure responsible and accurate reporting.

Some of the ethical principles which must be upheld generally in the media are truth and accuracy (the facts must be correct). These principles must influence dissemination of information, particularly reporting. Also, a degree of fairness must be observed and there must be objective reporting without bias. Equally important, the content of the report must not contain malice, and reporters must be responsible and accountable in their reporting.[8]

These regulations and ethical standards ensure content of reports do not incur ramifications both legally and socially. In-house editors review content and ensure that they comply with standards. The vetting process disallows mere busybodies from reporting without having regard for standards.

Apart from press and broadcasting media, the internet has expanded the ambit to which rights pertaining to freedom of expression and speech can be exercised. What was once a conventional platform where the right is exercised, technology has established a new platform and regulation and ethical standards have to be adjusted to address dissemination of information on technological platform. The convenience of the new platform, the internet has also resulted in news content being digitized and vulnerable to be manipulated at will by internet users.

General distrust in authority coupled with varying other factors has made social media a hotbed for lies, speculation and manipulative content being shared with exponential frequency. With technological convenience and also digital anonymity, digital news content is susceptible to being copied or shared by internet or social media users with no attribution to credible sources.[9]

---

6 *Yasangi v Padura* (2015); N5871 – this right does not extend to private documentation; there is no specific Act governing the freedom of information in PNG.

7 Section 39(1) of the *Constitution*.

8 The 5 Principles of Ethical Journalism, https://ethicaljournalismnetwork.org/who-we-are/5-principles-of-journalism (accessed 28/05/20).

9 *The Contradictory Influence of Social Media Affordances on Online Communal Knowledge Sharing,* accessed https://academic.oup.com/jcmc/article-abstract/19/1/38/4067499 by guest on 07 May 2020.

The traditional role of the press in society is somewhat challenged because of the peer to peer sharing and general distrust in authority. Government departments and authorized bodies tasked with the dissemination of information are also faced with the challenge of refuting false information circulated by social media and micro boggers online. The internet is being cluttered by too much unnecessary information - it is being polluted.

Information Pollution And False Information Online

Information pollution is the contamination of the information supply with irrelevant, redundant, unsolicited, hampering, low value and at times harmful information.[10] Digital content on topics ranging from social, financial, health, education, health and etc., pollute the internet. As with most pollutants, the information shared may have perfidious effects.

The effects of false information online are concerning, even the United States President, Donald Trump and Brazilian President, Jair Bolsonaro seem to have fallen prone to this trend. They have, on occasions, advised their constituents that hydroxychloroquine could be medically used to prevent covid-19 despite having no scientific basis for such a claim.[11] Political correctness cannot dampen the fact that people – even political leaders and persons of influence, are also likely to fall victim to false information disseminated on social media and messaging applications which they may rely on for news.[12]

PNG is no exception to the growing trend of misinformation online. A digression to our recent news headlines will explain why:

- Police storm treasury building in Tari, Hela over Facebook post;[13]
- Air Niugini Refutes False Information on Recruitment;[14]
- Police Commissioner, Manning concerned about the abuse and misuse of social media during State of Emergency;[15]
- Health Department condemns speculation on social media about corona virus;[16]
- Bank of South Pacific Refutes Claims on Social Media about fee increase.[17]

A brief glimpse of the above would lead one to the conclusion that false information breeds well in social media. Although, the above headlines provide no revelations, it does not take much imagination to deduce the financial losses individuals, businesses and the government may have incurred due to the effects of misinformation.

---

10 Orman, L. (1984). *Fighting Information Pollution with Decision Support Systems*. *Journal of Management Information Systems, 1*(2), 64-71. Retrieved May 26, 2020, from www.jstor.org/stable/40397792.

11 R. Goodman & C. Giles, *Coronavirus and hydroxychloroquine: What do we know?, 27/05/20,* BBC News https://www.bbc.com/news/51980731) (accessed at 28/05/20).

12 Navigating the CronavirusInfodemic, https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2020/04/Navigating-the-Coronavirus-infodemic.pdf (8/05/20).

13 R. Kuku, *Police Storm Treasury Building,* 21/05/20, The National, at https://www.thenational.com.pg/police-storm-treasury-building/ (accessed at 27/05/20).

14 *Advertisement on Facebook false: PX,* The National, 3/01/2020. https://www.thenational.com.pg/advertisement-on-facebook-false-px/.

15 *Abuse of social media concerning.* The National, 6/05/20 at https://www.thenational.com.pg/abuse-of-social-media-concerning/ (accessed at 27/05/20).

16 *Health Department condemns speculation on social media,* 28/01/20, The National, accessed 27/05/20 at https://www.thenational.com.pg/health-department-condemns-speculation-on-social-media/.

17 *Fleming responds to social media claims: No Fee increase*, 13/01/20 The National, https://www.thenational.com.pg/fleming-responds-to-social-media-claims-no-fee-increase/.

It is necessary that a brief is provided about the different variations or types of misinformation, as the latter term is usually conflated to mean fake news. There are varying nuances to the term that necessitate distinction.

These categories include:[18]

- Misinformation: information that is false but not created with the intention of causing harm – e.g., false connections and misleading content;
- Disinformation: information that is false and deliberately created to harm a person, social group, organization or country, e.g., false content, imposter content, manipulated content and fabricated content; and
- Mal-information: information that is based on reality that is used to inflict harm on a person, organization or country, e.g., *leaks, harassment and hate speech*.

These categories are provided in the Council of Europe's Information Disorder Report. The report is dedicated to understanding information disorder as perpetuated by contemporary social technology, and further assessing information pollution.[19] These definitions may be parallel to alternatives in law.

Translating the Distinctions into Legalese

With the distinctions provided above, there emerges a basis by which these definitions could be translated into legalese. Wrongs arising from false information online could either fall under the sphere of civil or criminal law depending on the nature of the wrong committed.

As far as civil law is concerned, civil actions may arise from tortuous grounds or from issues that arise from contractual relationships. Such an offence could attract civil action to protect or compensate the right of the victim that has been breached. Libellous acts are more likely to be instituted as civil proceedings.

Because an act of disinformation, mal-information or misinformation stems from the creation of false content with (whether with or without deliberate intention to cause harm), most of the wrongs committed in cyberspace is captured in the *Cybercrime Code Act.* State prosecution may be instituted if criminal culpability is proven upon the laying of a formal complaint.

Acts of disinformation, misinformation and mal-information are captured under the *Cybercrime Code Act* 2016. Examples include:

i. Identity theft: section 15

ii. Cyber Extortion: section 24

iii. With intent to commit fraud: (Electronic Fraud) Section 12;

iv. The intentional leak of confidential information: Unlawful Disclosure; Section 25;

v. Harassment; Cyber harassment Section 23 (1) and (2); and

vi. Spam: section 26

A closer look at section 23 (4) reveals that this provision creates an offence relating to the use of imagery and audio-visual material that is obscene, profane or vulgar and which grossly offends acceptable standards of society. The provision caters for online "public" indecency, but only within the confines of that provision. It does not elaborate on what actions would constitute as profane, vulgar or obscene.

---

18 C. Wardle, PhD, H. Derakshan, *INFORMATION DISORDER: Toward an interdisciplinary framework for research and policy making,* Council of Europe Report, DGI (2017) at https://rm.coe.int/information-disorder-report-november-2017/1680764666 (accessed: 19/05/20).

19 Ibid.

The *Cybercrime Code Act* is quite recent in the sphere of cyber law, a topic that is fairly new in our jurisprudence and leaves much room for development. This is a challenge which will undoubtedly be addressed in the development of our jurisprudence as it evolves over time.

The data and statistics used in drafting this article is from a research by the American Poynter Research institute which could be accessed online at their official website. A perusal of the comprehensive layout of data in that research would be necessary for the reader's appreciation when reading this article.[20]"

What other Governments Are Doing

Like PNG, Governments around the world also face the same predicament concerning false information online. Many governments hesitate to introduce legislation that would regulate information online and thereby limiting free speech by their people. Various international human rights groups are relentless and staunch in their position against such legislation.

That being said, it is noteworthy to mention what some governments are doing in terms of tackling the growing infodemic[21] to protect their constituents. Comparison will only be drawn from democratic countries who have, in one way or another, taken action to resolve this growing issue.

In May 2019, the Singaporean government passed a legislation criminalizing the dissemination of misinformation online.[22] The *Protection from Online Falsehoods and Manipulation Act* 2019 makes it illegal for individuals and entities to spread false statements of facts that compromise security, public tranquillity, public safety and the country's public relations with other nations.[23] If a malicious actor spreads misinformation, the new legislation imposes heavy sanctions which include:

- $37, 000 or 5 years in prison – Mere dissemination of false information.
- $74, 000 or 10 years in prison – If the misinformation was shared using an inauthentic online account (fake accounts) or a bot.[24]
- $740, 000 or 10 years in prison – Social platforms that play a role in disseminating misinformation.

Canada has taken a more liberal approach towards combating false information online by launching its digital charter. The charter necessitates the willing participation of government institutions to sign up to it. Its vision is to defend the freedom of expression and protect against online threats and disinformation designed to undermine the integrity of elections and democratic institutions. Although, the charter expresses its vision, it does not provide a clear definition on what fake news is nor the sanctions that would be imposed for offenders. A lot has been left unsaid in the charter.

Certain countries are also making strides in creating agreements with major social media corporations such as Facebook. The Brazilian government has entered into an agreement with Facebook and Google to combat disinformation created by third parties.[25] The focus, however, is only placed on applying that legislation during election periods.

Germany has also taken a more severe approach by introducing legislation that directly holds social media platforms accountable for facilitating misinformation. The German government is focused on

---

20 https://www.poynter.org/ifcn/anti-misinformation-actions/.

21 Information pandemic – an influx of information or misinformation rendering difficult the actions towards resolving an issue.

22 https://www.poynter.org/ifcn/anti-misinformation-actions/.

23 J. Russell, Singapore passes controversial fake news law which critics fear will stifle free speech, https://techcrunch.com/2019/05/09/singapore-fake-news-law/ (accessed: 10/05/19).

24 An automated program or robot (bot) that is coded especially for a specific use.

25 *Brazil Preparing to Fight Fake News During Elections,* The Rio Times, https://riotimesonline.com/brazil-news/rio-politics/brazil-preparing-to-fight-fake-news-during-octobers-elections/.

eradicating hate speech and is legislating for severe sanctions to support its vision. Currently, the German government is planning to sue Facebook for breach of that legislation.

With regards to most governments, bills introduced and legislation passed are dedicated only towards setup of cyber task forces to protect the integrity of their elections. After perusing the annexed table, the reader would deduce that most governments fear foreign powers influencing their election.

The American electoral history is riddled with instances where foreign and domestic powers have been alleged to have meddled with the turnout of their election. Leaked emails, recordings and audio-visual content have been used with malicious intent to influence and sway public opinion when voting.

The different American states have different approaches to addressing this issue ranging from proposed federal laws, media literacy laws, failed state advisory groups to state lawsuits. There are many vested political and corporate interests which may complicate plans for a federal bill to be passed.

Most democracies around the world have yet to develop legislation that work to effectively combat online misinformation. The hesitance in doing so arises from concerns that the introduction of such legislation would give the government unfettered powers which may be abused.

There are vehement criticisms against such a move by any government, as it may limit free speech and give the government broader powers that may be abused. An analysis of the annexed tabulated report shows that governments which have effectively controlled the dissemination of online misinformation exhibit tendencies akin to totalitarianism. This is evident in countries where false charges are laid resulting in the arrest of outspoken journalists and activists in countries such as Egypt, Cambodia and Rwanda.

As jurisdictions around the world develop, time and circumstance will only tell if governments will legislate against misinformation. Circumstances may differ by country due to their respective history and culture, but freedom of expression and free speech is universal and is embedded and exercised universally in most democratic countries.

PNG currently has no legislation dedicated to combating misinformation online. Although, such legislation would prove useful in governing and regulating the dissemination of information, an in-depth research is needed to understand whether such a law would be beneficial to the framework of our democracy or otherwise.

Assessing the Papua New Guinean Predicament

Much of PNG's laws concerning misinformation is captured under the *Cybercrime Code Act.* Similar to other criminal matters, breaches constituting a cybercrime is instituted in the legal system by first laying a complaint with the Royal Papua New Guinean Constabulary (hereinafter RPNGC). The RPNGC is the only mandated authority responsible for prosecuting offences under the *Cybercrime Code Act.*

In 2018, the National Information and Communication Technology Authority (NICTA) initiated a response team to deal with cyber complaints. The Papua New Guinea Computer Emergency Response Team (PNGCERT) has authority to address all cyber related incidents; however, it is not mandated to enforce the *Cybercrime Code Act* but only to assist RPNGC in their investigation.[26]

Moreover, NICTA does not have any specific powers to order any internet service provider to prohibit sites that breach PNG cyber laws. Unlike NICTA's counterparts in foreign jurisdictions, it does not have the power to effectively address cybercrimes.

[26] The PNGCERT Website, accessed https://www.pngcert.org.pg/ (accessed on 29/05/20).

The RPNGC attests that it has a cyber-unit based in the Nation's Capital. However, in 2017, both NICTA and RPNGC admitted that they lacked the capacity to effectively enforce cybercrime laws.[27] It was also admitted that both departments lack the technical expertise to enforce the *Cybercrime Code Act.*

The integrity of a cyber-unit embedded with the RPNGC is also a cause for concern as it may be exposed to political influence. In the 2019 case of *Mark v Neno*[28], the plaintiff – a journalist, made a formal complaint to the Police against a Member of Parliament for allegedly breaching the *Cybercrime Code Act.* The complaint arose from publication of an alleged material defaming her on social media by the politician.

The defendant (a Provincial Police Commissioner) advised the plaintiff to consider pursuing her grievance through civil proceedings. The reason being that the Member of Parliament was also the Police Minister during the time of the proceeding in court. The RPNGC was not able to investigate her complaint due to the accused being the Police Minister. It seems that in certain instances such as in *Mark v Neno,* the Police responsibility to conduct independent and impartial investigations on cyber complaints may be influenced and even waived due to political considerations.

PNG's cyber laws are also silent on hate speech, which is a growing concern. Hate speech within Papua New Guinean ethnicities may incite violence and perpetuate stereotypical behaviour. Hate speech against Pacific island neighbours and the world at large would damage the country's reputation. Having this concern captured under our cyber laws would go a long way to protect the integrity and reputation of our country.

A more practical approach towards resolving this issue, would be for government agencies, to disseminate information through its channels in a timely manner. Without proper awareness and directions from government departments, there will be confusion and social anxiety. Withholding vital information and lying to people in times of crisis would have irreparable repercussions when people lose trust in authority.

As exhibited in the Chimbu province, at the height of the pandemic, rural hospitals were not given any instructions nor were there any proper awareness. The latter resulted in the hospital closing its doors; the unfortunate result was the death of a woman who was in need of medication.[29]

Thoughts to Consider

Would these reforms to combat misinformation infringe the liberties of persons?

Without going into much jurisprudential banter, it is necessary to state that every human society has some form of social order, some way of making and encouraging approved behaviour, deterring disapproved behaviours and resolving disputes if conflict arises from a behavior.[30] In making laws, it is important to weigh out what is moral and what is legally and socially acceptable in different societies amongst other circumstances. The tension created by the different factors – if not considered would mean that legislating a law that is detached from the realities of the people, may lead to abuse.

The formulation of a legislation limiting or regulating free speech is one such topic subject to much debate. If factors such as political history, culture and other circumstances are not weighed in through research, such a law may be proficient in promoting abuse. International human rights

---

27 M. Arnold, *Lack of Capacity to Enforce Cybercrime,* 14/06/17, Post Courier https://postcourier.com.pg/lack-capacity-enforce-cybercrime/.

28 (2019) N8115.

29 *Panic over lack of covid info in rural PNG risks lives,* Radio New Zealand, https://www.rnz.co.nz/international/pacific-news/413394/panic-over-lack-of-covid-info-in-rural-png-risks-lives, (accessed 01/06/20).

30 *Legal Positivism*, Stanford Encyclopedia of Philosophy, 3/01/03 https://plato.stanford.edu/entries/legal-positivism/#DeveInfl.

groups such as Amnesty International, Human Rights Watch and the United Nations actively oppose the enactment of such laws.

However, with respect to human rights, it is unwise and impractical to allow freedom without restraint or limitation. The free reign of information dissemination by individuals who are not equipped or trained in the ethics of journalism on social media has and will continue to bear significant repercussion to the masses.

Lessons learned from history and from our analysis of the data in our tabulated report, show that most governments use such legislation to attack their opponents. Given both sides of the argument, it is safe to say that without consultation and proper research, the creation of such legislation may not be in the best interest of PNG at this point in time.

Taking Action

There are, however, practical steps already undertaken by democratic nations around the world that deserve recognition and can be adopted and practiced in PNG. Our existing cyber laws may be bolstered through amendments to support already existing bodies who are conferred powers to enforce our cyber laws.

Where our legislation is silent on certain cyber wrongs such as hate speech and holding internet service providers responsible for malicious content, changes may be introduced by way of amendments. Such amendments may also accommodate for the setting up of a separate independent and impartial cyber unit with prosecutorial powers.

This can be achieved by legislatively conferring more powers to the PNGCERT and setting it as an independent unit under NICTA. The unit would be occupied by officers from NICTA and other pertinent agencies who are technically equipped, skilled and dedicated towards investigating cyber related offences.

Also, most people may not know that some of their actions online would have constituted a cybercrime. Some may not even know of the existence of the cyber laws; therefore, priority must be given to educating our people on the existing cyber laws and carrying out cyber-literacy campaigns around the country. Embedding this as an education reform within the curriculum in our education system would also be effective in educating our young generation on proper online etiquette.

Conclusion

False information online will continue to be a problem in PNG if proper steps are not taken to enforce provisions of our cyber laws. A dedicated legislation to combat misinformation online, although enticing, may require further research and consultations from experts to understand its effects on the liberties of our people. As for enforcement, before the imposition of cybercrime laws are sanctioned, there is a strong need for a nationwide cyber literacy program to educate people on proper online use and the sanctions for breaching these laws. The PNGCERT must act as an independent body in order to efficiently enforce cyber laws and also conduct impartial investigations on cyber related allegations. As PNG jurisprudence evolves many of these developments will occur to reflect our changing times.