TAMING THE INTERNET: The good, the bad and the ugly parts of the Computer Misuse and Cybercrimes Act 2018

By Mercy Mutemi

Imagine a world without the Internet.

Now imagine a world where you are not free to say what you want to and where your social media posts could land you in jail. There are those who would love this world. To them, the Internet is encumbered with bigoted, sadistic and misogynistic speech that must be reined in.

Conversely, there are those who see any attempts to regulate online conduct as impinging on their freedom of speech. They believe that once you open the gates for government control, you risk political control and ultimately the death of online democracy.

A third school of thought is that you can never tame the Internet. John Gilmore's famous mantra comes to mind: "The net interprets censorship as damage and routes around it." No matter the laws and policies put in place, bad actors will always find a way to be there.

Regulation of online conduct has now hit close to home. This week, President Uhuru Kenyatta signed into law the Computer Misuse and Cybercrimes Act 2018. Here is what it provides.

The expected

There are offences that are standard in cybercrime legislation across the globe. In Kenya's case, this legislation was way overdue considering that Kenyans were relying on outdated statutes contained in the 1948 Penal Code and the 1998 Kenya Information and Communication Act to try digital crimes.

What most would simply refer to as "hacking" is now covered by the offences of unauthorised access, access with intent to commit a further offence, unauthorised interference and unauthorised interception. Hacking critical information infrastructure (very important public facilities) amounts to cyber espionage, which carries a hefty penalty – 20 years in prison and/or up to Sh10 million in fines.

Spying for Kenya's enemies is also covered under cyber espionage. Each of these offences requires different prerequisites and carry a different sentence. Other variations of these offences are covered under computer fraud and computer forgery. It is laudable that the Act has included the use of social engineering in the list of offences.

Trading in hacking tools, password crackers and social engineering tools is now an offence. Possession of such tools with the intent to use them to commit an offence can earn one a fine of Sh10 million or ten years in jail. Nevertheless, the Act protects "white hat" hackers (computer security specialists who deliberately break into protected systems or networks to assess their security).

Disclosure of a password or access code without permission could lead to a three-year stint in jail, a Sh5 million fine or both. If any of these offences are committed on a protected computer system (government, banks, telecommunications or witness protection systems), the perpetrator gets an enhanced penalty. He or she may be imprisoned for two decades, pay a Sh25 million fine or both.

Sections on mutual assistance and international cooperation in the investigation of cybercrime are commonplace yet necessary given the borderless nature of the Internet. What the Act lacks is an express condition that requests for investigation from other countries that will be subjected to the same legal procedures as local investigations.

> Disclosure of a password or access code without permission could lead to a three-year stint in jail, a Sh5 million fine or both. If any of these offences are committed on a protected computer system (government, banks, telecommunications or witness protection systems), the perpetrator gets an enhanced penalty. He or she may be imprisoned for two decades, pay a Sh25 million fine or both.

Finally, it wouldn't be a complete Kenyan law without the establishment of yet another government body, so the National Computer and Cybercrimes Coordination Committee and its secretariat were created. The Committee has heavy representation by national government agencies. However, the absence of county government representation in the Committee is worrying as it is assumed that counties have no role to play in cybersecurity.

The progressive

The Internet comes with its own share of ills, which, if unchecked, can affect vulnerable groups in society. The natural reaction by legislatures the world over is to over-legislate on online conduct in the hope that the law could re-engineer social order to counter the ever increasing incidents of

anarchy. However, a balance needs to be maintained between laws that could restore this order and laws that would have a chilling effect on online freedom. Here are some of the enacted offences that could be considered progressive.

Cyber harassment

The definition of this offence is wide enough to cover cyber stalking, cyber bullying, doxing, trolling and dogpiling. The determining factor is conduct that causes apprehension, detrimentally affects a person, or is indecent and gross. This offence carries with it a Sh20 million fine, a ten-year prison term or both.

Victims of ongoing cyber harassment will now be able to obtain court orders to put an end to the harassment. This order can be obtained at any time of the day, even outside court working hours. Since cyber harassment is often carried out by trolls hiding behind pseudo accounts, a court may order online service providers to provide the perpetrators' subscriber information, including their name, address, location, email address and phone number.

The framing of the offence, however, presents ambiguity. It is not clear what amounts to "detrimentally affects a person" and "indecent and gross". These are subjective judgements and could be used to undermine freedom of expression.

Child pornography

Children need overzealous protection online from perverts and sometimes from themselves. It is an offence to produce child pornography and publish it. Further, downloading, distributing, exhibiting, selling and "making child pornography available in any way" or simply having it on one's device also amounts to an offence calling for a Sh20 million fine, 25 years in jail or both. Any material showing a child engaging in sexual conduct or a similarly poor depiction amounts to child pornography. An example of this would be the photos recently shared under the #IfikieWazazi trend.

The ambiguous

Clarity in the letter of the law is key. It is equally important that laws prescribing the elements of an offence do so objectively using conduct-specific words. This not only gives a clear guide to the Office of the Director of Public Prosecutions as to when they should bring a criminal charge but also reduces the risk of such a law being declared unconstitutional. Precision is one of the areas where the Act falls short. There is a likelihood that most charges brought under it will be terminated prematurely.

The offence of identity theft and impersonation forbids the fraudulent and dishonest use of the password or unique identification feature of another person. However, the Act offers no definition of what constitutes "unique identification features". And what amounts to "dishonest" use? Is it possible that opening a social media account in the name of another person could now be considered impersonation? Parody accounts, which are used for social commentary, may be at risk.

> Clarity in the letter of the law is key. It is equally important that laws prescribing the elements of an offence do so objectively using conduct-specific words. This not only gives a clear guide to the Office of the Director of Public Prosecutions as to when they should bring a criminal charge but also reduces the risk of such a law being declared unconstitutional. Precision is one of the areas where the Act falls short. There is a likelihood that most charges brought under it will be terminated prematurely.

It is now an offence to hide information that was delivered to you by mistake. Take an email for example. The content of the email may not be relevant to you. However, it is impossible to tell that you were not the intended recipient. The intention of such a provision is unclear.

Unlawfully destroying messages is also an offence. However, the Act does not spell out what amounts to unlawful destruction, which makes the provision baffling.

Section 37 makes it an offence to distribute obscene or intimate images of another person. Use of general words such as "obscene" and "intimate" in laws that limit freedom of expression is unconstitutional. The intention may have been to ban revenge pornography or posting of personal photographs without the subject's consent. Regrettably, we may not realise this protection due to the ambiguous language used in the Act. Failure to restrict this offence to instances where photos are uploaded without consent means that it is generally illegal to post pornographic material online in Kenya, unless the subject of the material posts it.

In a surprising twist, the section on child pornography makes it illegal to download, distribute and disseminate pornographic material or making it available in any way. Could this mean that it is now illegal to watch pornographic material in Kenya even where the actors are adults? Will search engines such as Google be held culpable for "making available" pornographic material? As this is a section on child pornography, is it safer to assume that this was an error in drafting or was this deliberate?

The borderline unconstitutional

There are some sections in the Act that not only make good fodder for public debate but also raise constitutional issues.

Fake news

Any law banning certain types of speech finds itself in conflict with the constitutionally guaranteed freedoms of opinion and expression and of the press. While freedom of expression is not absolute, its limitation can only be to the extent allowed by the Constitution.

The Act has been nicknamed the "Fake News Law". Two sections in the Act have earned it this moniker. One criminalises "false publications" and the other outlaws "publication of false information". Is this a calculated ploy or a play on semantics? In both cases, the Act offers no definition of the word "publish". It will be interesting to see the interpretation adopted by the courts.

The first of these, Section 22, makes it an offence to publish fake news with the intention to deceive people who may treat it as authentic. This offence carries with it a Sh5 million fine, two years in the slammer or both. An obvious dilemma is how the prosecutors will prove that the information was published with the intention to deceive.

> The Act has been nicknamed the "Fake News Law". Two sections in the Act have earned it this moniker. One criminalises "false publications" and the other outlaws "publication of false information". Is this a calculated ploy or a play on semantics? In both cases, the Act offers no definition of the word "publish". It will be interesting to see the interpretation adopted by the courts.

There is, however, a rider in Section 22(2) that states that freedom of expression does not extend to speech that amounts to propaganda for war, incitement to violence, hate speech, advocacy for ethnic

hatred or discrimination, or fake news that negatively affects the rights and reputations of others. These are the exceptions allowed under Article 33 of the Constitution. Such a qualification is necessary for any law that purports to limit a constitutional freedom. The import of this is that any law restricting speech that does not fall into these categories is unconstitutional.

What this means, therefore, is that fake news is only an offence if it amounts to propaganda for war, incitement to violence, hate speech, advocacy for ethnic hatred, advocacy for discrimination, or if it negatively affects the rights and reputations of others. A person charged with the offence of false publication has the right to challenge the charge before a constitutional court if their speech does not fall under the forbidden categories.

The second fake news offence, Section 23, criminalises fake news that is calculated to cause or results in panic, chaos or violence. It also condemns fake news that is likely to discredit the reputation of a person. This offence attracts a Sh5 million fine, a ten-year sentence or both. This section runs afoul of the Constitution. For one, public order is no longer an acceptable limitation to the freedom of expression. This is because words such as panic and chaos are subjective. How do you determine panic or chaos? In addition, the High Court decided last year that an offence prescribing criminal defamation is unconstitutional. This section is likely to suffer a similar fate.

Government surveillance

Every person has the constitutional right to privacy, which means that they have the right not to have their person, home or property searched, to not to have information relating to their family or private affairs unnecessarily revealed and to not to have the privacy of their communications infringed.

However, it is sometimes necessary to impeach the right to privacy, especially to allow for investigation of criminal activity. What the Constitution requires is that such invasion of privacy be carried out according to clear procedures set out in law. The law that allows invasion of privacy by the government must be clear as to the extent of the limitation of the right to privacy. The investigation procedures in the Act feature some questionable provisions.

If a police officer wants to search or seize a computer in the investigation of an offence, they must obtain a search warrant from a court of law. The police officers will then make a list of all the information seized and allow one to copy the contents of the computer before taking it away.

ISPs to surrender subscriber information

As part of the investigative procedures, Internet service providers (ISPs) may be directed to submit information on any of its subscribers. This includes the name, address, location, email address and phone number. Further, they may be directed to either collect traffic data (identity of the sender and recipient of an email, its subject lines and size, titles of any attachments, websites visited by a user and the time spent at each website etc.) on behalf of the police or allow the police to tap into the ISP system in order to do so. Finally, ISPs may be directed to record the content of a subscriber's communication and surrender it to the police or, alternatively, allow police officers to dock into the ISP's system and collect the content data.

All these require court orders. This intermediate step of requiring judicial approval is a necessary check on police power. However, there is a catch. Where police officers consider an investigation "urgent", they are allowed to bypass the courts and directly issue a notice to the ISP to surrender information concerning any of its subscribers. This is a worrying exception that is prone to abuse. It is possible for police officers to cunningly term all their investigations as urgent and go straight to

the ISPs without involving the courts.

ISPs must comply with any police directives as failure to do so would amount to an offence. This is a blatant disregard of the right to privacy, and could be used as a form of retaliation against anti-government entities or individuals. The Act bestows too much authority on investigators/police officers, leaving Internet users vulnerable to the whims of the state or powerful individuals.

> Where police officers consider an investigation "urgent", they are allowed to bypass the courts and directly issue a notice to the ISP to surrender information concerning any of its subscribers. This is a worrying exception that is prone to abuse. It is possible for police officers to cunningly term all their investigations as urgent and go straight to the ISPs without involving the courts.

The unnecessary

The approach taken by this Act is to criminalise all unpleasant online conduct, so much so that it has encroached on the preserve of civil law, which will lead to the overburdening of an already under-resourced Office of the Director of Public Prosecutions. Worse still, the drafting language in many of the sections is vague, which could lead to the dismissal of cases brought under the Act.

The aim of criminal law should be to protect the general interests of the public, not to serve private interests. Where personal loss is occasioned, civil law offers perfect remedies. To go a step further and provide for compensation orders, as Section 45 does, is to usurp the role of civil courts, which are best placed to award damages. Try as we might, it is impossible to restore moral virtue via criminal legislation.

> The aim of criminal law should be to protect the general interests of the public, not to serve private interests. Where personal loss is occasioned, civil law offers perfect remedies.

Cybersquatting

Cybersquatting – the practice of registering domain names, especially of well-known companies, in the hope of re-selling them at a profit – is an offence punishable by a Sh200,000 fine, a two-year imprisonment or both. This would have been best handled under civil law as it raises concerns related to intellectual property and personality rights.

Reversing erroneous payments

More often than not, mobile money users make payments to the wrong recipient. Failure to reverse such erroneous payments is now an offence with a Sh200,000 fine, a two-year imprisonment or both. This is an example of criminalising conduct arising out of private affairs. It would have been more prudent to require a refund policy from the platforms that operate the mobile money service.

Reporting cyber attacks

Every computer user must now report every cyber attack to the National Computer and Cybercrimes Coordination Committee. Failure to do so is an offence. In fighting cybercrime, cooperation is key. Cooperation is achieved by reporting cyber attacks. This alerts other users of impeding attacks and

makes it possible to crowd-source solutions. However, making failure to report such attacks a crime is extreme. In other jurisdictions, only large organisations dealing in large amounts of data and monetary transactions are required to report. Failure to do so is not criminal but attracts administrative fines.

Failure to surrender passwords after employment

This is yet another superfluous offence. At the end of a contract of employment, one should surrender passwords to company computers and access codes. Failure to do so constitutes an offence. This would ordinarily give rise to a civil claim for breach of contract, which makes criminalising of the offence needless. The law is thus encroaching on a matter that is already handled by employers through contracts with their employees.

This is what the Computer Misuse and Cybercrimes Act, 2018 provides. I hope that this equips you adequately to participate in public discourse on the Act.

Published by the good folks at The Elephant.

The Elephant is a platform for engaging citizens to reflect, re-member and re-envision their society by interrogating the past, the present, to fashion a future.

Follow us on Twitter.