LEGAL PRACTITIONERS

Corpus

LEGAL ALERT

THE CYBER SECURITY AND CYBER CRIMES ACT NO. 2 OF 2021

Introduction

The Cyber Security and Cyber Crimes Bill was assented into law by the President of the Republic of Zambia, His Excellency Dr. Edgar Chagwa Lungu, on 24 March 2021 and consequently enacted into law by the Cyber Security and Cyber Crimes Act No. 2 of 2021 (the **"Cyber Act"**) on 1 April 2021 pursuant to the Cyber Security and Cyber Crimes Act (Commencement) Order, Statutory Instrument No. 21 of 2021.

The purpose of the Cyber Act is, amongst other things, to provide for cyber security in Zambia, to ensure protection of persons against cyber crime, to facilitate the identification, declaration and protection of critical information infrastructure, and to provide for the collection of and preservation of evidence of computer and network related crime.

Application of the Act

The Cyber Act applies to all persons both natural and artificial and for natural persons, it applies regardless of the person's nationality or citizenship i.e., both Zambian and non-Zambian and whether outside or within Zambia. Where an offence under the Cyber Act is committed by a person in a place outside Zambia, the person shall be dealt with as if the offence had been committed within Zambia provided that:

(i) the accused who committed the offence was in Zambia at the material time;

(ii) the computer, program or data was in Zambia at the material time; or

(iii) the damage occurred within Zambia whether or not (i) or (ii) applies.

The Zambia Information and Communications Technology Authority (**"ZICTA"**) may also, by declaration, exempt a person or class of persons, for a limited or unlimited period of time, from the requirement to abide by the provisions of the Cyber Act.

As ZICTA is yet to exempt persons or classes of persons from application of the Cyber Act, it is prudent for persons using the cyber space in Zambia or with an effect in Zambia, to be aware of provisions in the Act.

Some of the salient provisions in the Cyber Act

Cyber Inspectors

These are persons appointed by ZICTA to, amongst other things:

•monitor and inspect a computer system or activity on an information system where such activity or information is not in public domain or is not accessible to the public;
•enter and inspect the premises of a cyber security service provider if there is reasonable ground to believe that the licensee has contravened the provisions of the Cyber Act;
•audit critical information infrastructure;
•enter any premises or access an information system and:
-search the premises or that information system;
-search any person on the premises if there are reasonable grounds to believe that the person has possession of an article, document or record that has a bearing on an investigation;
-take extracts from, or make copies of any book, document or record that is on or in the premises or in the information system and that has a bearing on an investigation; and
-demand the production of, and inspect, relevant licences and registration certificates.

Cyber inspectors are therefore mandated with ensuring compliance with the Cyber Act. To note that as the Constitution of Zambia Act No.2 of 2016 provides for the right to privacy, a cyber inspector must have or be in possession of a warrant prior to exercising their powers to inspect, monitor, access, search and seize. The powers to access, search and seize can be exercised at any reasonable time and without prior notice. It is an offence for any person or entity to obstruct a cyber inspector from conducting a lawful search or seizure and if convicted, one would be liable to a fine not exceeding ZMW 60,000 (approximately USD 2,697.14 as at the date of this alert) or to imprisonment for a period not exceeding 2 years, or to both.

Powers to Investigate

ZICTA has investigative powers where it receives information regarding an alleged cyber security threat or an alleged cyber security incident to:

•require, by written notice, a person to attend at such reasonable time and place

as may be specified in the notice to answer any question or to provide a signed statement in writing concerning the alleged cyber security incident or alleged cyber security threat;
•require, by written notice, a person to produce a physical or electronic record, document or copy thereof in the possession of that person;
•require, by written notice, a person to provide the cyber inspector with information, which the cyber inspector considers to be relevant to the investigation;
•copy or take extracts from any physical or electronic record or document; or
•examine orally a person who appears to be acquainted with the facts and circumstances relating to the alleged cyber security incident or cyber security threat and to reduce the same to writing.

It is worth noting that where a person is orally examined and that person in good faith discloses information, that person is granted immunity from any duty imposed upon them not to disclose that information either under law, contract or rules of professional conduct.

It is an offence for any person to wilfully give false information or without lawful excuse to refuse to perform any act required of such person by ZICTA or indeed refuse to cooperate with or hinder a cyber inspector from conducting a lawful search or seizure. Any person that is found guilty of such offence is liable to a fine not exceeding ZMW 60,000 (approximately USD 2,697.14 as at the date of this alert) or to imprisonment for a term not exceeding 2 years, or to both.

Critical Information

The Minister of Transport and Communications (the "Minister") may by Statutory Instrument declare information which is of importance to the protection of national security, economic or social well being of the Republic, to be critical information. In addition, the Minister may equally prescribe the registration requirements for critical information infrastructure.

Unless the Minister so authorises, controllers of critical information are required to store all such information on a server or data centre located within Zambia.

Controllers of critical information infrastructure are also required on an annual basis to appoint an information technology auditor to audit the critical information infrastructure.

In addition, controllers of critical information are required to report any cyber security incident in respect of: critical information infrastructure; any computer or computer system under the controller's control that is interconnected with or communicates with the critical information infrastructure; and the critical information infrastructure that ZICTA may specify by written direction. A failure to report a cyber security incident is an offence and if convicted, one would be liable to a fine not exceeding ZMW 150,000 (approximately USD 6742.85 as at the date of this alert) or to imprisonment for a term not exceeding 5 years, or to both.

It would therefore be prudent to be on the look-out for the prescription by the Minister as persons captured to be in control of critical information will be required to adhere to the compliance obligations set out above. These obligations may require assessments of current systems to ensure compliance. In addition, there may be a cost attached to ensuring compliance.

Interception of communication

Law enforcement officers may, where the law enforcement officer has reasonable grounds to believe that an offence has been committed, is likely to be committed or is being committed and for the purpose of obtaining evidence of the commission of an offence under the Cyber Act, apply, ex-parte, to a Judge, for an interception of communications order. Such order is valid for a period of three months and may, on application by a law enforcement officer, be renewed for such period as the Judge may determine.

The court order may:

•require a service provider to intercept and retain a specified communication or communications of a specified description received or transmitted, or about to be received or transmitted by that service provider;
•authorise the law enforcement officer to enter specified premises with a warrant and to install on such premises any device for the interception and retention of a specified communication or communications of a specified description and to remove and retain such device;
•require any person to furnish the law enforcement officer with such information, facilities and assistance as the Judge considers necessary for the purpose of the installation of the interception device; or
•impose the terms and conditions for the protection of the interests of the persons specified in the order or any third parties or to facilitate any investigation.

Any information contained in a communication intercepted shall be admissible in proceedings for an offence under the Cyber Act, as evidence of the truth of its contents despite the fact that it contains hearsay. Notably, the prior written consent of the Attorney-General is required prior to making an application for an interception of communications order.

Worth noting is that an application for an interception order is made ex-parte i.e., without the attendance in court of the person whose communication will be intercepted. Further, any communication intercepted is admissible despite it containing hearsay. This deviates from the general position under Common Law that hearsay evidence is not admissible.
It is also worth noting that a law enforcement officer can be any person appointed as such by the Minister. The Act defines a law enforcement officer to mean:

•a police officer above the rank of sub-inspector;
•an officer of the Anti-Corruption Commission;
•an officer of the Drug Enforcement Commission;
•an officer of the Zambia Security Intelligence Service; and
•any other person appointed as such by the Minister for purposes of this Act.

No action lies in any court against a service provider, any officer, employee or agent of the service provider or other specified person, for providing information, facilities or assistance in accordance with the terms of a court order issued under the Cyber Act or any other law.

Communication can equally be intercepted by a law enforcement officer where the officer has reasonable ground to believe that:

•a person who is a part of any communication:
-has caused, may cause, threatens or has threatened the infliction of bodily harm to another person;
-threatens, or has threatened, to kill oneself or another person, or to perform an act which would or may endanger that party's own life or that of another person;
-has caused or may cause damage to property; or
-has caused or may cause financial loss to banks, financial institutions, account holders or beneficiaries of funds being remitted or received by such account holders or beneficiaries;
•it is not reasonable or practical to make an application for court order because the delay to intercept a specified communication would result in the actual infliction of bodily harm, the death of another person or damage to property; or
•the sole purpose of the interception is to prevent bodily harm to, or loss of life of, any person or damage to property

To note that no prior court order is required for the interception of communication to prevent bodily harm, loss of life or damage to property.

Licensing of cyber security service providers

It is an offence under the Cyber Act to provide cyber security services in the absence of a valid licence.

It is therefore now a mandatory requirement for any person providing cyber security services to be licensed with ZICTA. Any person who carries on cyber security services without being licensed commits an offence and is liable on conviction to a fine not exceeding ZMW 100, 000 (approximately USD 4,495.23 as at the date of this alert) or to imprisonment for a term not exceeding 1 year or to both.

Cyber Crime

The Cyber Act recognises several cyber crimes. A cyber crime is a crime committed in, by or with the assistance of the simulated environment or state of connection or association with electronic communications or networks including the internet.

The Cyber Act makes it an offence for a person to, with intent to compromise the safety and security of any other person, publish information or data presented in a picture, image, text, symbol, voice or any other form in a computer system. This offence is punishable by a fine of not less than ZMW 150,000 (approximately USD 6, 742.85 as at the date of this alert) or to imprisonment for a term not exceeding 5 years, or to both.

The Cyber Act also addresses issues of hate speech. A person who, using a computer system, knowingly without lawful excuse, uses hate speech commits an offence and is liable, on conviction, to a fine not exceeding ZMW 150,000 (approximately USD 6,742.85 as at the date of this alert) or to imprisonment for a period not exceeding 2 years, or to both.

Equally, a person who, using a computer system intentionally initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause emotional distress to a person commits an offence and is liable, on conviction, to a fine not exceeding ZMW 150,000 (approximately USD 6,742.85 as at the date of this alert) or to imprisonment for a period not exceeding 5 years, or to both.

It is an offence for a person to intentionally access or intercept any data without authority or permission to do so or exceed the authorised access. Also, a person who intentionally and without authority to do so, interferes with or deviates data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, commits an offence. Both are punishable, upon conviction, by a fine not exceeding ZMW 150,000 (approximately USD 6,742.85 as at the date of this alert) or to imprisonment for a term not exceeding 5 years, or to both.

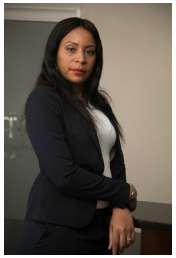
It is equally an offence for a person to knowingly, without lawful excuse, input, alter, delete, or suppress computer data, resulting in unauthentic data with the intent that it be considered or acted on as if it were authentic, regardless of whether or not the data is directly readable and intelligible. If convicted, such person would be liable to a fine not exceeding ZMW 210,000 (approximately USD 9, 439.99 as at the date of this alert) or to imprisonment for a term not exceeding 7 years, or to both. Should the foregoing offence be committed by sending out multiple electronic mail messages from or through computer systems, the penalty is ZMW 450,000 (approximately USD 20228.56 as at the date of this alert) or imprisonment for a period not exceeding 15 years, or to both.

In addition, a person who aids, abets, counsels, procures, incites, solicits another person to commit or conspire to commit, or attempts to commit any offence under the Cyber Act commits an offence and is liable, on conviction, to the penalty specified for that offence.

It must also be noted that an offence under the provisions of the Cyber Act is an extraditable offence for purposes of the Extradition Act, Chapter 94 of the Laws of Zambia.

Users of cyber space are therefore cautioned to note what constitutes a cyber crime under the Act as the penalties for a breach are quite severe if one is found liable.

We hope you found this Alert useful. Please contact our Corporate Advisory Partner and Associate, Jackie Jhala at JJhala@corpus.co.zm and Rabecca Banda at RBanda@corpus.co.zm respectively, if you have any questions or require guidance relating to the Cyber Security and Cyber Crimes Act.



Jackie Cornhill Jhala
Partner
Corporate Advisory Department
Corpus Legal Practitioners
Email: JJhala@corpus.co.zm
Tel: +2602 11 372300 / 01 / 04

Rabecca Banda
Associate
Corporate Advisory Department
Corpus Legal Practitioners
Email: RBanda@corpus.co.zm
Tel: +2602 11 372300 / 01 / 04