JULY 2026

IPPR 25 YEARS OF INSIGHT, DEBATE & IMPACT

PREVENTING OVERREACH:

HUMAN RIGHTS IMPLICATIONS OF NAMIBIA'S CYBERCRIME PROPOSALS

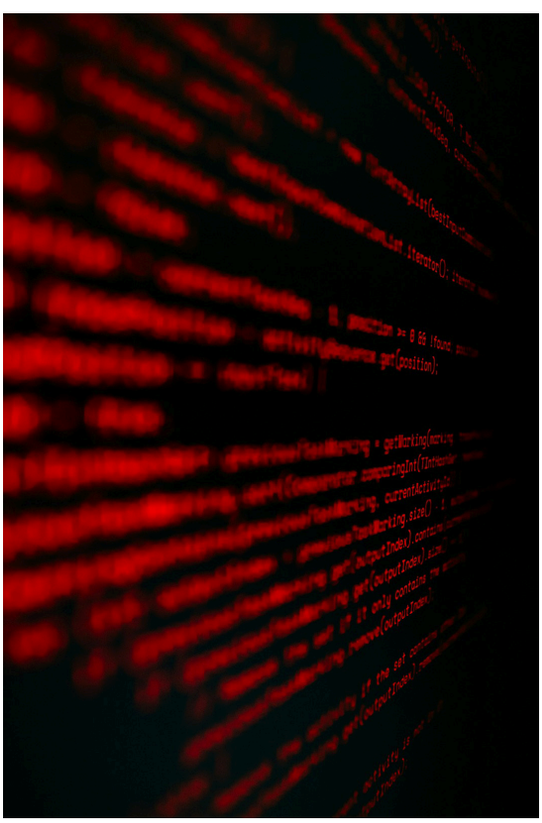
BY FREDERICO LINKS

Government of Ireland
International Development Programme

This paper forms part of a series of IPPR research publications supported by the Embassy of Ireland. The views and opinions expressed in this paper do not necessarily reflect those of the Embassy of Ireland.

IPPR 25 YEARS OF INSIGHT, DEBATE & IMPACT

Table of Contents



Cover image courtesy of Unsplash

Photo by Christina @ wocintechchat.com M on Unsplash

1. Overview of the draft Cybercrime Bill 2026

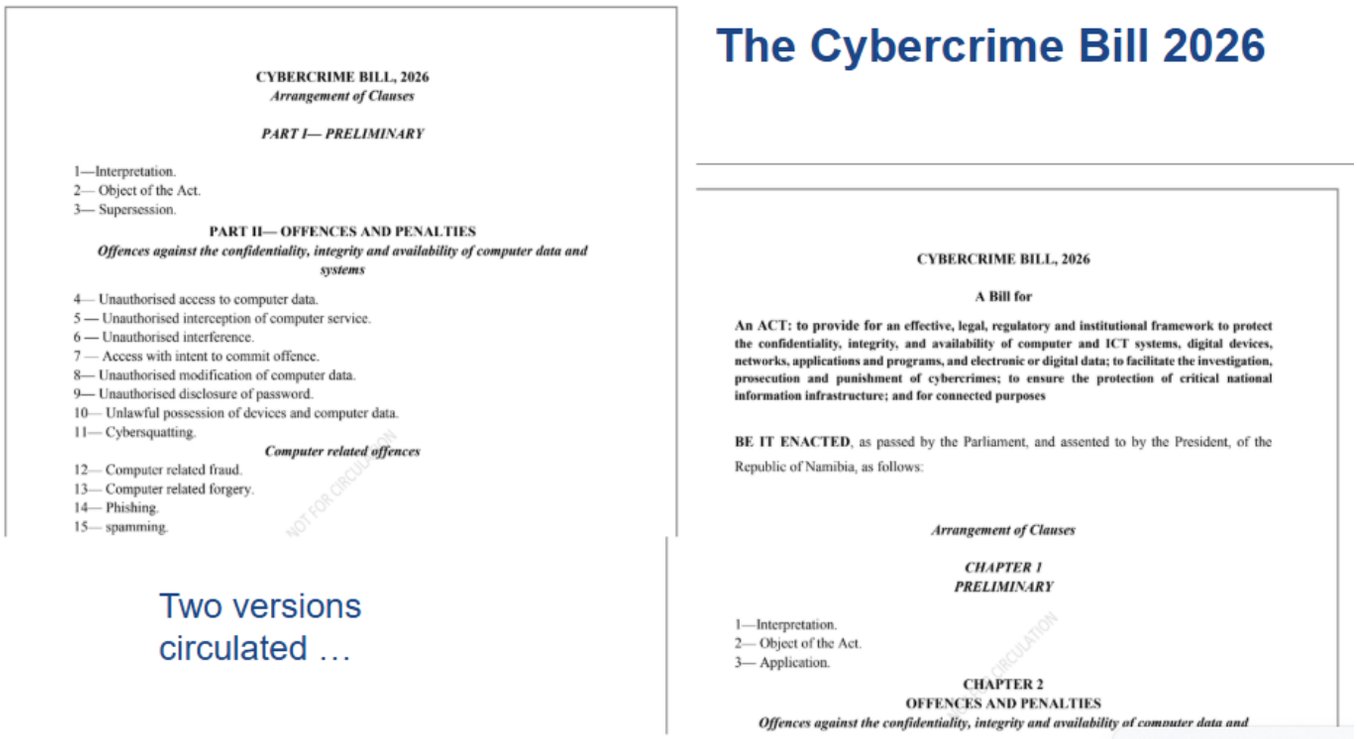
In February and March 2026 versions of a draft Cybercrime Bill were made available to stakeholders for scrutiny and input by the Ministry of Information and Communication Technology (MICT).

The 2026 draft is markedly different from a draft that was released for consultation in 2019-2020, and not in a good way. In fact, the 2026 draft comes across as a rough consultant's draft, rather than a substantive draft ready for serious and final consideration, and certainly nowhere near appropriate for tabling in parliament for debate and enactment.

While the 2019-2020 draft was significantly constitutionally flawed, the 2026 version is way worse, as this brief aims to illustrate.

To be clear from the outset, the draft Cybercrime Bill 2026 is fundamentally incompatible with the Namibian Constitution in numerous respects. This is because the way several offences and investigatory powers are drafted means that ordinary transparency practices - journalism, whistleblowing, public-interest reporting, documenting of wrongdoing, publishing leaked information, or even naming powerful actors - can be reframed as criminal conduct under the pretext of combatting cybercrime. At the same time, the bill, as drafted, can also plausibly justify internet shutdowns, authorise the banning of visual private networks (VPNs) and even criminalise encryption and anonymity.

This brief shows and argues that while it is probably the case that the provisions of the bill were drafted in good faith to legitimately enable the effective detection, investigation and prosecution of a range of serious cybercrimes, including the production and distribution of child sexual abuse material (CSAM), the same well-intentioned provisions can be repurposed for repressive purposes.



The risk arises from vaguely formulated offences, broad investigatory powers, and open-ended justifications that allow authorities leeway, should conditions pertain at some point in the future, to reframe these provisions for repression and to treat transparency as a threat rather than a democratic safeguard. Taken together, the bill's provisions as drafted create a system where surveillance power is concentrated, scrutiny is minimal, and abuse is difficult to detect or challenge.

To emphasise, should such a repressive reframing occur, then the provisions of the bill, as drafted, could be used to:

- Criminalise the naming of powerful actors;
- Criminalise the publishing of leaked documents;
- Criminalise the protecting of sources;
- Criminalise online anonymity;
- Criminalise encryption;
- Criminalise whistleblowing;
- Criminalise investigative journalism;
- Criminalise civil society monitoring;
- Criminalise public-interest reporting;
- Criminalise legitimate online political expression.

Making all this even worse would be the fact that the courts would have limited ability to enforce rights, parliament would have no visibility, and the public would have no recourse.

In the final analysis, the draft Cybercrime Bill 2026, as it is, is the opposite of what a constitutional, rights-respecting cybercrime framework should look like.

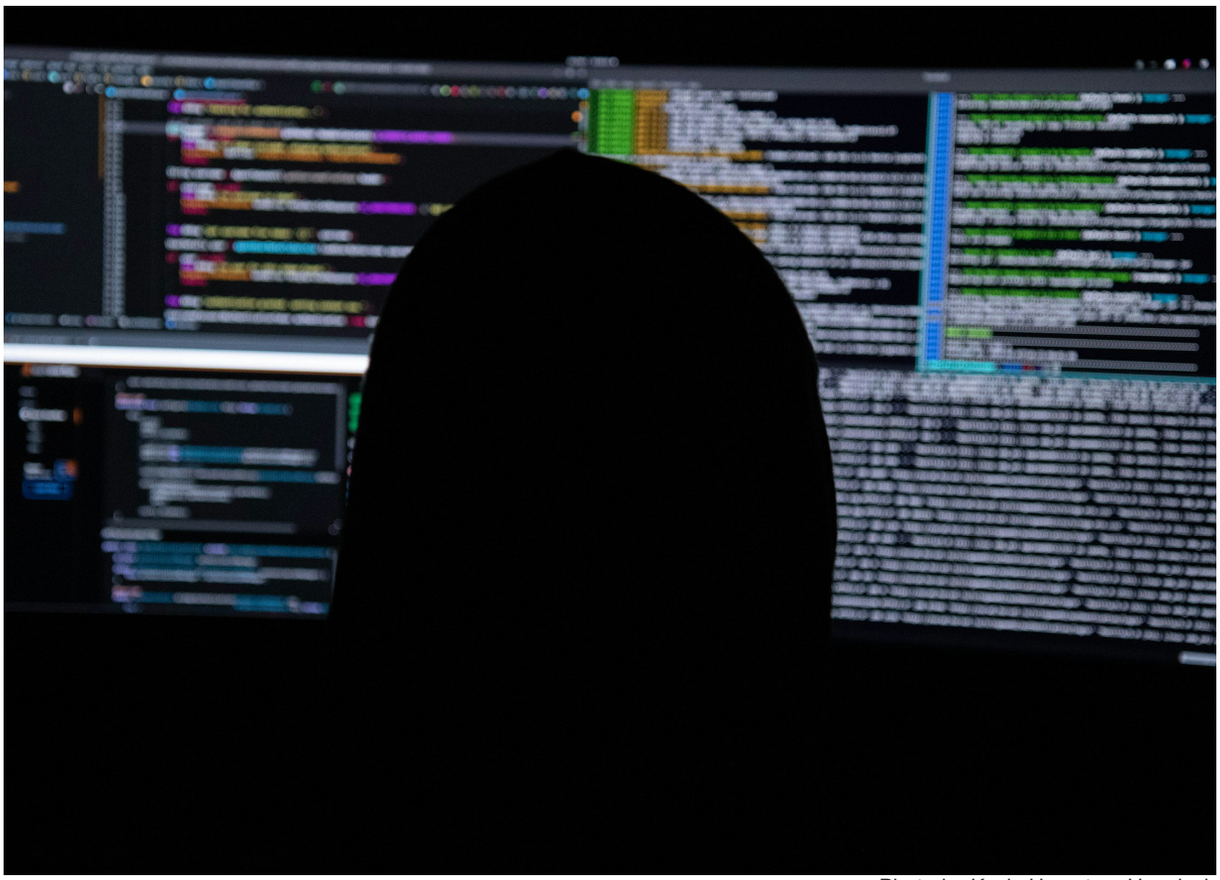


Photo by Kevin Horvat on Unsplash

2. Introduction

Cybercrime has become highly topical in Namibia over recent years as a number of high profile incidents have become emblematic and underscoring of how ill-prepared the country is in dealing with this growing and evolving scourge.

However, the country has been in cybercrime law and policy drafting mode since the early 2010s and various draft bills have been circulated for comment publicly over the last decade or so without any of them ever advancing to substantive draft, with only one ever making it as far as the Namibian parliament. In early 2017, in a move that caught stakeholders by surprise, then minister of Information and Communication Technology, Tjekero Tweya, tabled the Electronic Transactions and Cybercrime Bill in the National Assembly, arguing urgency, but the bill was almost immediately withdrawn by then prime minister Saara Kuugongelwa-Amadhila, following sustained and voluminous public criticism from civil society of what was essentially an under-baked and hugely flawed draft. In the wake of this incident, the Namibian government went ahead, on stakeholders' advice, and carved the electronic transactions sections out of the bill, passing the Electronic Transactions Act in late 2019, while committing to go back to the drawing board to craft a new stand-alone cybercrime bill.

In 2019-2020 a new cybercrime bill was circulated for stakeholder input, but this process never culminated with a substantive draft being developed even though the circulated draft had already been quite well-crafted, if still quite concerning in terms of its constitutional alignment, especially regarding human rights compliance.

Jump ahead to late January 2026, following more than five years of government silence and obfuscation of the status of cybercrime law drafting processes, when at the year opening engagement with Ministry of Information and Communication Technology (MICT) staff, minister Emma Theofelus announced that finalising a cybercrime bill for enactment had suddenly become a national security priority.

Photo: The Namibian

Emma Theofelus

Minister Theofelus stated:

> "As you know, legislation is an important instrument of governance to establish rule and order, and protect citizens. We also recognise that the public, industry and stakeholders have long waited for critical ICT legislations to be passed. Though this process has proven to be longer than anticipated, and given the importance of these laws, it is important that due diligence is done to ensure that laws are well crafted, adhere to Constitutional principles and are fit for purpose. Thus concerted efforts are underway to ensure the enactment of the Cyber Crime and Data Protection Bills as a matter of urgency.
>
> Therefore, we are due to resume stakeholder consultations on the draft Cybercrime Bill on 2 February 2026. This Bill is particularly important as it will address technology-facilitated crimes, including gender-based violence such as doxxing, online harassment, cyberstalking, image-based abuse, deepfake exploitation, and coordinated digital attacks; especially against women in public office and female journalists. In line with this, we signed the United Nations Convention Against Cybercrime during the last quarter. Cybercrime knows no borders, and therefore requires an internationally coordinated response. Our Cybercrime Bill will be aligned accordingly."

Following this ministerial announcement, a draft bill, dated end-January 2026, was circulated to stakeholders ahead of the consultative meetings. Another one, dated mid-February 2026, circulated immediately after the consultative meetings, but the two bills were identical. A third version, also almost identical to the first two, was circulated around the time that a validation workshop was convened in mid-April 2026. That said, whichever version of the bill is looked at, the text and provisions are highly problematic from a human rights and constitutional standpoint. The IPPR noted as much in a submission to the February consultative process.

This brief follows on from that February 2026 submission, providing a more detailed exposition of the potential human rights related threats that could be occasioned or enabled if the draft Cybercrime Bill 2026 is enacted as is.

3. The 'Repression Test'

For the purpose of assessing the human rights impacts of the draft Cybercrime Bill 2026, as drafted, the author has developed and deployed a simple 'repression test' with the help of an AI assistant to identify the potential human rights risks or threats in the draft text.

The 'repression test' asks a basic primary question, specifically: What human rights are implicated by the draft provisions of the draft Cybercrime Bill 2026?

This question consists of two secondary questions, which are:

- Which specific provisions / sections, as drafted, of the draft Cybercrime Bill 2026 pose a threat to human rights and what threat(s) do they pose?
- Which specific human rights, what activities, and who would be at risk?

These questions are applied to both the substantive (offences / crimes) and procedural (powers & procedures) provisions of the draft bill. The results of applying this 'repression test' to the draft Cybercrime Bill 2026 are mapped out in the following tables.

3.1 Substantive Provisions

Offence / Crime	Section	Human rights risks	Activities potentially threatened / criminalised	Actors / groups potentially threatened / criminalised	Risk / threat level
Unauthorised access to computer or electronic data	4	Freedom of expression, media freedom, the right to information, right to privacy	Viewing leaked documents, accessing public-interest information, exposing corruption, analysing data breaches, participating in digital activism	Journalists accessing leaked data, whistleblowers accessing internal systems to expose wrongdoing, cybersecurity researchers using dual-use tools, civil-society investigators, employees accessing systems in workplace disputes, researchers analysing publicly exposed but technically "unauthorised" data	High
Unauthorised interception of computer service	5	Freedom of expression, media and academic freedom, right to privacy, right to information	Cybersecurity testing; Digital forensics work; Whistleblowing involving leaked data; Journalists handling digital evidence;	Journalists; Whistleblowers; Ethical hackers; Cybersecurity researchers	High
Unauthorised interference	6	Freedom of expression, media and academic freedom, right to privacy, right to information	Routine IT maintenance; System updates; Penetration testing; Digital forensics work; Cybersecurity research; Whistleblowing involving leaked data; Journalists handling digital evidence; Employees accessing systems in workplace disputes	Journalists; Whistleblowers; Ethical hackers; Cybersecurity researchers	High

Access with intent to commit offences	7	Freedom of expression, media and academic freedom, right to privacy, right to information	Security testing and research; Whistleblowing; Journalistic investigation; Access for public-interest purposes	Journalists; Whistleblowers; Ethical hackers; Cybersecurity researchers	High
Unauthorised modification of computer or electronic data	8	Freedom of expression, media and academic freedom, right to privacy	Cybersecurity research; Harmless or routine digital activity; Journalists accessing leaked data; Whistleblowers handling evidence;	Journalists; Whistleblowers; Ethical hackers; Cybersecurity researchers	High
Unauthorised disclosure of password	9	Freedom of expression, media and academic freedom, the right to information, right to privacy	Parents sharing access with children; Couples sharing device passwords; Colleagues sharing access to a shared work account; IT staff providing temporary access; Teachers sharing login details for educational platforms; Community groups sharing admin credentials; Ordinary digital behaviour	Young people; Journalists; Whistleblowers; Cybersecurity researchers	High
Unlawful possession of devices and computer or electronic data	10	Freedom of expression, media and academic freedom, the right to information, right to privacy	Journalists receiving leaked data; Whistleblowers handling evidence; IT staff managing systems; Cloud-service users; People who unknowingly receive malicious files; Researchers analysing malware samples	Journalists; Whistleblowers; Ethical hackers; Cybersecurity researchers	High
Cybersquatting	11	Freedom of expression, media freedom, the right to information	Writing a restaurant review using the business name; posting “I love my Toyota”; a journalist naming a company in an article; a parody or satire account; academic commentary on a brand; registering a domain name that includes a generic phrase used by a business.	Investigative journalists investigating companies; Consumer criticism; Consumer reviewers of brands; Academics doing critical analysis; political commentators criticising companies; Comedians satirising companies or brands	High

Computer related fraud	12	Freedom of expression, media freedom, right to privacy	Routine IT maintenance; System updates; Data migration; Automated processes; Whistleblowing involving leaked data; Investigative journalism handling digital evidence	Whistleblowers; Investigative journalists; Civil society monitors	High
Computer-related forgery	13	Freedom of expression, media freedom, right to privacy, the right to information	IT staff correcting errors; System administrators restoring backups; Data migration processes; Whistleblowers exposing wrongdoing; Journalists handling leaked data	Whistleblowers; Investigative journalists; Civil society monitors	Moderate
Phishing	14	Freedom of expression, right to privacy,	Political campaign messages; Advocacy or civil-society mobilisation; Union organising; Community alerts; Marketing emails Newsletters; WhatsApp broadcasts; Automated notifications; Public-interest warnings	Political campaigners; Civil society advocates; Whistleblowers; Youth activists; Labour organisers; Young people; Journalists	Moderate
Spamming	15	Freedom of expression, right to privacy, freedom of association	Mass emails; Marketing messages; Political messaging; Advocacy campaigns; Automated notifications, Bulk SMS alerts; Social-media posting; Legitimate business communications	Political campaigners; Civil society petitioners; Whistleblowers; Youth activists; Labour organisers	High
Spreading of computer virus	16	Academic freedom, right to privacy	Cybersecurity research	Ethical hackers; Penetration testers; Digital forensics experts; Security researchers	Moderate
Identity theft and impersonation	17	Freedom of expression, media freedom, right to privacy	Children and young people sharing passwords, devices and accessing each others' accounts; Journalistic investigations; Whistleblowing exposing wrongdoing	Children and young people; Journalists; Whistleblowers	Moderate

Misuse of fake profile	18	Freedom of expression, media and academic freedom, right to privacy, freedom of association, equality and non-discrimination	Criminalises anonymity; Criticising government; Political debate; Satire or parody; Online activism; Participating in LGBTQ+ spaces; Heated arguments; Journalistic investigations; Whistleblowing exposing wrongdoing; Online research	Whistleblowers; Activists; Journalists; Opposition supporters; Satirical accounts; Community organisers; Academic researchers; Minority groups; Young people and children	High
Cyberbullying	19	Freedom of expression, media freedom, right to privacy	Harsh criticism; Political debate; Satire or parody; Online activism; Heated arguments; Journalistic investigations; Whistleblowing exposing wrongdoing; Labour organising; Consumer complaints; Interpersonal conflict; Legitimate political expression	Journalists; Activists; Opposition parties; Whistleblowers; Critics of government policy; Young people	High
Cyber extortion	20	Freedom of expression, media freedom, right to privacy, freedom of association	Whistleblowing; Political or labour activism; journalists threatening to publish a corruption exposé; Activists using digital campaigns	Whistleblowers; Activists; Journalists; Civil-society organisations	Moderate
Cyberterrorism	21	Freedom of expression, media and academic freedom, right to privacy, freedom of association, equality and non-discrimination	Activists organising protests online; Journalists accessing leaked documents; Whistleblowers exposing state wrongdoing; Security research; Civil-society groups researching extremism; Political opponents communicating online; Ordinary digital behaviour	Minority groups; Migrants; Political opponents; Religious communities; Activists; Journalists	High
Infringement of copyright and related rights	22	Freedom of expression, media and academic freedom, right to privacy, the right to information	Journalists quoting copyrighted text; Teachers sharing educational materials; Artists remixing or sampling; Researchers sharing extracts; Activists sharing graphics or documents	Journalists; Whistleblowers; Political critics; Civil-society organisations; Opposition parties; Online creators; LGBTQ+ activists using copyrighted imagery	High

Failure to moderate undesirable content	23	Freedom of expression, media freedom, right to privacy, freedom of association	Journalists managing newsroom accounts; Civil-society organisations campaigns; Satire, parody, or opinion; Community WhatsApp group admins; Facebook page moderators; Youth running school clubs; Church groups; Political-party volunteers; Ordinary citizens managing family groups	Opposition parties; Journalists; Activists and NGOs; LGBTQ+ groups; Minority communities; Critics of government policy; Ordinary citizens	Severe
Pornography	24	Freedom of expression, media and academic freedom, right to privacy	Artistic expression; Sexual-health education; LGBTQ+ content,\ Gender-rights advocacy; Academic research; Legitimate adult sexual expression; Journalistic reporting involving nudity or sexual content	LGBTQ+ people; Sex workers; Women and girls; Young people; Artists and performers; Journalists; Academic researchers	High
Distribution of obscene or intimate images	25	Freedom of expression, media and academic freedom, the right to information	People may be criminalised for sharing content that is not actually harmful; LGBTQ+ content or consensual adult sexuality; Chill legitimate artistic, journalistic, or documentary work; Criminalise reporting on matters of public interest involving nudity or sexual content; Interfere with whistleblowing or human-rights documentation; Academic publication or documentation;	Journalists; LGBTQ+ people; Sex workers; Young people sharing consensual intimate images; People in informal or communal living arrangements; Platforms or intermediaries held liable without due process.	High
Voyeurism	26	Freedom of expression, media and academic freedom	Criminalise legitimate newsgathering, especially in public-interest journalism / investigations; Create a chilling effect on documenting police misconduct, corruption, or public-space events; Risk of discriminatory enforcement.	Journalists; Human-rights monitors; Whistleblowers; LGBTQ+ people; Sex workers; Young people; People in informal settlements or shared living spaces.	Moderate

Child pornography and related offences	27	Freedom of expression, media and academic freedom, right to privacy	Digital forensics work; Academic research on child abuse and protection; Journalists reporting on exploitation; NGOs documenting abuse for legal purposes	Journalists; Sexual and reproductive health workers; Civil society and academic researchers; Whistleblowers	High
Revenge Pornography	28	Freedom of expression, media and academic freedom, equality and non-discrimination, right to privacy	Consensual adult sexual content; Artistic or documentary images; Breastfeeding images; LGBTQ+ content; journalism involving sexual-abuse reporting; Whistleblowing involving misconduct with sexual elements	Journalists; Whistleblowers; Artistic photographers; LGBTQ+ people; Marginalised groups; Sexual and reproductive health workers	Moderate
Exposing vulnerable person to sexually explicit act	29	Freedom of expression, right to privacy, the right to information	Consensual adult sexual expression; Sexual-health education; Artistic performances; Therapeutic content; Online animations or drawings; Content that is not intended to be sexual but is interpreted as such; Accidental or unavoidable exposure.	LGBTQ+ people; Sex workers; People in conservative or rural communities; People with disabilities; Young people experimenting with sexuality.	High
Attempt, conspiracy, aiding and abetting	30	Freedom of expression, media and academic freedom, the right to information, the right to privacy	Journalists reporting on cybercrime techniques; Researchers studying malware; Whistleblowers exposing wrongdoing; Civil-society training on digital security; Accidental exposure; Online expression; Artistic performances, drag shows, sexual-health demonstrations, and adult entertainment involving consenting adults; Legitimate educational content.	Journalists; Academic and security researchers; Whistleblowers; Civil society actors; Artists and performers; Young people.	High

Key take-aways:
Cumulatively, the assessment of the substantive provisions indicate the following:

- There is serious constitutional concern attached to the provisions as drafted;
- While the intention to provision for a range of cybercrimes is welcome, it seems clear that most or all of the substantive provisions can be repurposed for repressive purposes;
- In this regard, the proposed clauses / sections reflect some of the more repressive cybercrime laws to be found on the African continent, drawing in significant respects from East African laws that have been deployed repressively over the years.

3.2 Procedural Provisions

Powers / Procedures	Section	Human rights risks	Activities potentially threatened / criminalised	Actors / groups potentially threatened / criminalised	Risk / threat level
Expedited preservation and partial disclosure of traffic data	**45**	Freedom of expression, media freedom, the right to privacy	Public-interest reporting; Anti-corruption work; Democratic participation; Whistleblower communications; Civil society investigations; Lawyer-client confidentiality	Journalists; Whistleblowers; Civil society actors; Lawyers and their clients	High
Production order	**46**	Freedom of expression, media freedom, the right to privacy	Public-interest reporting; Whistleblower communications; lawyer-client communications; Civil society communications	Journalists; Whistleblowers; Civil society actors; Lawyers and their clients	High
Powers of access, search and seizure for purpose of investigation	47	Freedom of expression, media freedom, the right to privacy	Journalistic sources; Legal privilege; Medical records; Counselling or religious communications; Whistleblower communication and information; Political party data and communications; Trade secrets	Journalists; Whistleblowers; Civil society actors; Lawyers and their clients; Political opposition; etc.	High
Real-time collection of traffic data	**48**	Freedom of expression, media freedom, freedom of association; the right to privacy	Journalistic sources; Lawyer-client communications; Whistleblower identities and communications; Political organising; Civil society networks and communications	Journalists; Whistleblowers; Civil society actors; Lawyers and their clients; Political opposition; etc.	High
Interception of content data	**49**	Freedom of expression, media freedom, freedom of association; the right to privacy	Private conversations; Political opinions; Religious beliefs; Sexual orientation; Health information; Journalistic sources; Legal advice; Whistleblower communications; Intimate relationships	Journalists; Whistleblowers; Civil society actors; Lawyers and their clients; Political opposition; Government critics; etc.	High

Deletion order	**50**	Freedom of expression, media freedom, freedom of association; access to information; the right to privacy	Political speech; Criticism of government; Satire; Investigative journalism; Leaked documents; Civil society reports; Human rights documentation; Content that is merely alleged to be unlawful	Journalists; Whistleblowers; Civil society actors; Lawyers and their clients; Political opposition; Government critics; etc.	High
Limited use of disclosed computer data and information	**51**	Freedom of expression, media freedom, freedom of association; access to information; right to a fair trial; the right to privacy	Political speech; Criticism of government; Satire; Investigative journalism; Leaked documents; Civil society reports; Human rights documentation	Journalists; Whistleblowers; Civil society actors; Lawyers and their clients; Political opposition; Government critics; businesses in disputes; etc.	High

Key take-aways:
Cumulatively, the assessment of the procedural provisions indicate the following:

- As with the substantive provisions, the procedural provisions, as drafted, raise significant constitutional alarms;
- Collectively, the procedural provisions suggest the installation of a formidable, expansive and highly intrusive mass surveillance regime, devoid of any sort of meaningful oversight, safeguards and transparency.
- In fact, the levels of intrusiveness that the draft Cybercrime Bill 2026 seeks to install will have the unmistakable effect of almost completely eradicating any notions of serious data protection or digital privacy (see 'The ladder of intrusiveness' below).

The ladder of intrusiveness

Power	Main sections	What it allows	Privacy impact level
Preservation & disclosure	45, 46	Preserve traffic data; compel stored data & subscriber info	Medium
Search & seizure of data/ devices	47	Enter premises, access, copy, seize, render data inaccessible	High
Real-time traffic monitoring	48	Ongoing capture of metadata on specified communications	Very high
Real-time content interception	49	Live interception of message/ content streams	Extreme
Takedown & destruction of data	50	Court-ordered removal/deletion of "unlawful" data	High
Reuse & withholding of data	51	Secondary use, sharing, denial of access to owner	Systemic / structural

4. Additional Aggravating Cross-Cutting Threats

The human rights risks or threats sketched in the previous section are by no means the only ones that should be considered when engaging with the draft text of the draft Cybercrime Bill 2026. In fact, some of the already spotlighted sections, when read together with others or combined, could be used to enable additional and equally egregious harms if implemented and applied as is.

When subjecting the provisions of the draft Cybercrime Bill 2026 to the 'repression test', the author specifically also assessed which sections of the text, as drafted, could enable the following:

- Internet shutdowns;
- Banning the use of virtual private networks (VPNs);
- Weakening or eradicating encryption (anonymity).

Concerningly, it was unequivocally established that a number of sections of the draft bill, if enacted and implemented in its current form, could be used to justify the perpetrating of the above harms by a potential future repressive state apparatus.

4.1 Internet shutdowns

The text of the draft Cybercrime Bill 2026 does not explicitly refer to internet shutdowns, but some of its sections can be used to plausibly justify, if unconstitutionally so, it has to be said, the enabling or authorising of internet shutdowns.

Sections posing the greatest threat

Sections	Threat Level	Why
47(2)(e)	Extreme	"Render inaccessible" can be applied to entire networks.
50	High	Allows blocking or deletion of entire platforms.
51(1)	High	"Public interest" can justify broad restrictions.
48 & 49	Medium - High	Enable operational control over ISPs.
47(1)(b)	Medium - High	Allows warrantless extension into ISP systems.

4.2 Banning the use of virtual private networks (VPNs)

Once again, it should be noted that the text of the draft Cybercrime Bill 2026 does not explicitly criminalise the use of virtual private networks (VPNs), but some of its sections can also be used to enable or authorise this harmful practice.

How VPN use could be criminalised

Section	How it could be misused
4	VPN access to foreign servers = "unauthorised access"
5	VPN tunnelling = "interception"
6	VPN encryption = "interference"
7	VPN bypassing blocks = "intent to commit offence"
11	Using VPN domain/IP = "unauthorised use of name/phrase"
17	Masking IP = "identity concealment"
47	Refusing VPN credentials = "obstruction"
47(2)(e)	VPN encryption = "rendering data inaccessible"
50	Blocking VPNs as "unlawful material/activity"
51	VPN use framed as "public interest" threat

4.3 Criminalising encryption (anonymity)

As with the other two threats discussed in this section, the draft Cybercrime Bill 2026 does not explicitly touch the subject of criminalising the use of encryption. However, once again, sections of the bill, if enacted as is, could be used to enable such criminalisation. Encryption becomes criminalised indirectly because several sections are drafted so broadly that they treat ordinary encryption, secure communication, and privacy-enhancing technologies as suspicious, obstructive, or unlawful.

How encryption could be criminalised

Section	How it could be misused
5	Use of encryption could be argued to be “interception” of communications
6	Encryption could be framed as “interference” because it prevents normal inspection
11	VPN use could be framed as using a domain name “in use by another person”
17	Using encryption can be framed as impersonation or identity concealment
47(2)(e)	Encryption can be argued as “rendering data inaccessible” or obstruction
48 & 49	Users can be targeted because encryption makes interception difficult or impossible
50	Encrypted services can be labelled “unlawful material or activity” and removed
51(1)(d)	Encryption becomes a “public interest” threat

Key takeaways:

- As is illustrated, there appears to be considerable overlap between sections that can be used to enable internet shutdowns, authorise VPN bans or criminalise encryption (anonymity);
- Vague and overly broad provisioning and lack of definitional clarity around some of the sections of the draft Cybercrime Bill 2026 create openings or legal vacuums through which internet shutdowns, the criminalising of VPNs or the banning of encryption could be plausibly justified and enabled;
- The lack of safeguards proposed in the bill would establish a regulatory environment that would be ripe for abuse, if enacted as is.

5. Conclusion & Recommendations

The draft Cybercrime Bill, at least the versions seen through the first half of 2026, contain vague, overbroad, and/or unconstitutional provisions, whether regarding offences or procedures.

The Bill is significantly under-drafted and flawed and appears to be nowhere near a final draft, and it seems likely that a substantive draft will not be completed before the end of 2026.

As this brief has set out to illustrate and has already noted in earlier sections, the Bill is a compilation of grievous human rights threats. In short, the cumulative picture that emerges is one of a formidable, fearsome and comprehensive surveillance-plus-data-control system being proposed and provisioned.

Across its provisions, the pattern that surfaces is of:

- Legality gaps - Vague triggers ("reasonable grounds", "public interest", "unlawful material"), undefined terms, and weak foreseeability;
- Necessity & proportionality failures - No serious offence thresholds, no explicit least-intrusive-means tests, no duration limits for real-time powers, no minimisation;
- Due-process deficits - Limited or no notice, no clear right to challenge preservation, secondary use, or refusal of access; secrecy obligations on service providers;
- Privilege and role-based risks - No explicit protection for journalists, lawyers, doctors, or whistleblowers; real-time and stored-data powers can pierce all of these;
- Data-protection vacuum - No clear rules on retention, destruction, access logs, or secondary use, especially once section 51 kicks in.

Without fixing these very serious issues, the proposed law risks drifting from being about legitimately detecting, investigating and prosecuting crime to being a tool for securocratic abuse and overreach. In other words, a human rights-weakening and constitution-undermining framework of deeply intrusive and permanent bulk state surveillance that enables the suppression of free expression through repressive and selective enforcement.

That said, it is not too late to change this. Which is why the IPPR proposes the following recommendations.

Recommendations:

- The draft Bill should undergo further reforms to align with the UN Convention against Cybercrime and the Budapest Convention, including the requirement for offences to more clearly carry the element of intentionality;
- The procedural and substantive powers in Namibia's cybercrime bill should be subject to clear protections for privacy, freedom of expression, and other human rights;
- Recognising the need for thorough and harmonised protections for minors against all forms of sexual exploitation, both on- and offline, it is recommended that the offences relating to child sexual abuse material (child pornography) be removed from the draft Cybercrime Bill and for the equivalent provisions in the draft Combatting of Sexual Exploitation Bill be given precedence. Furthermore, the draft Combatting of Sexual Exploitation Bill should be finalised and tabled in Parliament with urgency.
- In the same vein, offences in the Cybercrime Bill relating to electronic harassment, especially through the sending of sexually explicit messages, should be reviewed for potential overlap with provisions in the draft Combatting of Harassment Bill and removed if necessary to ensure a single harmonised framework.
- Any investigative or monitoring measures provided for in the draft Bill, including the use of communications interception and forensic tools, must be subject to safeguards, oversight, and transparency measures that meet necessary and proportionate principles and the Declaration of Principles on Freedom of Expression and Access to Information in Africa; and
- The grounds for exercising intrusive digital surveillance powers should be much more clearly and narrowly defined and should not be subject to the nebulous concept of the 'public interest'. Rather, these should be restricted to a necessity for the investigations of serious offences, and where necessary to prevent serious imminent danger or death.

Notes

About the Author

Frederico Links

Frederico Links is a Namibian journalist, researcher, trainer and freedom of expression advocate. As a researcher he is mostly affiliated with Namibia's leading independent think-tank, the Institute for Public Policy Research (IPPR), where he coordinates a number of projects. In both his journalism and research, Links has a strong focus on good governance, human rights (including digital rights), state surveillance, corruption, rule of law, and transparency and accountability.

About the Institute for Public Policy Research (IPPR)

The Institute for Public Policy Research (IPPR) was founded in 2001 as a not-for-profit organisation with a mission to deliver, independent, analytical, critical yet constructive research on social, political and economic issues that affect development Namibia. The IPPR was established in the belief that development is best promoted through free and critical debate informed by quality research.

The IPPR is independent of government, political parties, business, trade unions and other interest groups.

Anyone can receive the IPPR's research free of charge by contacting the IPPR at the contact details below. Publications can also be downloaded from the IPPR website.

Institute for Public Policy Research (IPPR)
House of Democracy
70-72 Frans Indongo Street
PO Box 6566
Windhoek, Namibia
info@ippr.org.na
http://www.ippr.org.na

Incorporated Association Not for Gain Registration Number 21/2000/468
Directors: M M C Koep (Chairperson), D Motinga, J Ellis, G Hopwood, A Du Pisani, E Tjirera, N Shejavali