
THE CYBER CRIMES ACT, 2025

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY PROVISIONS

Section

1. Short title and commencement
2. Interpretation

PART II

OFFENCES

3. Prohibition of unauthorised access to computer system and data
4. Prohibition of unauthorised interference with computer system and data
5. Prohibition of unauthorised disclosure of data relating to critical information or critical information infrastructure
6. Prohibition of unauthorised possession of data relating to critical information or critical information infrastructure
7. Illegal acquisition of data
8. Prohibition of introduction of malicious software into computer system
9. Illegal system interference
10. Prohibition of recording of private conversation without prior notice
11. Prohibition of illegal devices and software
12. Prohibition of computer related misrepresentation and computer fraud
13. Prohibition of cyber extortion
14. Prohibition of identity related crimes
15. Prohibition of child pornography
16. Prohibition of child solicitation
17. Prohibition of child grooming
18. Prohibition of on-line human trafficking
19. Transmission of deceptive electronic communication

20. Prohibition of use of computer or computer system for offences
21. Prohibition of unlawful disclosure of details of investigation
22. Prohibition of harassment, humiliation etc.,..
23. Prohibition of cyber attack
24. Prohibition of cyber terrorism
25. Offences resulting in incapacity or destruction of critical information and critical information infrastructure

PART III

GENERAL PROVISIONS

26. Entering into agreement
27. Search and seizure by law enforcement officer
28. Restoration and forfeiture of property
29. Assistance
30. Expedited preservation order
31. Disclosure of traffic data
32. Collection of traffic data
33. Extradition

GOVERNMENT OF ZAMBIA

ACT

No. 4 of 2025

Date of Assent: 8th April, 2025

An Act to provide for offences relating to computers and computer systems; provide for the protection of persons against cyber crimes; provide for child online protection; and provide for matters connected with, or incidental to, the foregoing.

[15th April, 2025

ENACTED by the Parliament of Zambia.

Enactment

PART I
PRELIMINARY PROVISIONS

1. This Act may be cited as the Cyber Crimes Act, 2025, and shall come into operation on the date appointed by the Minister by statutory instrument.

Short title and commencement

2. In this Act, unless the context otherwise requires—

Interpretation

“access” has the meaning assigned to the word in the Electronic Communications and Transactions Act, 2021;

Act No. 4 of 2021

“article” has the meaning assigned to the word in the Cyber Security Act, 2025;

Act No. of 2025

“child” has the meaning assigned to the word in the Constitution;

Cap. 1

“child grooming” means a process, behaviour or an action used to establish a relationship of trust or an emotional connection with a child for purposes of facilitating or encouraging sexual conduct with that child;

“child pornography” means a material whether real or simulated, that depicts a presentation or a representation of—

- (a) a child engaged in explicit sexual conduct;
- (b) an image of a child engaged in sexually explicit conduct; or
- (c) the sexual parts of a child for sexual purposes;

“child solicitation” means persuading, luring, or attempting to persuade or lure a child into sexual activity through the use of a computer or computer system, regardless of the outcome;

Act No. 4 of
2021

“communication” has the meaning assigned to the word in the Electronic Communications and Transactions Act, 2021;

“communications data” means information relating to the usage of an electronic communications service;

Act No. 4 of
2021

“computer” has the meaning assigned to the word in the Electronic Communications and Transactions Act, 2021;

Act No. of
2025

“computer data” has the meaning assigned to the words in the Cyber Security Act, 2025;

Act No. of
2025

“computer data storage medium” has the meaning assigned to the words in the Cyber Security Act, 2025;

Act No. of
2025

“computer system” has the meaning assigned to the words in the Cyber Security Act, 2025;

Act No. of
2025

“critical information” has the meaning assigned to the words in the Cyber Security Act, 2025;

Act No. of
2025

“critical information infrastructure” has the meaning assigned to the words in the Cyber Security Act, 2025;

Act No. of
2025

“cyber attack” has the meaning assigned to the words in the Cyber Security Act, 2025;

“cyber crime” means a crime committed in, by or with the assistance of, a simulated environment or state of connection or association with electronic communications or networks including the internet;

Act No. of
2025

“cyber security” has the meaning assigned to the words in the Cyber Security Act, 2025;

Act No. of
2025

“cyber security risk assessment” has the meaning assigned to the words in the Cyber Security Act, 2025;

“cyber terrorism” means the use of a computer or computer system to attack or threaten to attack computers, networks and information stored on the computers and networks with intent to intimidate or coerce a government or its people in furtherance of political or social objectives and to cause severe disruption or widespread fear in society;	
“device” has the meaning assigned to the word in the Cyber Security Act, 2025;	Act No. of 2025
“digital file” means a computer file that contains computer data or information in electronic form, which can be stored, processed, and transmitted;	
“electronic communication” has the meaning assigned to the words in the Electronic Communications and Transactions Act, 2021;	Act No. 4 of 2021
“electronic communications service” has the meaning assigned to the words in the Information and Communication Technologies Act, 2009;	Act No. 15 of 2009
“harassment” has the meaning assigned to the word in the Anti-Gender Based Violence Act, 2011 and the word “harass” shall be construed accordingly;	Act No. 1 of 2011
“header information” means identifying or descriptive data that is included at the beginning of a digital file or electronic communication;	
“hinder” includes—	
(a) disconnecting the electricity supply to a computer or computer system;	
(b) causing electromagnetic interference to a computer system;	
(c) corrupting a computer or computer system; or	
(d) damaging, deleting, deteriorating, altering or suppressing a computer programme;	
“interception” has the meaning assigned to the word in the Cyber Security Act, 2025;	Act No. of 2025
“internet connection record” has the meaning assigned to the words in the Cyber Security Act, 2025;	Act No. of 2025
“information infrastructure” has the meaning assigned to the words in the Cyber Security Act, 2025;	Act No. of 2025
“information system” has the meaning assigned to the words in the Electronic Communications and Transactions Act, 2021;	Act No. 4 of 2021

Act No. of 2025	<p>“judge” means a judge of the High Court;</p> <p>“law enforcement officer” has the meaning assigned to the words in the Cyber Security Act, 2025;</p> <p>“malicious software” means a computer programme intentionally designed to—</p> <ul style="list-style-type: none">(a) gain unauthorised access to a computer, computer system or computer data;(b) cause unauthorised modification or transmission of computer data;(c) deprive access to a computer or computer system; or(d) interfere with normal computer or computer system usage; <p>“monitor” means to observe and analyse digital activities including network traffic, system logs, or user behavior, with the goal of detecting and preventing cyber security threats or cyber crimes;</p>
Act No. of 2025	<p>“penetration testing” has the meaning assigned to the words in the Cyber Security Act, 2025;</p> <p>“pornography” means audio or visual material whether real or simulated that depicts images of a person engaged in explicit sexual conduct;</p>
Act No. of 2025	<p>“private communication” has the meaning assigned to the words in the Cyber Security Act, 2025;</p> <p>“sexual conduct” includes sexual intercourse whether between persons or between a person and an animal, masturbation, sexual sadistic or masochistic abuse or lascivious exhibition of the genitals or pubic area of any person;</p> <p>“telecommunication infrastructure” means infrastructure that facilitates the conveyance of signals by wire, radio, optical, or other electro-magnetic means, including satellite networks and electronic communication service provider networks;</p>
Act No. 11 of 2008	<p>“trafficking in persons” has the meaning assigned to the words in the Anti-Human Trafficking Act, 2008; and</p>

“traffic data” means digital data that—

- (a) relates to a communication by means of a computer system;
- (b) is generated by a computer system that is part of the chain of communication; and
- (c) shows the communication’s origin, destination, route, time, date, size, duration or the type of underlying services.

PART II

OFFENCES

3. (1) A person shall not intentionally and without lawful authority or in excess of authority, infringe any security measure, access or monitor a computer system or any part of a computer system of another person.

Prohibition of unauthorised access to computer system and data

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

4. (1) A person shall not intentionally and without lawful authority, interfere with data or a computer system of another person in a way which—

Prohibition of unauthorised interference with computer system and data

- (a) causes the data or computer system to be modified, destroyed, altered or otherwise rendered ineffective;
- (b) obstructs, interrupts or interferes with another person’s lawful use of data;
- (c) denies access to data to a person who is authorised to access it;
- (d) causes data of another person to deteriorate; or
- (e) deletes data of another person.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

5. (1) A person shall not intentionally and without lawful authority, communicate, disclose or transmit data, information, a programme, an access code or a command relating to critical information or critical information infrastructure to any person not authorised to access such data, information, programme, access code or command.

Prohibition of unauthorised disclosure of data relating to critical information or critical information infrastructure

	<p>(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding seven hundred thousand penalty units or to imprisonment for a term not less than seven years and not exceeding fifteen years.</p>
Prohibition of unauthorised possession of data relating to critical information or critical information infrastructure	<p>6. (1) A person shall not intentionally and without lawful authority possess unauthorised data relating to critical information or critical information infrastructure.</p> <p>(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding seven hundred thousand penalty units or to imprisonment for a term not less than seven years and not exceeding fifteen years.</p>
Illegal acquisition of data	<p>7. (1) A person shall not intentionally and without lawful authority, using a computer or computer system acquire trade secrets or proprietary or confidential data by accessing or copying of electronic files.</p> <p>(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding one million penalty units or to imprisonment for a term not exceeding ten years, or to both.</p>
Prohibition of introduction of malicious software into computer system	<p>8. (1) A person shall not intentionally introduce or spread malicious software into a computer or computer system of another person.</p> <p>(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding one million five hundred thousand penalty units or to imprisonment for a term not exceeding fifteen years, or to both.</p>
Illegal system interference	<p>9. (1) A person commits an offence if that person intentionally and without lawful authority—</p> <p>(a) hinders or interferes with a computer or computer system of another person; or</p> <p>(b) renders a computer or computer system incapable of providing normal services to its legitimate users.</p> <p>(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.</p>

10. (1) A person commits an offence if that person, using a device, records a private conversation without notifying the parties to the conversation, whether or not that person is a party to the private conversation.

Prohibition
of recording
of private
conversation
without
prior notice

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

(3) Despite subsection (1), it shall not be an offence to record a private conversation where—

- (a) the private conversation is unintentionally recorded through a device;
- (b) a law enforcement officer reasonably suspects that there is—
 - (i) a threat to life or an imminent threat of serious violence to a person;
 - (ii) a threat of substantial damage to property; or
 - (iii) an offence under any written law that may be committed; or
- (c) it is reasonably necessary for the protection of the lawful interests of a party to the conversation.

11. (1) A person commits an offence if that person, intentionally and without lawful authority, produces, sells, procures for use, imports, exports, distributes or makes available a—

Prohibition
of illegal
devices and
software

- (a) device or a computer programme, that is designed or adapted for the purpose of committing an offence;
- (b) computer password, access code or any other electronic authentication data by which the whole or any part of a computer or computer system is capable of being accessed; or
- (c) software code that is capable of causing damage to a computer or computer system.

(2) A person convicted of an offence under subsection (1), is liable, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

Prohibition
of computer
related
misrepresenta-
tion and
computer
fraud

12. (1) A person shall not intentionally and without lawful authority, input, alter, delete, or suppress computer data resulting in inauthentic data, with the intent that the inauthentic data be considered or acted on by another person as if it were authentic, regardless of whether the data is directly readable or intelligible.

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

(3) A person commits an offence if that person with intent to defraud or deceive another person for the purpose of procuring an economic benefit for oneself or another person—

- (a) inputs, alters, deletes or suppresses electronic data; or
- (b) interferes with the functioning of a computer or computer system.

(4) A person who is convicted of an offence under subsection (3), is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

Prohibition
of cyber
extortion

13. (1) A person commits an offence if that person, through a computer system with intent to extort or gain anything from any person—

- (a) accuses or threatens to accuse any person of committing a crime or offering or making any solicitation or threat to any person as an inducement to commit or permit the commission of a crime;
- (b) threatens that any person shall be accused by any other person of commission of an offence;
- (c) knowing the contents of the writing, causes any person to receive any writing containing such accusation or threat;
- (d) knowingly transmits any communication containing any threat to cause damage to a computer system with the intent to extort from any person any money or other thing of value;
- (e) obtains any advantage from another person;

(f) compels another person to perform or to abstain from performing any act; or

(g) publishes or threatens to publish a private sexual photograph or film of a person who appears in the photograph or film.

(2) A person convicted of an offence under subsection (1), is liable to a fine not exceeding seven hundred thousand penalty units or imprisonment for a period not exceeding seven years, or to both.

14. (1) A person shall not, intentionally and without lawful authority, with intent to commit an offence—

Prohibition
of identity
related
crimes

(a) transfer, possess or use a means of identification of another person; or

(b) make use of an electronic signature or password of another person.

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding one million penalty units or to imprisonment for a term not exceeding ten years, or to both.

15. (1) A person commits an offence if that person intentionally—

Prohibition
of child
pornography

(a) produces child pornography for the purpose of its distribution through a computer or computer system;

(b) sells, imports, exports or makes available any pornography to a child through a computer or computer system;

(c) compels, invites or allows a child to view pornography through a computer or computer system;

(d) offers or makes available child pornography through a computer or computer system;

(e) distributes or transmits child pornography through a computer or computer system;

(f) procures and obtains child pornography through a computer or computer system for oneself or for another person;

(g) possesses child pornography in a computer or computer system or on a computer data storage medium; or

(h) obtains access of child pornography through a computer or computer system.

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to imprisonment for a term of not less than fifteen years and not exceeding twenty-five years.

(3) Subsections (1)(g) and (h) shall not apply to a person performing a bonafide function of a law enforcement officer.

Prohibition
of child
solicitation

16. (1) A person shall not intentionally, using a computer or computer system—

(a) arrange a meeting with a child with the intent of abusing or engaging in sexual activity with the child or producing child pornography, whether or not that person takes any steps to effect such a meeting;

(b) communicate with or attract a child for the purpose of making it easier to procure the child to engage in sexual activity with that person or another person; or

(c) recruit a child to participate in pornographic performances intended to be produced or recorded with or without the intention to distribute such material through a computer or computer system.

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to imprisonment for a term not exceeding twenty-five years.

Prohibition
of child
grooming

17. (1) A person shall not intentionally, using a computer or computer system, groom a child for the purpose of facilitating or encouraging sexual conduct with that child.

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to imprisonment for a term of not less than fifteen years and not exceeding twenty-five years.

Prohibition
of on-line
human
trafficking

18. (1) A person shall not, using a computer or computer system, intentionally engage in trafficking in persons.

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to imprisonment for a term not less than twenty-five years and may be liable to imprisonment for life.

-
- 19.** (1) A person shall not intentionally and without lawful authority—
- Transmission of unsolicited deceptive electronic communication
- (a) use a computer or computer system to relay or retransmit electronic communications to deceive or mislead users of a computer or computer system as to the origin of such communication;
 - (b) initiate the transmission of multiple electronic messages from or through a computer or computer system for purposes of causing harm or disrupting the computer or computer system;
 - (c) establish a software application system with the intent to deceive or mislead a visitor to the software application system as to the authenticity of the software application system for the purpose of gaining unauthorised access to information to commit an offence; or
 - (d) falsify header information in an electronic communication and initiate the transmission of such electronic communication to commit an offence, deceive or mislead users.
- (2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding seven hundred thousand penalty units, or imprisonment for a term of not less than two years and not exceeding seven years, or to both.
- 20.** (1) A person shall not use a computer or computer system for an activity which constitutes an offence under any written law.
- Prohibition of use of computer or computer system for offences
- (2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to the penalty specified for that offence in the applicable written law.
- 21.** (1) A person who receives an order relating to a criminal investigation under this Act, shall not without lawful excuse, disclose—
- Prohibition of unlawful disclosure of details of investigation
- (a) that an order has been made;
 - (b) anything done under the order; or
 - (c) any data collected or recorded under the order.
- (2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

Prohibition
of
harassment,
humiliation,
etc.

22. (1) A person shall not use a computer or computer system to—

- (a) publish or transmit electronic data that is obscene, vulgar, lewd, lascivious or indecent with intent to humiliate, harass or cause substantial emotional distress to another person ; or
- (b) repeatedly send to another person electronic data that is obscene, vulgar, lewd, lascivious or indecent with intent to humiliate or harass the other person to the detriment of that person's health, emotional well-being, self-esteem or reputation.

(2) A person shall not use a computer or computer system to disseminate information, statement or image, knowing the same to be false that—

- (a) causes damage to the reputation of another person; or
- (b) subjects another person to public ridicule, contempt, hatred or embarrassment.

(3) A person who contravenes subsection (1) or (2), commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

Prohibition
of cyber
attack

23. (1) A person shall not carry out a cyber attack.

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

Prohibition
of cyber
terrorism

24. (1) A person commits an offence if that person uses a computer or computer system to—

- (a) incite, urge, teach or train any person in or out of the Republic to commit or participate in the commission of a terrorist act or an offence under the Anti-Terrorism and Non-Proliferation Act, 2018;
- (b) incite or attempt to incite ethnic divisions among the people of the Republic;
- (c) encourage, entice, induce or motivate any person in the Republic to join a terrorist group or to commit or participate in the commission of an offence in relation to financing of terrorism under the Anti Terrorism and Non-Proliferation Act, 2018.

Act No. 6 of
2018

Act No. 6 of
2018

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to imprisonment for life.

25. Despite the penalties set out in any other provision of this Act or any other written law, a person is liable, on conviction, to a fine not exceeding one million penalty units or to imprisonment for a term not exceeding twenty five years, or to both where that person commits an offence under this Act or any other written law and the offence results in the incapacity or destruction of, or interference with, electronic data, computer or computer system or a computer network that—

Offences resulting in incapacity or destruction of critical information and critical infrastructure

- (a) is exclusively for the use of critical infrastructure of the Republic; or
- (b) affects the use, or impacts the operation or critical infrastructure of the Republic.

PART III GENERAL PROVISIONS

26. Subject to the Mutual Legal Assistance in Criminal Matters Act, the Republic may enter into an agreement with a foreign State or international body relating to the provision of mutual assistance and cooperation in the investigation and prosecution of—

Entering into agreement
Cap. 98

- (a) an offence committed under this Act;
- (b) any offence under the laws of the Republic which is or was committed by the use of an article; or
- (c) an offence substantially similar to an offence recognised in the Republic which is or was committed by the use of an article, in the foreign State.

27. (1) A law enforcement officer may, with a warrant, enter any premises to search and seize a computer or computer system, where a computer or computer system contains material—

Search and seizure by law enforcement officer

- (a) or evidence necessary in proving an offence; or
- (b) that has been acquired by a person as a result of an offence.

(2) A law enforcement officer who is undertaking a search under this Act may, where the law enforcement officer has reasonable grounds to believe that the data sought is stored in another device, computer or computer system or part of it, and such data is lawfully accessible from another device, computer or computer system, extend the search or access to the other device, computer or computer system.

Restoration
and forfeiture
of property

28. (1) A law enforcement officer shall, where a person from whom a computer or computer system has been seized during an investigation for a crime under this Act, is found not guilty or the proceedings against that person are withdrawn—

- (a) within thirty days of the finding of the court or the withdrawal of proceedings, restore a computer or computer system to that person; or
- (b) where the law enforcement officer is satisfied that the person cannot be found or is unwilling to receive back the computer or computer system, apply to the court for an order of forfeiture of the computer or computer system.

Act No. 19 of
2010

(2) Subject to the Forfeiture of Proceeds of Crimes Act, 2010, the court shall make an order of forfeiture under subsection (1) if—

- (a) the law enforcement officer has given notice, by publication in the *Gazette* and in a daily newspaper of general circulation in the Republic, to the effect that the computer or computer system which has been seized under this Act shall vest in the State if it is not claimed within three months from the date of publication of the notice; and
- (b) three months after the giving of the notice under paragraph (a), the computer or computer system remains unclaimed.

(3) Where a claim is made, in writing, by a person that is lawfully entitled to the computer or computer system seized under this Act, the law enforcement officer may order the release of the computer or computer system to the claimant if satisfied that there is no dispute concerning the ownership of the computer or computer system and that it is not liable to forfeiture.

Assistance

29. A person who has knowledge about the functioning of a computer or computer system or measures applied to protect the computer data that is the subject of a search under this Act may, permit and assist where reasonably required and requested by a person authorised to make the search by—

- (a) providing information that enables the undertaking of necessary measures in the circumstances;

- (b) accessing and using a computer system or computer data storage medium to search any computer data available to or in the computer system;
- (c) obtaining and copying such computer data; or
- (d) obtaining an intelligible output from a computer system in a format that is admissible for the purpose of legal proceedings.

30. (1) A law enforcement officer may, where the law enforcement officer has grounds to believe that computer data reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, by written notice given to a person in control of the computer data, require the person to ensure that the computer data specified in the notice be preserved for a period of up to seven days.

Expedited
preservation
order

(2) Where a law enforcement officer determines that computer data should be preserved for a period longer than seven days, the law enforcement officer shall apply to a judge or magistrate for a preservation order.

31. A law enforcement officer may, with a warrant, where the law enforcement officer is satisfied that computer data is reasonably required for the purposes of a criminal investigation, by written notice given to a person in control of the computer or computer system, require the person to disclose relevant traffic data about a specified communication to identify—

Disclosure
of traffic
data

- (a) an electronic communications service provider; or
- (b) a path through which a communication was transmitted.

32. (1) Where a judge is satisfied on the basis of an *ex-parte* application by a law enforcement officer, that there are reasonable grounds to suspect or believe that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the judge may order a person in control of such data to—

Collection of
traffic data

- (a) collect or record traffic data associated with a specified communication during a specified period; or
- (b) permit and assist a specified law enforcement officer to collect or record that data.

(2) The judge may, where the judge is satisfied on the basis of an *ex-parte* application by a law enforcement officer that there are reasonable grounds to suspect or believe that traffic data is reasonably required for the purposes of a criminal investigation, authorise a law enforcement officer to collect or record traffic data associated with a specified communication during a specified period.

Extradition
Cap. 94

33. An offence under the provisions of this Act is an extraditable offence or extraditable crime for the purposes of the Extradition Act.
