

Legal Development in Kenya Enactment of the Computer and Cybercrimes Bill 2017

By Andrew Ndikimi, O&M Law LLP, Kenya

BRIEF SUMMARY ON THE COMPUTER AND CYBERCRIMES ACT, 2017

INTRODUCTION:

The President of the Republic of Kenya assented to The Computer and Cybercrimes Act, 2017 (the “Act”) on 16th May 2018. Below is a summary of its provisions:

Objectives:

The Act was to provide for a framework to prevent and control the threat of cybercrime, i.e. offences against computer systems.

The Act stipulates its objectives as:

- (1) Protecting the confidentiality , integrity and availability of computer systems, programs and data;
- (2) Prevent the unlawful use of computer systems (including mobile devices);
- (3) Facilitate the investigation and prosecution of cybercrimes; and
- (4) Facilitate international/states cooperation on matters provided for under the Act.

OFFENCES AND PENALTIES/ PUNISHMENT:

The Act introduces numerous offences related to computers, computer systems, data, storage media, telecommunication devices, hand held devices etc and prescribes the punishment for each such offence. Some of the offences introduced by the Act include the following:

- 1) Unauthorised access to computer systems;
- 2) Access to computer systems with intent to commit a further offence;
- 3) Unauthorised interception of data, computer programs, computer systems etc;
- 4) Manufacture, selling, importation, supply, distribution etc of illegal devices, programs, passwords, access codes etc;
- 5) Cyber Spying and cyber espionage;
- 6) False, misleading or fictitious publication of data or information with intent that such data be acted upon as authentic;
- 7) Publishing of child pornographic material through a computer system;
- 8) Computer forgery and fraud; and
- 9) Cyber stalking and cyber-bullying.

The Act also makes it an offence for any person to aid or abet any person in the commission of any crime and criminalized attempting to commit any crime (attempt to commit an offence) and provides for the punishment in both instances.

The Act provides for stiff penalties in relation to computer systems related offences.

We have discussed the ingredients of each of these offences and their punishments below:

1) Unauthorised access:

The Act stipulates that a person who causes a computer system to perform a function infringing security measures, with intent to gain unauthorised access (and knowing that the access is unauthorised) commits an offence. The punishment for this is a fine **not exceeding Kshs. 5,000,000/- or imprisonment for a term not exceeding 3 years, or both**. The Act define “unauthorised access”, as access by a person to a computer system where the person: (i) is not entitled to control or access such computer sytem, program or data; and/or (ii) does not have consent from any person who is entitled to access the computer system through any function to the program or data.

2) Access with intent to commit a further offence

A person who commits any offence, with intent to commit a further (second) offence/crime, or facilitates the commission of such a further (second) offence also commits an offence. The punishment for this is a fine **not exceeding Kshs. 10,000,000/- or imprisonment for a term not exceeding 10 years, or both**.

3) Unauthorised interception/interference

Any person who intentionally and without authorisation does any act which causes an unauthorised interference to a computer system, program or data commits and offence. The punishment for this is a fine **not exceeding Kshs. 10,000,000/- or imprisonment for a term not exceeding 5 years or both**. The Act defines ‘unauthorised interception/ interference’ as where such offender: (i) is not legally entitled to cause such interference; or (ii) does not have consent to interfere with such computer system, data etc, from a person with legal authority to do so. Further any person who commits such offenses, and the offence leads to significant financial loss to any third party, threat to national security, causes physical injury or death to any third party or causes threat to public health or public safety is liable to **a fine not exceeding Kshs. 20,000,000/- or imprisonment for a term not exceeding 10 years, or both**.

The Act also criminalizes intentional and unauthorised interception of transmission of data to or from a computer system over a telecommunication system. The punishment for this is **a fine not exceeding Kshs. 10,000,000/- or imprisonment for a term not exceeding 5 years, or both**. In addition, where such an offence leads to significant financial loss to any third party, threat to national security, causes physical injury or death to any third party or causes any threat to public health or public safety, such a person shall be liable **to a fine not exceeding Kshs. 20,000,000/- or imprisonment for a term not exceeding 10 years, or both**.

4) Illegal devices, programs, passwords and access codes etc

The Act criminalizes the manufacture, adaption, selling, procurement, importation, supplying, distribution and/or availing of any device, program, computer password, access code or similar data (collectively referred to as “**Illegal Devices and Access Codes**”) designed or adapted primarily for purpose of committing any offence under the Act. The punishment for this is **a fine not exceeding Kshs. 20,000,000/- or imprisonment for a term not exceeding 10 years, or both**. Further any person who knowingly receives or is found in possession of any Illegal Devices and Access Codes

with intent to use the same for hacking (without sufficient justification or excuse) shall be liable to **a fine not exceeding Kshs. 10,000,000/- or imprisonment for a term not exceeding 5 years, or both**. However, no offence is committed where a person found with such Illegal Devices and Access Codes can demonstrate that the same was: (i) for any legal and authorised training, testing or protection of a computer system; or (ii) undertaken pursuant to a court order or pursuant to the Act. Such therefore would be defences in such a case.

The Act also criminalizes unauthorised disclosure of any passwords, access codes or other means of gaining access to any program or data held in any computer system. The punishment for this is **a fine not exceeding Kshs. 5,000,000/- or imprisonment for a term not exceeding 3 years, or both**. Further, any person who commits such an offence for any wrongful/unlawful gain to himself, unlawful purpose or to occasion any loss to any third party shall be liable to **a fine not exceeding Kshs. 10,000,000/- or imprisonment for term not exceeding 5 years, or both**.

5) Cyber spying and cyber espionage

The Act now criminalizes cyber spying and cyber espionage. This is what is commonly known as 'hacking'. The Act provides a very stiff penalty for this. It provides stiff and prohibitive imprisonment term and fine for criminalizes cyber spying or cyber espionage. The punishment for this is **a fine not exceeding Kshs. 10,000,000/- or imprisonment for a term not exceeding 20 years, or both**. Further, it provides that if any person unlawfully and intentionally undertakes cyber spying or cyber espionage to directly or indirectly benefit a foreign state/country against the Republic of Kenya, the same is punishable by imprisonment for **a term not exceeding 20 years or a fine not exceeding Kshs. 10,000,000/-, or both**.

In addition, any person who allows another person to undertake cyber spying or cyber espionage for the direct or indirect benefit of a foreign state against the Republic of Kenya, shall be liable to imprisonment for **a term not exceeding 10 years or a fine not exceeding Kshs. 5,000,000/- or both**.

6) False publication (publishing false news)

The Act also criminalizes publishing false, misleading or fictitious data or misinforming with intent that the data shall be considered or acted upon as authentic/true. The punishment for this is imprisonment for **a term not exceeding 2 years or a fine not exceeding Kshs. 5,000,000/-, or both**.

7) Child pornography

The Act further criminalizes child pornography. It provides that any person who intentionally publishes child pornography through a computer system, produces child pornography for purpose of its publication through a computer system or is found in possession of child pornographic material in a computer system or data storage medium, shall be liable to imprisonment for **a term not exceeding 25 year or a fine not exceeding Kshs. 20,000,000/-, or both**. However, the Act provides that it shall be a defence if such a person establishes that such material was intended for a bona fide scientific, research, medical or law enforcement purpose. The Act defines a "child" as any person below the majority age. "Child pornography" includes both visual and audio data.

8) Computer forgery and fraud.

Any person who commits computer forgery, through **intentional** input, alteration, deletion or suppression of computer data resulting in inauthentic/false/incorrect data, with an intent that it be considered as authentic/true, is guilty of a criminal offence. The punishment for this is **imprisonment for a term not exceeding 5 years or a fine not exceeding Kshs. 10,000,000/-, or both**. Further, any person who undertakes computer forgery for wrongful/unlawful gain, wrongful loss to another person

or for economic benefit to himself or another person, is liable to imprisonment for **a term not exceeding 10 years or a fine not exceeding Kshs. 20,000,000/-, or both.**

The Act also prohibits computer fraud. It states that any person who fraudulently and dishonestly gains, occasions unlawful loss to another person or obtains economic benefit for himself or for another person through computer fraud is guilty of an offence. The punishment for this is **imprisonment for a term not exceeding 10 years or a fine not exceeding Kshs. 20,000,000/-, or both.**

9) Cyberstalking and cyber-bullying

The Act prohibits cyber stalking and cyber bullying. Cyberstalking and cyber-bullying has been a big problem in Kenya especially on social media and has even lead victims to committing suicide in certain instances¹. It provides that any person who, individually or with others, willfully and repeatedly communicates, directly or indirectly, with another person knowing that such communication: (i) is likely to cause such a person apprehension or fear of violence to them or damage or loss on that person's property; or (ii) will detrimentally affect that person, commits an offence whose punishment is **imprisonment for a term not exceeding 10 years or a fine not exceeding Kshs. 20,000,000/-, or both.** This Act therefore puts cyberstalkers and cyber-bullies on notice as the punishment for such is a severe fine and a prolonged imprisonment term.

The Act however provides that it shall be a defence if such a person accused of cyberstalking or cyber-bullying demonstrates that that his conduct was pursued: (i) for purpose of preventing or detecting a crime; (ii) pursuant to any legislation/law; or (iii) in public interest.

In addition to the above nine (9) offences introduced by the Act, the Act also provides of the following:

Aiding or abetting in the commission of an offence under the Act

The Act criminalizes assisting, aiding or abetting a third party in the commission of a computer systems related offence. It stipulates that any person who knowingly and willfully assists another person to commit any offence is liable **to imprisonment for a term not exceeding 4 years or a fine not exceeding Kshs. 7,000,000/-, or both.**

Attempt to commit an offence

The statute also criminalizes any attempt to commit a computer systems related offence. Any attempt (willingly and knowingly) by any person to commit an offence under the Act is punishable by **imprisonment for a term not exceeding 4 years or a fine not exceeding Kshs. 7,000,000/-, or both.**

Offences by body corporates

The Act treats corporate offenders differently from individual offenders and provides a stiffer penalty (fine) for corporate offenders. It provides that if an offence under the Act is committed by a body corporate (e.g. a company, association, government body, institution etc), such body corporate shall be liable to **a fine not exceeding Kshs. 50,000,000/-**. The Act also makes principal officers of such corporate offenders culpable of any offence committed by the corporate where they were aware of the same or failed to exercise due diligence to prevent the same. It provides that the principal officers of such body corporates (unless they prove that the offence was committed without their knowledge or consent and that they exercised due diligence to prevent the commission of the offence) will be liable to imprisonment for **a term not exceeding 3 years or a fine not exceeding Kshs. 5,000,000/-, or both.**

¹ Please see <https://nairobi.news.nation.co.ke/life/cyber-bullying-womans-suicide/>

Enhancement of penalty in relation to protected computer systems

The Act also provides a stiffer penalty for offences relating to any protected computer system. It provides that any person who commits any of the previously discussed offences on a **protected computer system**, shall be liable to **a fine not exceeding Kshs. 25,000,000/- or imprisonment for a term not exceeding 20 years, or both**. The Act defines a “**protected computer system**” as a computer system used in connection with: (i) the security, defence or international relations of Kenya; (ii) existence of identity of a confidential source of information relating to enforcement of criminal law; (iii) provision of services relating to communications, infrastructure, banking and financial services, payment and settlement systems and instruments, public utilities or public transportation and delivery of digitalized government services; (iv) protection of public safety, including emergency services e.g. police, civil defence and medical services; (v) provision of national registration systems; or (vi) such other systems as the Cabinet Secretary for Information Communication and Technology may prescribe.

Confiscation, forfeiture and compensation orders

The Act provides that a court may order the confiscation or forfeiture of monies, proceeds, properties and assets purchased or obtained through commission of an offence. Further the court can make an order for restitution (restoration/ re-compensation) of any asset gained from the commission of an offence. Where a person is found culpable of an offence under the Act or any other law relating to a computer system, the court may order that any such person be paid compensation for any resultant losses. Such order for compensation is recoverable as a civil debt.

General punishment

Any person who commits an offence under any other Kenyan law relating to any computer system, shall be liable to **a fine not exceeding Kshs. 3,000,000/- and imprisonment for a term not exceeding 4 years, or both**.

OTHER RELEVANT PROVISIONS:

Search with warrants

The Act gives certain powers to police officers (or any other person authorised by law), having reasonable grounds to believe that there may be a certain computer system, data or program that is required for any investigations or legal proceedings or acquired pursuant to commission of an offence. Such officers are allowed to apply to court for search warrant to enter any premises for purposes of accessing, searching and seizing such data. However, such an officer must satisfy the court: (i) as to the reason why he believes that such material may be found at the premises to be searched; (ii) show that the search may be frustrated or seriously prejudiced unless an investigating officer may at the first instance on arrival at the premises secure entry to the premises; (iii) identify and explain the type of evidence sought; and (iv) explain measures that shall be taken to prepare and ensure that the search and seizure is carried out through technical means such as imaging, mirroring or copying of relevant data and not through physical custody of computer system, program, data or storage medium.

Search without a warrant

Further, the Act allows such investigating officers to search such premises without a warrant where the officer suspects that an offence has been committed and to take possession of such computer system.

Failure to comply with court orders is an offence

The Act provides that any person who fails to comply with the court's order is liable to **imprisonment for a term not exceeding 3 years or a fine not exceeding Kshs. 5,000,000/-, or both**.

The Act further allows a police officer, where he has reasonable grounds to believe that there is any data stored in any computer system which is required for a criminal investigation or there is risk or is

vulnerable to be modified, deleted, lost or destroyed or rendered inaccessible, to serve notice on any person in possession of such data requiring such a person to preserve such data etc or disclose it to him.

Telecommunications Service providers

The Act also allows any police officer, pursuant to a court order, to have access to traffic data of any telecommunications service provider (e.g. mobile network providers) and collect or record such data, where he has reasonable ground to believe that such data is required for investigations.

The court in giving such orders must ensure that the police officer: (i) states the grounds upon which he believes that the data sought is available; (ii) states the type of data sought; (iii) identifies and explain the subscribers, users or unique identifiers of the subject; (iv) states the identifiable offences suspected to have been committed; and (v) explains the measures he will take to prepare and ensure that the data will be procured while maintaining the privacy of other users, customers and third parties and without disclosure of data to any party who is not a part of such investigating team. However, such collection of data shall not be allowed for a period exceeding 6 months, unless with the court orders otherwise.

Any telecommunications service provider who refuses to comply with such an order shall be liable to **a fine not exceeding Kshs. 10,000,000/- in the case of a corporation or in the case of a principal officer of the service provider, a fine not exceeding Kshs. 5,000,000/- or imprisonment for a term not exceeding 3 years, or both.**

Obstruction of an officer

Any person who obstructs an officer undertaking his duties under the Act, including by destruction of data or failing to comply with the officer's request is liable to **a fine not exceeding Kshs. 5,000,000/- or imprisonment for a term not exceeding 3 years, or both.**

Misuse of powers by a police officer

On the same breath, an officer who misuses his powers under the Act commits an offence and is liable to **a fine not exceeding Kshs. 5,000,000/- or imprisonment for a term not exceeding 3 years, or both.**

Appeals

Any person aggrieved by a decision or order of the court may appeal to the High Court or Court of Appeal (as the case may be) **within 30 days from the date of the decision or order.**

International cooperation

The Act also allows the office of the Attorney General (the Central Authority) to make a request for mutual legal assistance to a requested state (country) to investigate, collect evidence, prosecute, repatriate etc any person who commits an offence under the Act. The state may also receive such a request from a requesting state.

Forfeiture

In addition to the penalties prescribed above, a court may order the forfeiture of any apparatus, device or thing that it deems appropriate to do, to the Communication Authority of Kenya, e.g. hacking devices, infringing data etc.

Conclusion

The Act introduces nine (9) main offences and provides severe punishment for these offences, including huge fines and prolonged jail terms. With this new legislation, it will be interesting to see the punishment that courts will grant offenders as the punishment stipulated on the Act are the maximum punishments and courts are allowed to exercise their discretion in sentencing and most states provide for the maximum punishment.

For more information, please contact:



© Andrew Ndikimi
Kenyan advocate
O&M Law LLP
Tel. +254722613888/ +254739935929
andrew@omlaw.co.ke
www.omlaw.co.ke

Andrew Ndikimi, is a Kenyan advocate with ten (10) years post admission experience and is a senior lawyer at O&M Law LLP, Park Place, Limuru Road & 2nd Parklands Avenue Junction, Nairobi, Kenya.