CONSTITUTION WATCH 2/2019

[19th January 2019]

Internet Shutdown

In this bulletin we shall examine the legality of the Internet shut-downs against the background of the Constitution, international law and the Interception of Communications Act.

On the 15th January, the second day of a stay-away called by the Zimbabwe Congress of Trade Unions, all Internet services across the country were switched off under government instructions. Econet, the country's largest mobile telecommunications operator and Internet service provider *[ISP]*, issued the following statement to its subscribers:

> *"Further to a warrant issued by the Minister of State in the President's Office for National Security through the Director-General of the President's Department acting in terms of the Interception of Communications Act, internet services are currently suspended across all networks and internet service providers. We are obliged to act when directed to do so and the matter is beyond our control."*

Other ISPs issued similar messages.

Service was restored, then shut down for another day, and now has been restored again, though most social media sites remained blocked.

The Constitutional Guarantee of Freedom of Expression

Section 61 of the Constitution guarantees the right to freedom of expression which, it says, includes:

> *"freedom to seek, receive and communicate ideas and other information".*

It is one of the most precious of all human rights because, together with freedom of association, it forms the bedrock of democracy.

Freedom of expression is not absolute, however. Section 61 of the Constitution itself says it does not extend to incitement to violence or to hate speech. And section 86 goes on to say that a law may limit it and other freedoms so long as the limitation is "fair, reasonable, necessary and justifiable in a democratic society based on openness, justice, human dignity, equality and freedom." In deciding whether a limitation meets this test, one must consider, among other things, whether the limitation imposes greater restrictions on the freedom than are necessary, and whether the limitation's objective may be achieved by less restrictive means [section 86(2) of the Constitution].

International Law

The Constitution must be interpreted in the light of international law. Freedom of expression is recognised internationally as a fundamental human right, protected by both the International Covenant on Civil and Political Rights (article 19) and the Universal Declaration of Human Rights (article 19).

The African Commission on Human and Peoples' Rights, in art 1.1 of its Banjul Declaration (2002), goes so far as to declare:

> *"Freedom of expression and information including the right to seek, receive and impart information and ideas, either orally, in writing or … through any other form of communication … is a fundamental and inalienable human right and an indispensable component of democracy."*

The African Charter on Broadcasting, agreed at Windhoek in 2001, says in Article 1 of Part IV:

> *"The right to communicate includes access to telephones, email, Internet and other telecommunications systems, including through the promotion of community controlled information communication technology centres."*

In 2018 the United Nations Human Rights Council passed a resolution:

- affirming that the same rights people have offline must also be protected online, in particular freedom of expression, and
- condemning unequivocally measures in violation of international human rights law that prevent or disrupt an individual's ability to seek, receive or impart information online, and calling upon all States to refrain from and cease such measures.

In other words, the Council condemned intentional disruption of Internet access by governments.

The Interception of Communications Act

Against this background the Government would have to show very clear statutory authority before it could credibly claim that the shut-down of the Internet was lawful. The Government relied on the Interception of Communications Act, but it does not provide that authority.

The long title of the Act explains its objectives in the following words:

> *"An Act to provide for the **lawful interception** and **monitoring** of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Zimbabwe; to provide for the establishment of a monitoring centre; and to provide for any other matters connected with or incidental to the foregoing."*

The objectives of the Act are therefore twofold:

1. To permit the interception and monitoring of communications
2. To establish a monitoring centre.

Shutting down whole communication systems is not stated to be an objective of the Act and cannot be regarded as connected with or incidental to the Act's two stated objectives. After all, how can one intercept or monitor communications if one has shut down the whole communication system?

What the Act does is to allow a Minister – and we shall deal later with who that Minister is – to issue warrants authorising the interception of communications and, instead of warrants, to issue directives. The scope of these warrants and directives are as follows:

Interception Warrants

The Econet statement [see above] refered to a "warrant". Section 5 of the Act allows officials responsible for state security and crime investigation to apply for

warrants authorising the "interception" of communications, and section 6(1) goes on to empower a Minister – we shall explain below who that might be – to issue a warrant in response to such an application. Sections 5, 6 and 7 of the Act make it clear that a warrant can only authorise the interception of communications, and "intercept" is defined in section 2 of the Act as meaning listening to, recording or copying electronic communications, or reading or copying communications sent by post.

Interception does not therefore extend to stopping communications from being sent, or shutting down communication systems. Warrants, in other words, permit the Government to snoop but not to stop.

Directives

Section 6(2) of the Act states that where the Minister receives an application for a warrant, he may instead issue "any directive … not involving any interception or monitoring of communications".

Notices issued by some ISPs referred to "directives" ordering them to shut down services, which suggests that the Government relied on section 6(2) to close down the Internet. If the Government did so, it was wrong. The section cannot be construed as impliedly giving the Minister such a drastic power, a power far exceeding those the Act expressly gives him under a warrant – a power moreover which is not even hinted at in the long title of the Act.

What section 6(2) obviously means is that if the Minister is asked for a warrant authorising the authorities to intercept – i.e. read, listen to, record or copy – someone's communications, the Minister can instead issue a directive authorising a different, less intrusive, type of eavesdropping: for example, a directive ordering an ISP to disclose who the person has been communicating with, how often, and when.

The Act certainly does not empower the Government to shut down the Internet or any part of it, and there is no other law that allows it to do so.

Who is the Minister responsible for the Interception of Communications Act?

The warrants and directives were apparently issued by the Minister of State for National Security in the President's Office, but he was not the right person to issue them.

The Act was originally assigned to the Minister of Transport and Communications, but the President has power under section 104(1) of the Constitution to assign it to some other Minister or even to reserve its administration to himself. In SI 212 of 2018 the President chose to reserve the administration of the Act to himself. Hence the word "Minister" must be read as "President" wherever it appears in the Act.

Whatever else the Minister of State Security may be, he is not the President – or wasn't at the time of writing, at least – and does not have authority to issue warrants and directives under the Act.

Conclusion

The inevitable conclusion is that the Government acted unlawfully in shutting down the Internet. In doing so it has wrought incalculable damage to the country. One

estimate is that the shutdown cost over $5,5 million in direct costs, and to that must be added all the indirect costs such as transactional delays and lost opportunities, to say nothing of the damage to the country's reputation as a place that is "open for business".

It has to be recognised – indeed the Constitution itself recognises – that freedom of expression can be abused through hate speech and incitement to violence. The Internet and social media were misused in this way both before and during the recent disturbances. The Government is entitled to curb such misuse, if it can, but it must do so lawfully. By issuing illegal and arbitrary warrants and directives the Government has laid itself and ISPs open to legal challenges and, possibly, liability for heavy damages.

Veritas makes every effort to ensure reliable information, but cannot take legal responsibility for information supplied
To subscribe or unsubscribe from this mailing list please email ***billwatch@mango.zw***
If you wish to contact Veritas please email ***veritas@mango.zw***
If you are requesting legislation please email ***veritas@mango.zw*** *or look for it on* ***www.veritaszim.net***

follow us on (+263 71 893 3633)