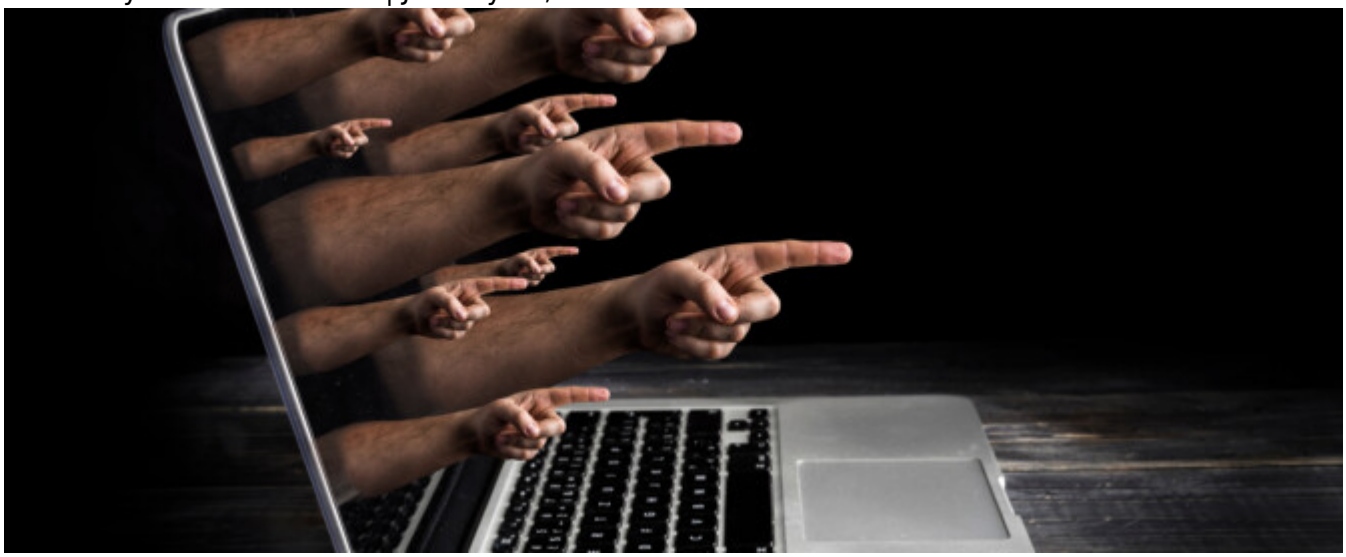
CRIMINALISATION OF CYBERBULLYING IN SOUTH AFRICA

Category: Media and OTT,Privacy Law, Infosec, and POPIA,Technology Law
written by Zandile Mthabela | January 28, 2022



The recent death of a veteran actor, Patrick Shai set tongues wagging after it was reported that he committed suicide following alleged cyberbullying((Kedibone Modise "Somizi Mhlongo probes if cyberbullying played a part in Patrick Shai's passing" IOL news 25 January 2022.)) on social media platforms. The cyberbullying allegedly stemmed from the prominent actor's heated argument with a celebrity. Furthermore, not so long ago, a pupil overdosed on pills after she was cyberbullied.((Phakamile Khumalo "Suicide of Limpopo teen highlights urgent need for a social media policy for schools" Daily Maverick 18 April 2021.)) As more people make use of social media and the internet, we can anticipate an increase in the number of cyberbullying events. The law should be able to provide protection to internet users from cyberbullies.

What is cyberbullying?

Peculiarly, neither cyberbullying nor cybercrime is defined in the Cybercrimes Act, 19 of 2020 ("**Cybercrimes Act**"). Cyberbullying is a form of bullying that occurs when a person bullies another using electronic method. This can take place on social media platforms, such as WhatsApp, FaceBook, text messages, or over the internet. *Eye Witness News*((Mihlali Ntsabo "SA has one of the highest prevalence of cyberbullying" Eye Witness News 25 February 2019.)) newspaper reported that South Africa has one of the highest prevalence of cyberbullying. In November 2021, *The Citizen* reported that:

> "*Before the Covid-19 pandemic, 54% of South African parents were aware of a child experiencing cyberbullying and according to experts, these numbers will only escalate as a result of the huge push to digital mediums brought about by the Covid-19 lockdown*."

Examples of cyberbullying activities include instances where people fight on online platforms, repeatedly sending offensive, cruel, rude and insulting messages and/or threats to harm others. These data messages can be in a form of intimidation. Cyberbullying activities also include sending or posting cruel gossip or rumours about a person. With online schooling, many kids are being

subjected to some form of cyberbullying by being intentionally excluded from an online school group. Other forms of cyberbullying include trolling/baiting a person to engage in a fight, sending pictures of a person in a compromising position, for instance, where a video of a person being attacked or bullied is circulated on social media platforms, or sending a data message that damages a person's reputation, friendships etc. A video of a prominent politician was once circulated on social media platforms.

How is cyberbullying carried out?

Cyberbullying can be carried out in a form of fraping. Fraping means logging into a person's social networking account and impersonating a relevant person's child by posting inappropriate content in that child's name.

Cyberbullying can occur, for instance, where a former lover, a bitter friend, an acquaintance or any person gains access into your social media account and circulates intimate pictures of you on social media platforms, share your secrets and/or embarrassing information online.

Cyberbullying is not limited to circulation of information on social media platforms. It can occur where a person repeatedly sends you inappropriate/offensive messages or subscribes to unwanted websites or dating sites under your name.

Sometimes cyberbullying takes place in a form of identity theft, where a person creates a social media account in your name and impersonates you to your social media friends.

Trickery is when a person will become 'friends' with a person for the purposes of gaining that person's trust so that they confide in them. A cyberbully will then share that person's secrets or embarrassing information publicly online. Once the cyberbully has obtained the information, he/she will unfriend a person and then send the confidante's private information to a third party.

Catfishing is when a person steals a person's online identity, usually photos, and re-creates social networking profiles for deceptive purposes.

Is cyberbullying criminalised under the Cybercrimes Act?

The Cybercrimes Act was enacted for the purposes of combatting cybercrimes and creating offences incidental thereto. Part II of the Cybercrimes Act bears significance to malicious communications which purport to be cyberbullying.

Section 14 of the Cybercrimes Act deals with a data message which incites damage to property or violence. It provides that any person who discloses, by means of an electronic communications service, a data message to a person, group of persons or the general public with the intention to incite the causing of any damage to property belonging to or violence against, a person or a group of persons, is guilty of an offence.

A data message is data generated, sent or received or stored by electronic means where any output of the data is in an intelligible form.

What conduct constitutes cyberbullying?

A data message which threatens persons with damage to property or violence constitutes cyberbullying/cybercrime.

Section 15 of the Cybercrimes Act provides that a person commits an offence if they, by means of an electronic communications service, unlawfully and intentionally discloses a data message, which—

(a) threatens a person with—
(i) damage to property belonging to that person or a related person; or
(ii) violence against that person or a related person; or
(b) threatens a group of persons or any person forming part of, or associated with, that group of persons with—
(i) damage to property belonging to that group of persons or any person forming part of, or associated with, that group of persons; or
(ii) violence against the group of persons or any person forming part of, or associated with, that group of persons,

and a reasonable person in possession of the same information, with due regard to all the circumstances, would perceive the data message, either by itself or in conjunction with any other data message or information, as a threat of damage to property or violence to a person or category of persons mentioned in section 15(a) and (b) above.

In this instance, cyberbullying could take place when a group of people gang up on a person by bullying him/her on social media platforms and/or by inciting violence against that person or his or her property. Property is not limited to a person's tangible property. It can include instances where a person's dignity or reputation is violated.

As much as some perpetrators are identifiable, there are instances where perpetrators act under pseudonymity. In this instance, perpetrators can pretend to be anyone that you know, in an attempt to milk you for information. Once they gain your trust, they can strike. This can happen when you receive an email, a text message etc. (which purports to be from a family member), or anyone that you know.

Fictitious cyberbullies can also threaten to cause harm to your reputation or anyone close to you if you don't give in to their demands. They tend to ravage people on social media platforms by creating untruthful information and then circulating that false information on social media platforms.

Cyberbullies tend to troll people on social media platforms. *Wikipedia* defines a "troll" as:

> *"a person who posts inflammatory, insincere, digressive, extraneous, or off-topic messages in an online community, with the intent of provoking readers into displaying emotional responses, or manipulating others' perception. This is typically for the troll's amusement, or to achieve a specific result such as disrupting a rival's online activities or manipulating a political process. Even so, Internet trolling can also be defined as purposefully causing confusion or harm to other users online, for no reason at all."*

Victim’s recourse against a perpetrator

A victim may lay a charge against a perpetrator with the South African Police Service and apply to a magistrate for a protection order pending the finalisation of the criminal proceedings. In a protection order, a victim may request that the perpetrator be prohibited from bullying/inciting violence against him or her and/or that the service provider remove such threatening data message.

If the court is satisfied that a protection order must be issued and the particulars of the perpetrator, who discloses the data message, or the electronic communications service provider, whose service is used to host or was or is used to disclose the data message, is not known, the court may issue a direction, directing an electronic communications service provider, that is believed to be able to furnish such particulars, to furnish the court in the prescribed manner by means of an affidavit in the prescribed form with certain information that may identify a perpetrator. The Cybercrimes Act also empowers the court to make an assessment on whether or not the electronic communications service provider is in a position to (1) remove the data message or a link to such data message, or (2) disable access to the data message or a link to such data message. This means that in certain circumstances, the court may order that the electronic communications service provider, such as MTN, Twitter, Facebook take down the public post or disable/block the perpetrator from sending you any messages, videos etc.

Penalties imposed by the Cybercrimes Act

The Cybercrimes Act provides that any person who contravenes the provisions of section 14,((Section 14 of the Cybercrimes Act deals with a data message which incites damage to property or violence.)) 15((Section 15 of the Cybercrimes Act deals with a data message which threatens persons with damage to property or violence.)) or 16((Section 16 of the Cybercrimes Act deals with disclosure of data message of intimate image.)) is liable on conviction to a fine or to imprisonment for a period not exceeding three years or to both a fine and such imprisonment.

If a perpetrator is charged with contravening the cybercrime but the evidence does not prove the offence, but proves that the perpetrator committed the crime, the perpetrator may be found guilty of the offence.

Conclusion

The Constitution of the Republic of South Africa is the supreme law of the land. It provides that everyone has the right to privacy, equality, freedom, security and dignity. Cyberbullying and/or trolling a person is inexcusable and does not only have devastating effects on a victim, it is punishable by law and a perpetrator stands to bear the brunt of the law if found guilty of committing the offence. People must be cautious of what they post online. Nowadays, it has become relatively easy for a person to just look your name up on social media platforms and create a fictitious social media account in your name and using your picture. If you post your pictures/videos on social media platforms, you are not spared from becoming a victim to cyberbullying. In order to limit the chances of having your pictures/videos leaked on social media platforms, it is best to not post your pictures/videos on social media platforms, that way, you will somewhat fly under the radar.

Contact us for more good, clear, precise advice.