BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

JUN 2025

DEPARTMENT OF MARKETING

PROGRAMME: Master of Marketing Degree

Legal, Ethical and Social issues in Digital Marketing **MMkt 509**

DURATION: 3 HOURS 15 MINUTES

INSTRUCTIONS

1. Answer **QUESTION ONE AND ANY THREE QUESTIONS**.
2. Start answering each main question on a fresh page.
3. Credit will be given for appropriate use of case studies and examples.
4. No cell phones and programmable calculators are allowed in the examination room.

QUESTION 1 (Compulsory)

Read the passage below and then answer the questions that follow

6 DEC, 2021

An analysis of the recently gazetted Data Protection Act of Zimbabwe.

On 3 December 2021, Zimbabwe enacted the Data Protection Act which also has aspects relating to cybersecurity and cybercrimes.

The object of this Act is *"to increase data protection in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects".*

This law is also amending provisions of the following three pieces of legislation:

- Criminal Law (Codification and Reform Act)
- The Criminal Procedure and Evidence Act
- The Interception of Communications Act

The Bill was gazetted in May 2020 and underwent public hearings in July 2020 when it was known then as the Cybersecurity and Data Protection Bill. The following were some of the recommendations by the relevant Joint Parliamentary Portfolio Committees Report following the public hearings:

- Objectives of the Bill should clearly describe its provisions.
- The Bill should be amended to improve on the definitions of terms as they should be clearly defined.
- The need to split the Bill into two, to separately cater for Cyber Security and Data Protection.
- Establish an independent body which is set up as the Cyber Security Centre and Data Protection Authority instead of having POTRAZ (Postal and Telecommunications Regulatory Authority of Zimbabwe) serve as the Cyber Security Centre and Data Protection Authority.
- Bill should be amended, to have a clause that guarantees the protection of whistle-blowers in terms of handling investigations.
- The Bill should be amended and have a clause that provides for the right to oblivion, that is the right to delete information and records of the past in cyberspace, and clearly spell out the data retention period.
- That the Bill should be amended to include a standalone clause that recognises the rights of data subjects.
- Be amended to include the time under which a security breach should be notified.
- The Bill should strike a balance between the protection of national security and the exercise of rights of ordinary individuals.
- The Bill should be amended to include the terminology that criminalises upskirting and recording of intimate images without a person's consent.

- That the provision on child pornography should be renamed to child sexual abuse materials and should also provide for offences such as cyber grooming.

Post the public hearings, this law underwent several changes and amendments during the Parliamentary processes. Below is MISA Zimbabwe's analysis of the Act;

To begin with, the Act clearly defines what consent is, which is defined as *any manifestation of specific unequivocal, freely given, informed expression of will by which the data subject or his or her legal, judicial or legally appointed representative accepts that his or her data be processed.* The specification of unequivocal, freely given and informed is quite critical in establishing consent.

Personal information is also defined in the law, similar to definitions in other jurisdictions, for example, the South African Protection of Personal Information Act which includes name, address, telephone number, an identifying number and biometric information, among others.

This definition also qualifies opinions expressed about an identifiable person as personal information and also the individual's personal views or opinions, except if they are about someone else as personal information. This appears to be contradictory as opinions about someone else can be qualified under opinions about an identifiable person.

The definition of sensitive data is very comprehensive and seems to have been informed by the EU's General Data Protection Regulation, which definition includes health information, religious beliefs and political opinions.

Sensitive data requires a higher degree of protection as its processing can create significant risks to the fundamental rights and freedoms of the data subject. In enforcing the Zimbabwean Data Protection Act, it is hoped that this data will receive the levels of protection that it should.

The Act is also establishing the Postal and Telecommunications Regulatory Authority (POTRAZ) as the Data Protection Authority. From stakeholder submissions and public hearings, the appointment of POTRAZ was criticised on the basis that it would create a super administrative authority as POTRAZ is also the telecommunications sector regulator.

The functions of the Data Protection Authority include establishing conditions for the lawful processing of data, issuing its opinion either of its own accord or at the request of any person with legitimate interest on any matter relating to the application of fundamental principles of the protection of privacy.

While it is important that the Authority should shed light on any contentious or vague issues relating to data protection and privacy, it is hoped that this function will not be abused by some stakeholders qualifying as 'any person with legitimate interest'.

One critical function which will go a long way in promoting data protection and privacy, particularly under the banner of consumer rights and or consumer protection and their data, is the role of the Authority to receive, by post or electronic means or any other equivalent means, the complaints lodged against data processing and give feed-back to the claimants or complainants.

Another body that is established through this law, is the Cybersecurity and Monitoring of Interception of Communications Centre. This Centre is being established through the repeal of provisions in the Interception of Communications Act and the refurbishment of what used to be the Monitoring Centre by only vesting it with functions on Cybersecurity.

What is clearly noted from these provisions, is that the government is operating under a very misled presumption that cybersecurity equals national security. Cybersecurity issues concern

every person who is an internet user, more so now when the entire globe is living in a digital age.

This Centre shall be housed in the Office of the President. It is provisions such as these that continue to infringe on fundamental rights. Not only is it not advisable for a Cybersecurity centre to be housed in the Office of the President, but the same body is also now responsible for the issuing of interception of communications warrants.

This presents a legal basis for the government, and more so, the Executive to be monitoring and intercepting communications of targeted persons, who, believed reasonably or not' to be enemies of the State, especially political opponents.

In saying this, MISA Zimbabwe is mindful of the approach that was taken following the *#ZimbabweanLivesMatter* campaign wherein proponents of that campaign were viewed as enemies of the State when these were merely ordinary citizens demanding the respect of human rights in Zimbabwe.

Be that as it may, the functions of the Centre will also include the following:

- be the sole facility through which authorised interceptions shall be effected
- advise Government and implement Government policy on cybercrime and cyber security
- identify areas for intervention to prevent cybercrime
- establish and operate a protection-assured whistle-blower system that will enable members of the public to confidentially report to the Cybersecurity Committee cases of alleged cybercrime
- promote and coordinate activities focused on improving cyber security and preventing cybercrime by all interested parties in the public and private sectors

A Cybersecurity Committee will also be in place and shall comprise the following 11 members appointed by the Minister of ICTs, with representatives from the following:

- the Postal and Telecommunications Regulatory Authority of Zimbabwe
- the ministry responsible for information and communications technologies
- the ministry responsible for science and technology
- the ministry responsible for justice
- the Zimbabwe Republic Police
- the National Prosecution Authority
- the ministry responsible for defence
- the Central Intelligence Organisation
- the Prisons and Correctional Services
- one representative from the Cyber Security and Monitoring Centre
- any representative from any sector of the economy or any other person who may be necessary to the deliberations in respect of a particular warrant.

All these people shall be appointed on an ad hoc basis.

As part of the data protection and privacy safeguards, data controllers have a duty to ensure that the data processed is adequate, relevant and not excessive in relation to the purposes to which it was collected for.

Similarly, data retention should also not be longer than necessary for the intended purpose. Data controllers will also ensure that they facilitate the right to access by data subjects by ensuring that processed data is in an accessible format.

It is also progressive that the law is explicitly highlighting the rights of data subjects in Section 14 which include the right to access, right to be informed, right to object and the right to deletion, among others.

Further, the law also requires data processors to put in place necessary security mechanisms for the protection of data. In the event of a security breach, data processors are required to notify the Data Protection Authority within 24 hours.

While it is progressive that a time frame was put on this aspect, 48 hours' notice period would have been more reasonable, as processors need to be given ample time to also investigate the nature and impact of a security breach. However, the provision is still lacking on the aspect of notification to data subjects, that aspect should have been provided for.

With regards to cross-border transfers of personal information, the law obligates data controllers to ensure that adequate levels of protection are available in the recipient country or recipient international organisation.

However, as with several aspects in the Act, a gap has been left to be filled by the Data Protection Authority with regards to categories or circumstances under which the transfer of data to countries outside Zimbabwe will be unauthorised.

Yet again, the law also gives discretion to the Cybersecurity and Monitoring Centre to give directions on how to implement the law relating to transfers of personal information outside Zimbabwe.

Section 31 of this Act speaks to the issue of whistleblowers and unfortunately does not provide for the necessary safeguards for the whistleblowers themselves as per the requirements from the public hearings for a specific piece of legislation on whistleblower protection.

The Act requires the Data Protection Authority to put in place regulations that shall govern the whistleblowing system, guided by principles that include fairness and lawfulness.

With regards to the Amendments to the Criminal Law (Codification and Reform) Act, several provisions have been catered for that relate to cybercrimes like hacking, unlawful interference and unlawful acquisition of data, among others.

For purposes of the exercise of fundamental rights such as freedom of expression, there are numerous provisions that are also of interest. One of the provisions is that which criminalises what is termed as the transmission of data message that incites violence or damage to property. Incitement laws have been there in the statute books for a while now. Several individuals particularly activists and opposition leaders have been charged for allegedly contravening such provisions. However, what amounts to incitement in Zimbabwe is very vague.

Critical examples of the enforcement of this provision include the arrest of Evan Mawarire, who used his Facebook account to air his concerns regarding the high cost of living and of basic commodities in Zimbabwe.

Similarly, prominent journalist Hopewell Chin'ono was also arrested on the same charge. In short, this provision potentially criminalises digital activism in Zimbabwe. Ordinary citizens in Zimbabwe cannot campaign, or demonstrate and petition online, in line with their constitutional rights, without running the risk of being charged with inciting violence.

Another problematic provision is the one relating to the transmission of false data messages.

MISA Zimbabwe reiterates its long-standing position that false news offences promote self-censorship and unjustifiably infringe on freedom of expression. This position is also supported by an existing constitutional court order which struck off criminal defamation.

This provision is highlighting that any person who unlawfully and intentionally, by means of a computer or information system, makes available, broadcasts or distributes data to any other person concerning an identified or identifiable person knowing it to be false with intent to cause psychological or economic harm, shall be guilty of an offence and liable to a fine not exceeding level 10 or to imprisonment for a period not exceeding five years.

These penalties are too stiff with very high chances that this provision will also smuggle back criminal defamation which was declared unconstitutional.

The other provision is on cyber-bullying and harassment. Such provisions are progressive as far as women's rights online are concerned.

Several women, particularly female journalists and female politicians in Zimbabwe, have been victims of cyber-bullying and harassment which has greatly affected the exercise of digital rights by women.

Further, such bullying and harassment have also been perpetrated by individuals defending their political parties as has been seen in the online wars between *Varakashi* and the *Nerrorists.* If implemented properly, this provision might be critical in ensuring that individuals respect the rights of others to also freely express themselves and access information online.

Victims will also benefit greatly from the provision on the transmission of intimate images without consent as cases of revenge pornography have been on the rise, not only in Zimbabwe but also in other jurisdictions.

Other progressive provisions relate to child-related materials, hence the criminalisation of child sexual abuse material and exposing children to pornography, among others.

On the amendments to the Criminal Law and Evidence Procedure Act, one key aspect is the admissibility of electronic evidence. This had to be catered for as we are living in the digital age, and likewise, the court system needs to be updated in consideration of such developments.

There is a need to ensure that mechanisms are in place to verify the authenticity of electronic evidence.

In terms of the Act, regard shall be given to several factors including the reliability of the manner in which the evidence was generated, stored or collected and also the manner in which the originator or recipient of the evidence was identified.

Conclusion

MISA Zimbabwe welcomes the enactment of the Data Protection Act, which was long overdue, but remains concerned by the inclusion of cyber security regulatory framework in the Act.

The demands of the digital age, include a comprehensive data protection framework with safeguards on the collection, processing, transmission and storage of data as guided by data protection and privacy principles.

Be that as it may, this law is still an omnibus law, which is addressing several thematic aspects including cybersecurity and cybercrime, as noted above, through the manner in which the law was amending three other pieces of legislation.

MISA Zimbabwe also recognises the progressive provisions relating to specifications on the rights of data subjects, notification of security breach and all the other responsibilities that have been placed on data controllers for purposes of promoting data protection and privacy.

However, the other provisions in this Act have also created a give and take situation as discretion has also been given to the Cybersecurity and Monitoring of Interception Communications Centre to make decisions and influence processes relating to data protection.
This includes their role on conditions relating to the processing of sensitive data and the transfer of personal information outside Zimbabwe.
MISA Zimbabwe remains concerned with the claw-back approach on regulations governing media, privacy, expression, and access to information in Zimbabwe. It's a typical case of moving one step forward and three backwards.
The unjustified limitations also include exemptions based on national security, state interests and public interests, which aspects have always been vague, more so if they are implemented through a Centre that is housed in the President's office.
The law is also silent on when exactly it will take effect. The principles of natural justice demand that ample time be given for purposes of application or enforcement of a law of this nature, which not only requires regulations and directives from the Data Protection Authority, but also the setting up of necessary structures and safeguards.
MISA Zimbabwe also calls for the repeal or amendment of some of the provisions particularly the one relating to incitement of violence and the transmission of false data messages.
If the government had taken on board recommendations by the relevant Joint Parliamentary Portfolio Committees Report following the public hearings referred to earlier, and specifically on the need to unbundle the laws, we would as a country have made a bold move forward in respect of the right to privacy.
Suffice to say in its current state, the Act seeks to take away the rights provided through the first three-quarters of the law through its last sections that provide for the regulation of cyberspace.

About MISA
The Media Institute of Southern Africa (MISA) was founded in 1992. Its work focuses on promoting, and advocating for, the unhindered enjoyment of freedom of expression, access to information and a free, independent, diverse and pluralistic media.

Questions
In light of the above passage, evaluate the role of the Data Protection Act of Zimbabwe with respect to the following
a. Protection of state security (15)

b. Protection of personal security and freedoms (15)

c. Role of POTRAZ (10)

[40 Marks]

QUESTION 2

Write notes on the following

Revenge porn (10)
Defamation (10)

[20 Marks]

QUESTION 3

Discuss the contrasting views on the role of social media with respect to the promotion of issues of public interest on one hand and protection of privacy on the other. Cite relevant cases to support your viewpoints

[20 Marks]

QUESTION 4

Discuss the measures that have been put in place by a government of your choice to address cyber bullying and hate speech

[20 Marks]

QUESTION 5

Discuss the assertion that ethical conduct does not exist in social media. Cite relevant examples to support your views.

[20 Marks]

QUESTION 6

Critique the role of tech media giants in the development/promotion of social media. Cite relevant examples to support your answer.

[20 Marks]

END OF PAPER