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

To Whom It May Concern

Submission in respect of the draft Cybercrime Bill 2026

Introduction

1. The following comments are made on behalf of the Institute for Public Policy Research (IPPR) and with regard to the draft Cybercrime Bill 2026 (a document titled 'NAMIBIA CYBERCRIME BILL-12.2.2026 Clean Version (1)'), which was shared as part of a consultative process in February 2026.

2. The aim of this submission is to flag certain concerning aspects of the draft Cybercrime Bill 2026, as it is, from a human-rights focused perspective.

3. First, though, it is apparent that this version of the draft Cybercrime Bill is markedly different from a version circulated for comment in 2019 and 2020, and appears to be a substantial redraft.

4. Second, in a public statement on 26 January 2026, the Minister of ICT stated: "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." In our assessment, this version of the bill does not align with the United Nations Convention Against Cybercrime.

5. The following comments are made with regard to the draft substantive elements (offences) and certain specific draft procedural elements in the draft Cybercrime Bill 2026.

6. The human-rights assessment of and comments on provisions of the Cybercrime Bill 2026 was done using a tool developed by Global Partners Digital (GPD) for this purpose, as well as an AI tool for analysis.

Comments

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

Offences / Crimes

7. **Unauthorised access to computer or electronic data** – This clause is one of the most foundational offences in cybercrime law. It has a legitimate purpose, but the way it is drafted creates major human-rights implications because it is extremely broad, attaches very severe penalties, and applies even when no harm occurs. It affects legality, proportionality, privacy, freedom of expression, and the work of IT professionals, journalists, researchers, and civil society.

8. **Unauthorised interception of computer service** – This clause is one of the most sensitive provisions in the Bill because it directly regulates surveillance, monitoring, communications privacy, and access to information. It has a legitimate cybersecurity purpose, but the drafting creates major human-rights implications, especially because subsection (3)(c) appears to remove protections even for people acting under lawful duties.

9. **Unauthorised interference** – This clause is one of the most far-reaching and high-stakes provisions in the Bill. It has a legitimate cybersecurity purpose, but the way it is drafted creates major human-rights implications because it is extremely broad, attaches very severe penalties, and applies even when the interference is temporary or not directed at any specific system. It affects legality, proportionality, freedom of expression, privacy, digital rights, and the work of IT professionals, researchers, journalists, and civil society.

10. **Access with intent to commit offences** – This is an unnecessary crime, as a properly formulated section on **Unauthorised access to computer or electronic data** would and should be broad enough to capture this crime in formulation. This clause articulates one of the core 'unauthorised access' offences in cybercrime law. It has a legitimate protective purpose, but the way it is drafted creates significant human-rights implications because it blends a broad access offence with very severe penalties and an unclear intent requirement. It affects legality, proportionality, freedom of expression, privacy, and the work of journalists, researchers, and IT professionals.

11. **Unauthorised modification of computer or electronic data** – This is an unnecessary crime, as a properly formulated section on **Unauthorised interference** would and should be broad enough to capture this crime in formulation. Even so, this clause is one of the most consequential provisions in the entire Bill. It expresses a legitimate cybersecurity purpose, but the way it is drafted creates major human-rights implications because it is extremely broad, carries very severe penalties, and applies even when the modification is temporary or causes no harm. It affects legality,

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

proportionality, freedom of expression, privacy, digital rights, and the work of IT professionals, journalists, researchers, and civil society.

12. **Unauthorised disclosure of password** – This is an unnecessary crime, as a properly formulated section on **Unauthorised access to computer or electronic data** would and should be broad enough to capture this crime in formulation. This clause expresses a legitimate cybersecurity purpose, but it also creates significant human-rights implications because it touches on privacy, freedom of expression, legality, proportionality, and the rights of workers, journalists, and ordinary users. It is one of the more sensitive provisions because it regulates the sharing of access, which is extremely common in everyday digital life.

13. **Unlawful possession of devices and computer or electronic data** – This clause has a legitimate cybersecurity purpose, but it also creates major human-rights implications because it touches on dual-use technology, freedom of expression, legality, proportionality, privacy, and the rights of cybersecurity researchers, journalists, and civil society. It is one of the most sensitive provisions in any cybercrime law because it determines whether Namibia protects or criminalises the people who keep systems safe.

14. **Cybersquatting** – This is an unnecessary crime, as a properly formulated section on **Unauthorised access to computer or electronic data** would and should be broad enough to capture this crime in formulation. This clause creates a new criminal offence for unauthorised use of another person's name, business name, trademark, domain name, or similar identifier on the internet. On the surface it looks like a simple anti-impersonation or anti-passing-off rule, but when you unpack it, the drafting is extremely broad, overlaps with existing intellectual-property and consumer-protection law, and creates significant human-rights and constitutional risks because it criminalises conduct that is normally handled through civil law.

15. **Computer related fraud** – This clause targets computer-enabled property loss through data manipulation or system interference, which is a core cybercrime. Its human-rights implications are therefore mixed: it strongly supports certain rights (privacy, property, economic security), but the drafting also raises concerns around legality, proportionality, due process, and potential overreach.

16. **Computer-related forgery** – This clause targets data manipulation for fraudulent or deceptive purposes, which is a core cybercrime. It is one of the more serious and technically grounded offences in the Bill, and it has clear human-rights justifications. But the way it is drafted, especially the very high penalties, the breadth of conduct captured, and the lack of precision around key concepts, creates important implications for legality, proportionality, due process, privacy, and freedom of expression.

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

17. **Phishing** – This clause has a legitimate cybersecurity purpose, but the way it is drafted creates major human-rights implications because it blends a serious cybercrime (phishing) with extremely broad, undefined conduct (sending unsolicited messages). The result is a provision that risks violating legality, proportionality, freedom of expression, digital rights, and due-process safeguards.

18. **Spamming** – This clause has a legitimate cybersecurity purpose, but the way it is drafted creates several important human-rights implications. These relate to legality, proportionality, freedom of expression, digital rights, and due-process safeguards. Because "spamming" is extremely common online and often ambiguous, the human-rights risks are real unless the offence is narrowly and precisely defined.

19. **Spreading of computer virus** – This clause is one of the more defensible provisions in the Bill, because it targets conduct that directly undermines cybersecurity, economic stability, and public safety. But even here, the human-rights implications depend on how precisely the offence is drafted and how proportionately it is enforced.

20. **Identity theft and impersonation** – This provision is one of the clearer and more defensible clauses in the Bill. It targets conduct that directly undermines privacy, security, and property rights, but it still raises important human-rights considerations around legality, proportionality, due process, and digital privacy.

21. **Misuse of fake profile** – A clause that criminalises "making use of a fake profile to cause harm" raises significant human-rights implications because it targets a very common form of online behaviour but does so with no definition, no harm threshold, and severe criminal penalties. The result is a provision that has a legitimate protective purpose but is drafted in a way that risks violating multiple constitutional and international rights.

22. **Cyberbullying** – The offence of cyberbullying, as drafted here, has a legitimate protective purpose, but the combination of no definition, no harm threshold, and extreme penalties creates serious human-rights implications. Because this clause is unusually broad and punitive, it affects freedom of expression, legality, proportionality, children's rights, digital privacy, and non-discrimination.

23. **Cyber extortion** – The offence of cyber extortion is one of the more straightforward provisions in the Bill, but it still carries important human-rights implications because it criminalises conduct that sits at the intersection of digital security, economic rights, privacy, and proportionality in criminal law. The implications depend heavily on how cyber extortion is defined in the Bill (if at all), and whether the definition is narrow, harm-based, and precise.

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

24. **Cyberterrorism** – This clause looks narrow at first glance but its human-rights implications are wide-ranging because it links ordinary digital behaviour to one of the most serious categories of crime. The key issues arise from vagueness, intent, proportionality, due-process safeguards, and freedom of expression and privacy in the digital environment.

25. **Infringement of copyright and related rights** – This clause criminalises certain forms of online copyright infringement, but because it does so through criminal law, with severe penalties, and with broad, unclear drafting, it carries several important human-rights implications. These implications sit at the intersection of freedom of expression, legality and due process, proportionality of punishment, digital rights, and economic rights.

26. **Failure to moderate undesirable content** – This provision creates one of the most far-reaching human-rights risks in the entire Bill, because it imposes criminal liability on any "administrator of an online account" who fails to "moderate and control undesirable content" once notified by an investigating authority. The combination of vague definitions, broad duties, and criminal penalties directly affects freedom of expression, media freedom, due process, privacy, and equality.

27. **Pornography** – A clause that criminalises the publication or dissemination of "pornography" or "pornography which is lascivious or obscene" through ICT systems carries major human-rights implications because it directly touches on freedom of expression, privacy, equality, legality, and proportionality. The combination of broad moral terms and extremely high penalties creates significant constitutional risks. This clause should be scrapped altogether.

28. **Distribution of obscene or intimate images** – A clause criminalising the transfer, publication, or dissemination of another person's intimate or obscene image without consent has strong human-rights justifications, but it also raises important risks if drafted or applied without precision. Words like "intimate", "obscene", and "image" require clear definitions. The implications sit at the intersection of privacy, dignity, freedom of expression, equality, and due-process safeguards.

29. **Voyeurism** – A provision like this has clear human-rights benefits, but also important risks if drafted or applied too broadly. Terms like "private act", "exposing sexual parts", and "reasonable expectation of privacy" require careful definition. The implications sit at the intersection of privacy, dignity, freedom of expression, due process, and equality.

30. **Child pornography and related offences** – This provision deals with child sexual abuse material (CSAM), grooming, solicitation, and the use of digital systems to

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

harm children. Unlike many other clauses in the Bill, this one addresses conduct that is inherently unlawful, inherently harmful, and universally criminalised under international law. Because of that, the human-rights analysis looks different: the core offences are legitimate and necessary, but the drafting still raises important constitutional and rights-based questions, especially around definitions, scope, proportionality, and overbreadth.

31. **Revenge Pornography** – This provision targets non-consensual disclosure of sexual images, a form of technology-facilitated gender-based violence. The clause focuses on disclosure, not creation. But if the image was created consensually, the law still criminalises disclosure without consent. If the image was created non-consensually, the offence may not capture the full harm unless other provisions apply. Its human-rights implications are therefore two-sided: it strongly advances certain rights, but the drafting also raises constitutional concerns around proportionality, clarity, and freedom of expression.

32. **Exposing vulnerable person to sexually explicit act** – This provision is aimed at protecting children and vulnerable persons from sexual exploitation, including exposure to sexual acts or sexualised content. That goal is fully aligned with Namibia's constitutional duties and international human-rights obligations. But the way the clause is drafted creates significant human-rights implications, both protective and risky, because it covers a wide range of conduct, includes digital and simulated content, and imposes severe penalties. International human-rights law requires criminal offences to be precise and predictable. The inclusion of "drawn" or "animated" content without clear limits risks over-criminalisation.

33. **Attempt, conspiracy, aiding and abetting** – The three subsections in this clause raise very different human-rights questions. Each engages constitutional and international human-rights standards in distinct ways. The first subsection (attempts, aiding, abetting) is acceptable only if the underlying offences are narrowly defined, harm-based, and constitutionally sound. If not, it becomes a multiplier of rights violations. The second subsection (enhanced liability for financial-sector employees) is more defensible, but still raises concerns. This subsection is defensible if "connive" is defined as intentional participation, not mere association or negligence, and if restitution is tied to proven benefit. The third subsection (criminalising attending a pornographic performance involving a "protected person") is the most sensitive and human-rights-intensive subsection. If narrowly drafted to target child sexual exploitation, the clause is legitimate and necessary. If drafted broadly, it risks violating freedom of expression, privacy, legality, and proportionality.

<u>Powers / Procedures</u>

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

The following comments are made with regard to the digital surveillance-related sections in the draft Cybercrime Bill 2026.

34. **Expedited preservation and partial disclosure of traffic data** – This provision creates a data-preservation power for investigators. It is one of the most important procedural clauses in the Bill because it governs how the State may compel individuals or service providers to preserve and disclose traffic data during an investigation. While the purpose is legitimate, the drafting raises serious human-rights implications around privacy, due process, necessity, proportionality, and potential for abuse.

35. **Production order** – This clause creates a court-supervised power for investigators to compel disclosure of stored computer data and subscriber information. Compared to many other procedural powers in the Bill, this one is much closer to international human-rights standards because it requires judicial authorisation. But it still raises important concerns around scope, definitions, privacy, necessity, and proportionality, especially given Namibia's constitutional protections for communications privacy (Art. 13).

36. **Powers of access, search and seizure for purpose of investigation** – This clause creates one of the most intrusive investigatory powers in the entire Bill: the ability to obtain a search-and-seizure warrant for electronic data, extend that search across interconnected systems, seize devices, copy data, render data inaccessible, and compel individuals to assist investigators. While such powers are legitimate in serious criminal investigations, the drafting raises major constitutional and human-rights concerns, especially around privacy, due process, necessity, proportionality, and compelled assistance.

37. **Real-time collection of traffic data** – This clause authorises real-time collection of traffic data, one of the most intrusive surveillance powers in the Bill. While it includes the important safeguard of judicial authorisation, it still raises serious constitutional and human-rights concerns because real-time traffic monitoring can reveal intimate details about a person's life, associations, movements, and communications patterns. It is one of the most sensitive powers in any cybercrime law.

38. **Interception of content data** – This clause authorises real-time interception of content data, the most intrusive surveillance power in the entire Bill. Unlike traffic-data monitoring (section 48), this provision allows the state to capture the actual substance of communications: messages, emails, voice notes, video calls, documents, images, and any other content transmitted through a computer system. Because content interception is equivalent to wiretapping, it triggers the highest level of constitutional scrutiny under Article 13 of the Namibian Constitution (privacy of

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

communications) and international human-rights law. The clause has a legitimate purpose, but the drafting creates major human-rights risks around privacy, proportionality, due process, secrecy, and potential abuse.

39. **Deletion order** – This clause empowers a court to order the removal, deletion, or destruction of computer data that contains "unlawful material or activity". It is one of the most consequential provisions in the Bill because it authorises state-mandated takedowns and destruction of digital content. While the purpose is legitimate in some contexts (e.g., child sexual exploitation material, malware, fraud tools), the drafting is extremely broad and raises serious constitutional and human-rights concerns around freedom of expression, legality, due process, proportionality, and risk of censorship.

40. **Limited use of disclosed computer data and information** – This clause governs how computer data obtained under the Act may be used, shared, withheld, or accessed. It looks administrative on the surface, but it is actually one of the most far-reaching and constitutionally sensitive provisions in the entire Bill because it determines:

- how widely investigators may reuse seized data;
- when data can be shared outside the original investigation;
- when data can be withheld from the person it was taken from;
- whether data can be used for purposes unrelated to the original case;
- whether privacy, fair-trial rights, and due-process protections are respected.

It has major implications for privacy, freedom of expression, due process, data protection, self-incrimination, and state power over digital evidence.

Concluding observations

41. The definitions section in the draft bill needs to be expanded considerably to address significant concerns with the absence of definitions (i.e. cyberbullying, cyber extortion, etc.) and definitional vagueness throughout the draft text. Similarly, the draft bill suffers from overbroad formulations in significant sections.

42. The element of intentionality needs to be clearly incorporated into some offences formulations (i.e. Unauthorised access to computer or electronic data).

43. The use of morality-laden and subjective or nebulous terms or concepts, such as "lascivious", "obscene", etc., in law is inconsistent with Namibia's legal drafting tradition and practice, which embraces objective or neutral terms or formulations in law.

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

44. The digital surveillance-related sections (45 - 51) appear to establish a parallel and more expansively intrusive surveillance framework to the one created under the Communications Act of 2009.

45. The many and serious structural issues identified throughout the draft bill and the quality of the text suggests that the bill is still in an early phase of drafting.

46. The drafters are encouraged to consider the draft provisions of relevant bills in the drafting pipeline that might have an impact on the formulation of definitions, scope and procedures of the draft Cybercrime Bill 2026. These other bills are:
    - The draft Combating of Sexual Exploitation Bill;
    - The draft Combating of Harassment Bill;
    - The draft Prohibition of Unfair Discrimination, Harassment and Hate Speech Bill.

47. Similarly, the drafters are encouraged to view the Prevention and Combating of Terrorist and Proliferation Activities Act 4 of 2014, for the purpose of aligning the definition of "terrorist act". The drafters are also encouraged to consider the provisions of the Communications Act 8 of 2009 when drafting the substantive digital surveillance-related sections in the next version of the bill.

48. Finally, given that the draft bill substantially appears to still be a work-in-progress, the Ministry of ICT is encouraged to continue consultations and calls for inputs around subsequent drafts.

49. The human rights implications flagged briefly in this submission are discussed in greater detail in the briefing paper titled 'Preventing Overreach: Human-rights implications of Namibia's cybercrime proposals', which can be accessed via the IPPR's website, www.ippr.org.na.

Compiled by:

Frederico Links

February 2026