IPPR

• BY FREDERICO LINKS

FEBRUARY 2022

Familiar Flaws – Unpacking Namibia's draft Cybercrime Bill

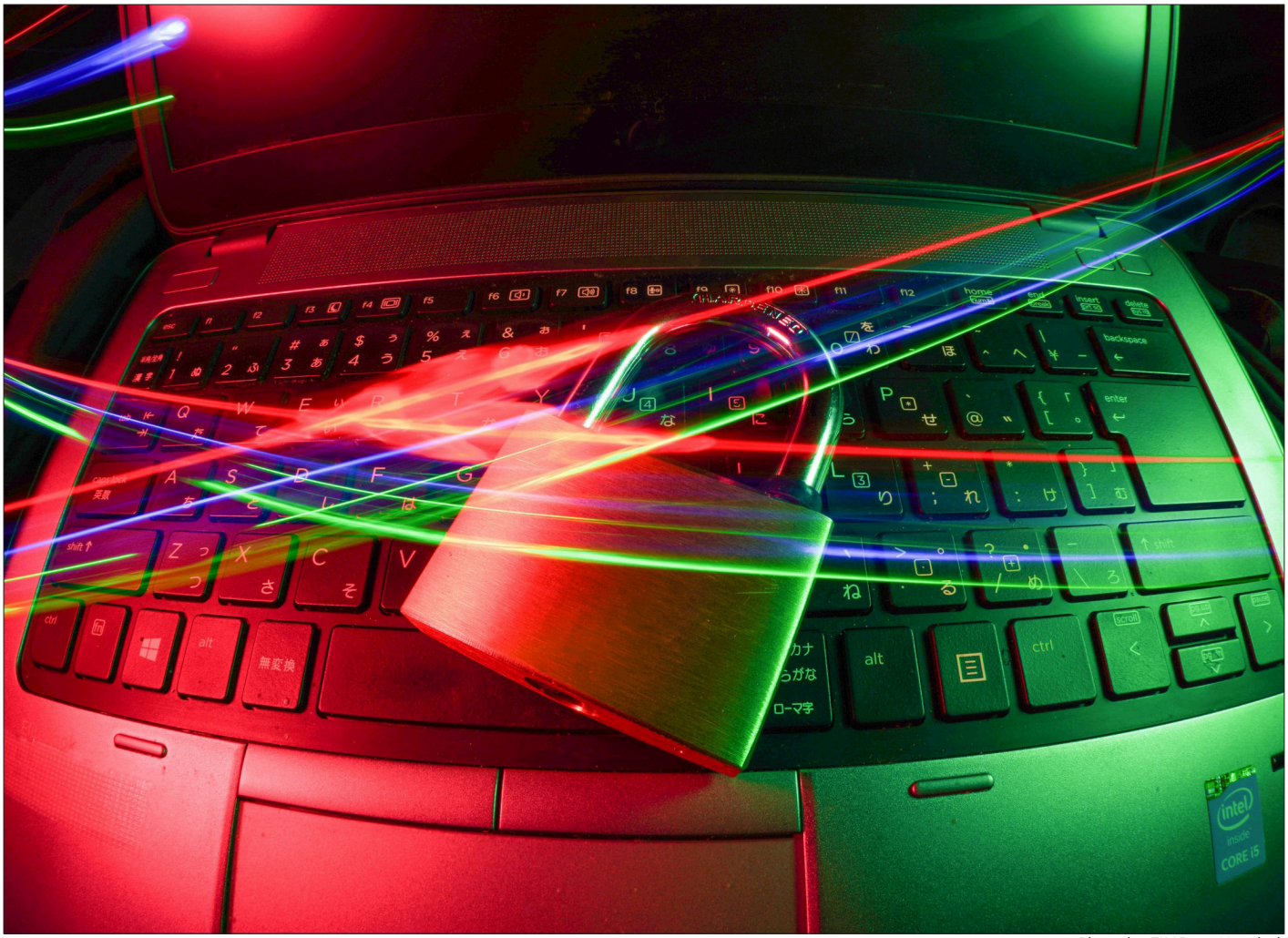

Photo by FLY:D on Unsplash

1. Introduction – A historical challenge

Namibia has been in the process of drafting cybercrime legislation for roughly 15 years, with various drafts of a cybercrime law having surfaced in public since 2013, and one even making it as far as being briefly tabled in the Namibian parliament in early 2017 before being withdrawn.

Namibia's initial effort at cybercrime legislation came as a result of the International Telecommunications Union's (ITU) Harmonisation of the Telecommunication and ICT Policies in Africa (HIPSSA) project, from which emerged the Computer Crime and Cybercrime SADC Model Law in 2013. That was also the year during which the first draft of Namibia's Electronic Transactions and Cybercrime Bill appeared in public.

This briefing paper is an output of the 'Mainstreaming Human Rights in Cybercrime Law and Policy Making (MHRC)' project, which is funded by Global Partners Digital (GPD).

GLOBAL PARTNERS DIGITAL

The Electronic Transactions and Cybercrime Bill floated around for a while as the process to finalise the Bill appeared to have stalled between 2013 and 2016. In 2017 the Bill, a substantially flawed draft, suddenly and surprisingly was tabled in the National Assembly (NA) by then Minister of Information and Communication Technology (MICT), Tjekero Tweya, before being hastily withdrawn again with the Namibian Prime Minister Saara Kuugongelwa-Amadhila indicating at the time that the Bill needed more work. Why Minister Tweya had tabled the Bill without warning at the time, when it was clear it needed more work, has never been adequately clarified. The tabling of the Bill at the time was accompanied by civil society criticism of the draft, which arguably contributed to the Bill being withdrawn shortly after it was tabled in February 2017.

The withdrawal of the Bill was followed by a period of engagement and consultation between MICT, the justice ministry, civil society and telecommunications service providers and information and communication technology (ICT) sector stakeholders. The consultations included a call for submissions to the Bill's text in mid-2017, followed by two workshops organised by the MICT, and a round-table discussion hosted by the Access to Information in Namibia (ACTION) Coalition in August 2017 for MICT officials, and other government and private sector stakeholders.

It was after this process, and the publication of a critique of the draft Bill and the consultation process by the IPPR[1], that in 2018 MICT announced that the Bill would be split into two – a separate Electronic Transactions Bill and a Cybercrime Bill would be drafted and enacted.

However, while the Electronic Transactions Act (No.4 of 2019) was enacted in November 2019, a cybercrime law has yet to be tabled in the Namibian parliament by the time of the publication of this briefing paper in February 2022.

> "A surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protesters in many countries around the world. While the role that technology can play in promoting terrorism, inciting violence and manipulating elections is a genuine and serious global concern, such threats are often used as a pretext to push back against the new digital civil society."
>
> *– UN Special Rapporteur on the rights to freedom of peaceful assembly and of association (17 May 2019)*

2. Where we are now

In early 2020 the MICT had indicated to this author that a Cybercrime Bill would be tabled in the Namibian parliament during that year. The same was said again in 2021 when a similar question was asked as to the status of such a Bill.

This is because since 2019 a draft Bill – officially the Computer Security and Cybercrime Bill (2019) – has been floating around. When questioned again about the status of this Bill in February 2022 for this paper, the Executive Director in the MICT, Mbueta Ua-Ndjarakana, issued the following brief response:

"The Cybercrime Bill was scrutinised at the Cabinet Committee on Legislation (CCL) during 2021 as directed by Cabinet. CCL discussed the Bill and referred it back to this Ministry and Advocate Bekker, a government legal drafter who has drafted this Bill from scratch. A working session was held between the parties and Advocate Bekker was to incorporate the changes before the Bill could be taken back to CCL. Sadly, Advocate Bekker demised (sic) during June 2021 and his death left a notable knowledge gap in the finalisation of this Bill. The Ministry of Justice has since assigned two legal drafters

[1] For a historical overview and critique of the then Electronic Transactions and Cybercrime Bill see the IPPR's 'Tackling Cyber security/Crime in Namibia: Calling for a Human Rights Respecting Framework' at the following URL: https://ippr.org.na/publication/tackling-cybersecurity-crime-namibia/

who will soon assume responsibility of drafting of the Bill which will then be submitted back to CCL which will then direct on the next course of action."

It should be noted though that the 2019 draft of the Cybercrime Bill emerged around the time that a joint Commonwealth Secretariat and Council of Europe (CoE), in conjunction with the World Bank and the UK's Foreign Commonwealth Office, assessment was underway or had been completed on the state of Namibia's cybersecurity legislative and regulatory landscape. This assessment informed the drafting of the country's National Cybersecurity Strategy and Awareness Raising Plan 2022 – 2027.

Significantly, what appeared to be the final draft of the National Cybersecurity Strategy – that was circulated to stakeholders in late 2021 for validation purposes – recognises that "cybercrime has the potential to negatively impact the nation's ability to achieve its development objectives" and identified, first, among a range of "gaps and vulnerabilities" that:

"The current cybercrime Bill is not aligned to the Budapest Convention which is internationally recognized as the leading treaty on cybercrime legislation. The Government of Namibia has indicated their desire to accede to the Convention."

Consequently, among the first steps to be taken under the implementation of the National Cybersecurity Strategy, from 2022 onwards, would be to:

"Conduct a detailed analysis of the cybercrime bill using the Budapest Convention as the target legislation and identify areas that require modification."

The prioritising of the completion of the drafting and enactment of a Cybercrime Bill is further underscored in Pillar 3 (Enabling Legal Framework and Enforcement) of the envisaged National Cybersecurity Strategy Framework, which states:

"The objective for this pillar is to prioritise & fast-tracking the adoption of modern and robust cybercrime legislation, in line with international standards, which could effectively tackle the challenges currently faced in cyberspace. Suitable legal provisions are needed to facilitate the cross-country investigation, prosecution and adjudication of cyber and cyber-related crimes."

The purpose of mentioning all this here is to illustrate that by its own statements, and the invoking of the Budapest Convention[2], the Namibian state clearly seeks to align its cybercrime legislative and regulatory initiatives to international best practice.

It is against this backdrop that this paper seeks to serve two goals simultaneously, specifically:

- To bolster the Namibian state's stated positive intent in ensuring that the eventual cybercrime legislative and regulatory framework is in line with international best practice;
- And to inform and enable Namibian civil society efforts at ensuring that the eventual cybercrime legislative and regulatory framework and environment are human rights respecting in substance.

These goals are served by critiquing and analysing provisions of the 2019 iteration of the Cybercrime Bill, notably the parts that impact on freedom of expression, freedom of association, freedom of assembly and the right to privacy, all of which are fundamental human rights enshrined in the Namibian Constitution. This is done to encourage the legal drafters, and policy-makers, to pay special attention to these and associated rights when crafting the final text of the eventual substantive Cybercrime Bill.

[2] The Budapest Convention text can be accessed at the following URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Concerning aspects carried over from the Electronic Transactions and Cybercrime Bill (2017)

The 2019 draft Cybercrime Bill contains some of the issues spotlighted as problematic in the scrapped Electronic Transactions and Cybercrime Bill of 2017.

The aspects are:

- Problems with / absence of key definitions;
- Under-provisioning around unauthorised access, secret warrants and warrantless search & seizure;
- Lack of transparency by relevant officials and entities;
- Lack of adequate oversight of relevant officials and entities;
- Lack of data and privacy protections;
- Excessive and unaccountable discretionary ministerial power.

3. Areas where the Cybercrime Bill (2019) is flawed and could be strengthened in terms of upholding free expression, association, assembly and privacy

In mid-2021, the IPPR contracted the Legal Assistance Centre (LAC) to conduct a constitutional and legal review of the text and provisions of the draft Cybercrime Bill (2019). What follows is derived from the report submitted to the IPPR by the LAC in June 2021[3].

- Access to information should not be the province of cybercrime legislation. Access to information is a vital issue which should be covered by a dedicated law on this topic, alongside a general law on data protection. In any event, it is unwise to allow rules about access to information from critical or important databases to be set by the minister responsible for information technology by means of regulations.

- With regards to child pornography, we recommend that the offence of child pornography should be addressed in a comprehensive law on this topic which includes but is not limited to child pornography transmitted via information systems.

- We recommend that online and offline harassment should be addressed together in one law, to avoid the anomaly in several other African countries which provide protection against online harassment but no protection whatsoever if the same conduct occurs in any other context.

- With regards to non-consensual dissemination of sexual images (revenge porn) and voyeurism, the current draft fails to define important terms such as "nudity" (what body parts must be shown to constitute nudity?) and "pictorial" and "photographic" (do these clearly include video material?). It also uses inconsistent terminology ("information", "pictorial" and "photographic") which may cause confusion. Some related issues are excluded, such as some forms of voyeurism, and threatening to distribute intimate images of a person ("sextortion"). Because voyeurism can take both online and offline forms, it would be better addressed in the proposed Bill on harassment instead of a cybercrime alone.

- With reference to child pornography and grooming, it is necessary to clarify whether solicitation must be followed by material acts aimed at leading to a meeting (as in Article 23 of the Lanzarote Convention[4]). The definition of a child should be broadened as in the case of

[3] The full report by the Legal Assistance Centre (LAC) can be viewed at the following URL: https://drive.google.com/file/d/1Yt6c5fjL09KdKVz4pKkAf3p9meemF8Px/view?usp=sharing

[4] The text of the Lanzarote Convention can be accessed at the following URL: https://www.coe.int/en/web/children/convention#{%2212441481%22:[2]}

child pornography, to include a person who, the offender believes to be under the age of 16, in order to facilitate prosecution of the crime. Grooming of persons with severe mental disabilities should be included, as such persons are often targeted for sexual exploitation.

- It would make sense to broaden section 17(c) beyond Namibian citizens to include persons ordinarily resident in Namibia. (Compare the South Africa Cybercrimes Bill [B6B-2017], section 24(2)). This section could also cover situations where the program, computer, data, or information system used in the commission of the offence or against which the offence was directed is in Namibia (Compare Uganda's Computer Misuse Act 2011, s. 30 (3); Zimbabwe's draft Cybercrime and Cybersecurity Bill, 2017, s. 38(1)(e) and Tanzania's Cybercrime Act 2015, s. 30.)

- With regards to production orders, the law should provide for the possibility where a court might need to issue a production order on its own, without application by a member of the police. For example, the need to examine some information from a computer system might arise during a court proceeding as well as during a criminal investigation.

- Consider broadening the group of persons who can be asked to produce data to include persons who have access to the data itself, but not to the computer system on which the data is stored – such as service providers who may record subscriber information in some manner which is not on the computer system referred to.

- With regards to preservation orders we suggest that the requirement of "grounds to believe that data may be lost" should be qualified by reasonableness: "reasonable grounds to believe that data may be lost". (Compare Botswana's Cybercrime and Computer Related Crimes Act 2018, s. 24 and Uganda's Computer Misuse Act 2011, s. 9 – both of which also require court approval of a preservation order.)

- With regards to interception and use of forensic tools, any authority for interception should respect the International Principles on the Application of Human Rights to Communications Surveillance ("International Principles")[5], the right to privacy (Namibian Constitution, Article 13 and ICCPR, Articles 13 and 17) and the right to an effective remedy in case of human rights violations (ICCPR, Article 2(3)(a)). There is an insufficient guarantee of proportionality between the benefits and harms following interception. Subsections 21(8) and (9) of the draft Bill allow for broad warrants, while the International Principles provide more proportionality by including principles that limit interception in the following way: (a) the information accessed must be confined to that reasonably relevant to the crime alleged; (b) any excess information collected must be promptly destroyed or returned; and (c) information may be accessed only by the specified authority and used only for the purpose for which authorisation was given.

- Subsection 21(2) has no user notice requirement, while the International Principles require that individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision, and that they should have access to the materials presented in support of the application for authorisation. Similar requirements follow from the right to a fair and public hearing within a reasonable time (as in the ICCPR, Article 14). Only in exceptional circumstances can this notification be delayed:

    1. where notification would seriously jeopardise the purpose for which the surveillance is authorised, or there is an imminent risk of danger to human life;
    2. where authorisation to delay notification is granted by the competent judicial authority at the time that authorisation for surveillance is granted; or
    3. where the individual affected is notified as soon as the risk is lifted or within a reasonably practicable time period, whichever is sooner, and in any event by the time the communications surveillance has been completed.[6]

[5] These principles were drafted by experts in privacy and security, with global consultation and the participation of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. The principles have been adopted globally by more than 400 organisations.rately publishing information about the use and scope of communications surveillance techniques and powers; and to publish periodic reports and other information relevant to communications surveillance."

[6] In terms of the International Principles, the obligation to give notice rests with the State, but in the event the State fails to give notice, communications service providers are free to notify individuals of the communications surveillance, voluntarily or upon request. It should be noted that the mere risk of flight or destruction of evidence is insufficient to justify a lack of notification.

- There is a lack of public oversight in this area. The International Principles specify which powers should be granted to such oversight mechanisms.[7]

- There is a lack of transparency. According to the International Principles the requirement of transparency includes, at a minimum, an obligation to publish aggregate information on the number of requests approved and rejected, and a disaggregation of the requests by service providers and by investigation type and purpose.

- The draft Bill lacks remedies in the case of illegal interception, which violates the right to an effective remedy for human rights violations in ICCPR, Article 2(3)(a). The International Principles provide the following options for remedies:

    1. States should enact legislation criminalising illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistleblowers, and avenues for redress by affected individuals;
    2. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence in any proceeding, as is any evidence derivative of such information.

- The relationship between this provision of the draft bill and Part 6 of the Communications Act 8 of 2009 on interception of telecommunications needs clarification.

- The law should ensure that the right to privacy is also protected when transmitting information to a foreign authority. For example, it might require that the police make sure that the foreign authorities' criminal justice system adequately protects human rights. Grounds for refusal to engage in information-sharing with foreign authorities in the UN Model Treaty on Mutual Assistance in Criminal Matters (Article 4) include these:

    1. Criminal sanctions do not fully address the harm caused by cybercrimes or harassment;
    2. there is a need to provide for a fair procedure for removal of the content which gave rise to the crime, or the disabling of access to it, and a mechanism for prohibiting the person convicted from publishing similar content;
    3. Rapid response can be crucial to protect privacy and dignity, but there must also be safeguards to protect freedom of speech and expression;
    4. The draft Bill under preparation by the LAC would propose a quick and accessible procedure for a "harassment prevention order", modelled on domestic violence protection orders, which could provide for appropriate "take-down" action.

Similar Fears

In a detailed assessment of the constitutionality of the Cybercrime Bill 2019, published in August 2021, the Windhoek-based Economic Policy Research Association (EPRA) found that[8]:

"This bill is very likely unconstitutional, for various reasons. It clearly impugns the constitutional right to privacy. This is acknowledged in the bill itself. It provides for wide-ranging powers to a "Management Committee" (of possibly only two persons) to access any data and communication in private domain, on the sole discretion of the Minister responsible for technology.

There is no specific safeguard of data that would otherwise be confidential, for example information subject to client-attorney privilege, doctor-patient privilege, funding to political parties within the statutory prescribed limits, membership to private institutions, even intellectual property held by private organisations or businesses. The data on ongoing investigations by

[7] "Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been transparently and accurately publishing information about the use and scope of communications surveillance techniques and powers; and to publish periodic reports and other information relevant to communications surveillance."

[8] The full report by the Economic Policy Research Association (EPRA) can be accessed at the following link: https://drive.google.com/file/d/1Nvnj135HiX6X39Tnz4A-ojiSPSbkT0Ez/view?usp=sharing

the Anti-Corruption Commission can also be accessed by persons appointed through political channels, and even be shared with foreign entities.

The bill does address some legitimate issues of concern, such as cyber hacking and child pornography, but the powers provided to Government to access private information in the process are largely unlimited. Once the Government uses this power to obtain otherwise private data and communications, there is no remedy, for the data would have been accessed and possibly distributed already. A court cannot be approached to interdict the Government from accessing data as the process up to such point of access is done in secret, unknown to any affected person.

There is little safeguard against government surveillance of private citizens and organisations for possible sinister reasons, which then allows for the State to become a surveillance state unchecked by constitutional safeguards. We urge policymakers to revisit this bill and reconsider the issues addressed herein.

We implore our policymakers to identify the numerous constitutional rights and freedoms (not only the right to privacy as stated in the bill itself) this bill will breach and to then continue to engage civil society, the Namibian public, to amend the bill to ensure that the protection it aims to provide is balanced, reasonable, and achieved through constitutional means while upholding the principles of the rule of law."

4. Conclusion and recommendations

As this paper shows, the draft Cybercrime Bill (2019) has serious, but fixable flaws, which can and should be appropriately and adequately addressed as the eventual substantive draft is crafted and finalised.

It is with this in mind that the following recommendations are made:

- That the Namibian government prioritise the country's acceding to the Budapest Convention on Cybercrime, as articulated in the National Cybersecurity Strategy and Awareness Raising Plan 2022 – 2027;
- That the crafting and drafting of the eventual substantive Cybercrime Bill incorporate multi-stakeholder consultative processes towards ensuring meaningful inclusivity;
- And that the legal drafters use the Namibian Constitution's bill of fundamental human rights and freedoms (Chapter 3) as their guide in crafting and drafting human rights respecting provisions of the eventual substantive Cybercrime Bill.

ABOUT THE AUTHOR

Frederico Links has been an IPPR Research Associate since 2009. He has focussed on democracy and elections, party political finance, empowerment policies, internet governance, and public procurement. He has previously worked as a journalist and editor for a number of Namibian news media. He is the Chairperson of the Access to Information in Namibia (ACTION) Coalition which advocates and campaigns for an access to information law in Namibia.

About Global Partners Digital

Global Partners Digital (GPD) is a social purpose company working to enable a digital environment underpinned by human rights. GPD does this by making policy spaces and processes more open, inclusive and transparent, and by supporting public interest actors to participate strategically in them.

About IPPR

The Institute for Public Policy Research (IPPR) is a not-for-profit organisation with a mission to deliver independent, analytical, critical yet constructive research into social, political and economic issues that affect development in Namibia. The IPPR was established in the belief that free and critical debate informed by quality research promotes development.

Institute for Public Policy Research (IPPR)
House of Democracy
70-72 Frans Indongo Street
PO Box 6566
Windhoek
Namibia
info@ippr.org.na
www.ippr.org.na
Tel: +264 61 240514