The Gambia: Cybercrime Bill 2023

March 2024

Legal analysis

Executive summary

In this analysis ARTICLE 19 provides a close look at a draft Cybercrime Bill (the Draft Bill) for its compliance with international freedom of expression standards.

ARTICLE 19 has worked for many years with several civil society organisations to analyse the state of freedom of expression in the Gambia, as well as on cybercrime issues generally. Against the backdrop of an increasingly repressive environment for journalists and human rights defenders in the Gambia, ARTICLE 19 is deeply concerned that the Bill will serve to effectively crush the exercise of online freedom of expression and dissent in the country. At the outset, we point out the following issues:

- **The Bill would make an alarming scope of online speech a crime under the guise of combating 'cybercrime'.** The majority of proposed offences have nothing to do with cybercrime, apart from having the word "cyber" or "computer" attached. Instead they represent a broad effort to criminalize a wide range of speech online, from "false news" and "prurient" speech, to causing "harm" to the "self-esteem" of political figures. Provisions that are framed as protecting against 'cyberbullying' are instead so broadly crafted as to allow for the punishment of journalists for reporting on or criticizing public officials.

- **The Bill would make media organizations, civil society, and their senior leadership individually criminally liable for stories and investigations.** Under the Bill, senior leadership of corporate entities would be individually criminally liable for the actions of entities, and they would have the burden to prove that they actively conducted "due diligence" of published content. Given the Bill's wide criminalization of "false news" and statements made against the reputation of officials, the Bill would put the editors and leadership of any media or human rights organization at risk for any story or investigation issued by that entity. This creates a potent weapon for the government to cripple any opposition media or civil society groups.

- **The publication of evidence or data in the public interest could be criminalized.** The computer crime offences are so broadly worded that they make any "unauthorized act" in relation to a computer or "data" a crime. Read on its face, this provision would appear to criminalize a journalist who publishes incriminating text messages, which by its nature would be "unauthorized" by the official incriminated.

- **The Bill would create significant police and surveillance powers that in some cases are subject to no judicial or similar independent oversight.** These powers, including preservation and production orders which may be issued at will by law enforcement, are accompanied by gag orders on service providers with no opportunity for appeal.

- **The Bill would criminalize digital security and legitimate academic or security research.** Other police powers include the ability to force service providers to compel decryption

of content, as well as hold the mere possession of digital security tools, without intent to commit any crime, a criminal offence in itself. This would have the effect of chilling vital tools for protection of sources, confidentiality of communications, and physical safety of journalists and human rights defenders. Moreover, the cyber-dependent offences of the Bill do not contain public interest carve-outs that would protect the legitimate use of computers or software for auditing or research purposes.

ARTICLE 19 observes that the Draft Bill comes at a moment when nations are debating an international convention on cybercrime at the UN level, in a process the Gambia is actively participating in. It is thus questionable why the Bill is necessary at this point in time, when States are currently attempting to reach a consensus on the international standards that govern both substantive offences as well as investigative provisions that, if passed, would imminently require the Gambia to rewrite its new domestic legislation. To be sure, the draft Bill does not even reflect the current draft text of the proposed convention, which contains higher thresholds to establish criminality and numerous references to international human rights standards that are absent in the Bill. While ARTICLE 19 and numerous human rights organizations have taken issue with the UN negotiations and current draft text of the Convention, we note that the Bill falls even short of that standard.

ARTICLE 19 believes the Bill to be fatally flawed in its current state. ARTICLE 19 urges the drafters of the Bill and the relevant committees in charge of scrutinising it to address the shortcomings identified above to ensure the compatibility of any cybercrime legislation with international standards of freedom of expression. We also encourage the proposal to be tabled in anticipation of any outcomes of the ongoing UN cybercrime convention negotiations. We stand ready to provide further assistance in this process.

Key recommendations:
While we believe the draft Bill is fatally flawed, we also offer the following specific recommendations should the draft Bill proceed for further deliberations in the Parliament:

- Include, in a separate provision, reference to the Gambia's obligations under international human rights law to protect and promote freedom of expression, as well as an affirmation that no provision of the Bill will be used to stifle the activities of journalists, human rights defenders, or dissidents.
- Strike Articles 5-8 entirely, as these offences are not cyber-dependent offences and have no place in a cybercrime legislation. They uniformly constitute restrictions on freedom of expression by criminalizing valid criticism of public officials.
- Strike Article 15 as written; individual criminal liability for corporate actions should never automatically attach in a "guilty unless proven innocent" manner, but instead must require specific intent to cause an identifiable harm that is justified under international standards.
- Remove content-based offences elsewhere in the Bill, including in Article 12(7) which punishes "pornographic" and "prurient" content, as they are not compatible with international law.
- Strike Article 12 as written, which vaguely punishes "unauthorized acts" in relation to a

computer system or data, whereby "acts" are never defined. This fails the test of legality and is so broadly worded that it would criminalize public interest reporting.

- Strike Article 13 as written, which punishes the mere possession of certain data or software with no requirement of criminal intent. The provision does not track any existing internationally or regionally accepted definitions of cybercrime, and would criminalize not only academic and security research but also the widespread use of digital security and anonymity tools by journalists and human rights defenders.
- Strike Articles 9(4), 10(3), 11(2), and 12(4), which explicitly eliminate the requirement for specific intent to impact computer systems or data. Instead, make clear that every cyber-dependent offence requires specific, dishonest intent.
- Include clear requirements of "serious harm" before criminal liability attaches.
- Include a public interest defence to protect publicly beneficial cyber-dependent conduct.
- Strike Article 16(2)(vii), which allows compelled decryption, undermining a necessary tool for the realization of the right to freedom of expression by journalists, human rights defenders, and the public at large.
- Provide for mandatory independent review of any preservation or production orders issued by law enforcement pursuant to Articles 19 and 20, and eliminate the automatic gag order for recipients as well as afford an opportunity to judicially challenge the validity of such an order.
- Define key terms such as what it means to "expeditiously" or "sufficiently" comply with orders, in order to provide legal certainty.
- Remove Part IV, which goes beyond the scope of a cybercrime bill, explicitly applies beyond the scope of the Bill, and seems more appropriately placed in separate mutual legal assistance or extradition legislation. At a minimum, require voluntary data sharing to be subject to safeguards under domestic law.

Table of contents

Introduction

On 18 March 2023, the proposed 2023 Cybercrime Bill (the draft Bill) was approved in the first reading in the National Assembly of the Gambia and committed to the second reading in the Assembly Business Committee.

ARTICLE 19 finds that the draft Bill is problematic from the perspective of the international human rights and freedom of expression standards. We have extensive experience in analysing cyber-crime and cybersecurity legislation, as well as various freedom of expression laws. Most recently, ARTICLE 19 has actively participated in several rounds of ongoing negotiations to propose a comprehensive treaty on cybercrime at the UN level, as well as participated in the Gambia's most recent Universal Periodic Review (UPR).[1]

In that UPR, the Gambia stated that it has "committed itself to upholding freedom of expression."[2] However, we are deeply concerned at how true this commitment holds in light of the recent downward trend of media freedom in the Gambia. In November we observed a "discernible pattern of authorities curtailing free speech, stifling political dissent, and narrowing the civic space within the country," based on five instances of arrests of journalists, political figures, and human rights defenders merely for expressing opinions online or through traditional media.[3] While we have observed a positive track since President Yahya Jammeh's leadership came to an end in 2017, we note with particular concern the recent prosecutions of journalist Alhagie Bora and human rights defender Madi Jobarteh, in addition to comments by President Adama Barrow expressing hostility toward media freedom.

Specifically, in November 2023, Mr. Jobarteh was charged with seditious intention, incitement to violence, false broadcasting and information, which civil society organizations have called "politically motivated."[4] A coalition of Special Rapporteurs, including the Rapporteurs on the situation of human rights defenders, freedom of expression, and the right to privacy, wrote to express their concern that the charges are inconsistent with international standards of necessity and proportionality, as Mr. Jobarteh was being "discriminately targeted for the exercising of his right to freedom of expression by critically responding to the President's remarks." They emphasized that "[i]n accordance with international law and standards, individuals exercising the highest public authority, such as heads of state and government, are legitimately subject to criticism and opposition, by virtue

[1] Joint submission to the Universal Periodic Review of the Gambia by ARTICLE 19, Access Now and the Committee to Protect Journalists, 4 April 2019. Specifically, we recommended that the Gambia "Ensure full protection to all human rights online, including freedom of expression and privacy, and safeguard against arbitrary arrests and/or prosecutions of individuals for exercising their rights online."

[2] National report submitted in accordance with paragraph 5 of the annex to Human Rights Council resolution 16/21, A/HRC/WG.6/34/GMB/1, 22 August 2019.

[3] ARTICLE 19, The Gambia: Crackdown on free speech must stop, 7 November 2023.

[4] Amnesty International, Gambia: Further information: Drop charges against human rights defender: Madi Jobarteh, 21 February 2024.

of the office they hold."[5]

In general, President Barrow has consistently portrayed the United Democratic Party (UDP), the main opposition party, as a national security threat. He has also threatened to arrest individuals merely for expressing their opinions. On Friday, 29 September 2023, during the opening of a regional office for his party, the National People's Party (NPP), President Barrow threatened the opposition, the media and online activists, stating that he could use his presidential power to arrest them.[6]

Other arrests we have monitored closely include:

- Bakary Mankajang, the proprietor of the Mankajang Daily media outlet, was apprehended by Gambian law enforcement on 20 September 2023 in relation to his coverage of fatalities involving the police. Mankajang was subsequently granted bail and formally accused of 'interference with a witness' on 23 September 2023.
- On 15 September 2023, opposition activists Modou Sabally and Bayo Sonko were taken into custody; they have since been released on bail.
- Comedian Alhagie Bora Sisawo was initially arrested on 13 August 2023 after he criticised President Barrow. He was granted bail by Gambian police forces but the bail was revoked on 15 August 2023.

Against this backdrop, the draft Bill's numerous provisions punishing various forms of speech and criticism of officials online is alarming. We believe that it is vital that the Gambia's efforts to address cybercrime are consistent with its obligations to protect and promote freedom of expression under international law, and that countering cybercrime is not used as an excuse to repress dissent.

The analysis not only highlights concerns and conflicts with international human rights standards within the Bill but also actively seeks to offer constructive recommendations on how the Bill can be improved. We explain the ways in which problematic provisions in the Bill can be made compatible with international standards on freedom of expression and privacy, and set out key recommendations at the end of each section.

ARTICLE 19 urges the drafters of the Bill and the relevant committees in charge of scrutinising it to address the shortcomings identified above to ensure the compatibility of the Bill with international standards on freedom of expression. We stand ready to provide further assistance in this process.

[5] Mandates of the Special Rapporteur on the situation of human rights defenders; the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur on the right to privacy, Letter to the Government of Gambia Regarding the Situation of Madi Jobarteh, Ref: AL GMB 1/2023, 10 November 2023.

[6] "Nobody will henceforth insult me in this country and go scot-free. Even if anybody calls a radio station to insult, we will arrest the radio owner. We will also go after those who insult people on social media and even if a judge bails you, we will rearrest you. We want this country to move forward." ARTICLE 19, The Gambia: Crackdown on free speech must stop, 7 November 2023.

Applicable international human rights standards

The protection of freedom of expression under international law

The right to freedom of expression is protected by a number of international human rights instruments that are binding on states, including the Gambia; it is protected in particular by Article 19 of the **Universal Declaration of Human Rights** (UDHR)[7] and Article 19 of the **International Covenant on Civil and Political Rights** (ICCPR).[8] Article 9 of the African Charter on Human and Peoples' Rights, to which the Gambia is a signatory, guarantees the right to freedom of expression.

Additionally, **General Comment No. 34**,[9] adopted by the UN Human Rights Committee (HR Committee) in September 2011, explicitly recognises that Article 19 of the ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and Internet-based modes of expression.[10] In other words, the protection of freedom of expression applies online in the same way as it applies offline. State parties to the ICCPR are also required to consider the extent to which developments in information technology, such as Internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world.[11]

Similarly, the four special mandates for the protection of freedom of expression have highlighted in their **Joint Declaration on Freedom of Expression and the Internet** of June 2011 that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the Internet.[12] In particular, they recommend the development of tailored approaches for responding to illegal content online, while pointing out that specific restrictions for material disseminated over the Internet are unnecessary. They also promote the use of self-regulation as an effective tool in redressing harmful speech.

As a state party to the ICCPR, the Gambia must ensure that any of its laws attempting to regulate electronic and Internet-based modes of expression comply with Article 19 of the ICCPR as interpreted by the HR Committee and that they are in line with the special mandates' recommendations.

Limitations on the right to freedom of expression

While the right to freedom of expression is a fundamental right, it is not guaranteed in absolute terms. Restrictions on the right to freedom of expression must be strictly and narrowly tailored and may not put in jeopardy the right itself. The determination of whether

[7] UN General Assembly Resolution 217A(III), adopted 10 December 1948.
[8] GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc.
[9] CCPR/C/GC/3, adopted on 12 September 2011, available at http://bit.ly/1xmySgV.
[10] *Ibid*, para. 12.
[11] *Ibid*, para. 17.
[12] Joint Declaration on Freedom of Expression and the Internet, June 2011.

a restriction is narrowly tailored is often articulated as a three-part test. Restrictions must:

- **Be prescribed by law**: this means that a norm must be formulated with sufficient precision to enable an individual to regulate their conduct accordingly.[13] Ambiguous, vague or overly broad restrictions on freedom of expression are therefore impermissible;

- **Pursue a legitimate aim:** exhaustively enumerated in Article 19(3)(a) and (b) of the ICCPR as respect of the rights or reputations of others, protection of national security, public order, public health or morals. As such, it would be impermissible to prohibit expression or information solely on the basis that they cast a critical view of the government or the political social system espoused by the government;

- **Be necessary and proportionate**. Necessity requires that there must be a pressing social need for the restriction. The party invoking the restriction must show a direct and immediate connection between the expression and the protected interest. Proportionality requires that a restriction on expression is not over-broad and that it is appropriate to achieve its protective function. It must be shown that the restriction is specific and individual to attaining that protective outcome and is no more intrusive than other instruments capable of achieving the same limited result.[14]

The same principles apply to electronic forms of communication or expression disseminated over the Internet.[15]

Regulation of disinformation, "false information" or "fake news"

Concepts such as "false information," "disinformation," or "fake news," are not terms that are defined under international law. Therefore, they are not, as such, legitimate aims for justifying restrictions on the right to freedom of expression under Article 19(3) of the ICCPR. The HR Committee has been explicit now for decades that the "prosecution… for the crime of publication of false news merely on the ground, without more, that the news was false" violates human rights.[16]

In recent years, the international community has reiterated concerns about and demonstrated increasing consensus on the threat that such restrictions pose for freedom of expression. For example, in 2022, the **UN Secretary General** issued a report on disinformation from a framework of human rights and fundamental freedoms, in which he emphasised that "State responses to disinformation must themselves avoid infringing on rights, including the right to freedom of opinion and expression."[17] He cited the tripartite test of Article 19(3) of the ICCPR, as well as the African Commission on Human and Peoples'

[13] HR Committee, *L.J.M de Groot v. The Netherlands,* No. 578/1994, UN Doc. CCPR/C/54/D/578/1994 (1995).
[14] HR Committee, *Velichkin v. Belarus*, No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).
[15] General Comment No. 34, *op.cit.*, para. 43.
[16] Human Rights Committee, Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, Cameroon, CCPR/C/79/Add.116, November 1999.
[17] United Nations General Assembly, Countering disinformation for the promotion and protection of human rights and fundamental freedoms, Report of the Secretary General, A/77/287, 12 August 2022, para 10.

Rights, to emphasise the importance of responses to disinformation adhering to international and regional standards.[18] Ultimately, the Secretary General advised against a criminal approach to addressing disinformation, instead promoting access to robust public information, and ensuring that any regulatory measures be implemented with caution and separate executive function "to avoid abusive or manipulative approaches."[19]

The Secretary General's report followed a strong call by the **UN General Assembly** to ensure that attempts to counter disinformation adhered to human rights standards. The General Assembly made it clear that countering disinformation requires State responses to be in "compliance with international human rights law" and accordingly did not include criminal measures as an appropriate response.[20] The General Assembly explicitly highlighted the need for media and information-related technology literacy to be achieved "through independent and free media, awareness-raising and a focus on the empowerment of people."[21] Elaborating on effective solutions, the call emphasised the need to address disinformation in a multi-stakeholder fashion that includes civil society, media, and business, through "education, capacity-building for prevention and resilience to disinformation, advocacy and awareness-raising."[22] We observe, importantly, that the resolution was adopted without a vote.[23] Many West African countries sponsored the resolution on disinformation standards, including Nigeria, Côte d'Ivoire, Burkina Faso, and Guinea.[24]

The **Human Rights Council** subsequently echoed this call, reiterating the need that approaches to disinformation are rooted in human rights, and not used as a "pretext to restrict the enjoyment and realization of human rights or to justify censorship, including through vague and overly broad laws criminalizing disinformation."[25]

The **Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression** issued a comprehensive report on international standards surrounding disinformation in 2021.[26] In that report, she found that so-called "false news" laws typically failed to meet the three-pronged test of legality, necessity and legitimate aims set forth in Article 19(3) of the ICCPR.[27] Specifically, these laws usually "do not define with sufficient precision what constitutes false information," and "[w]ords such as 'false', 'fake', or 'biased'

[18] *Ibid*., para 14.
[19] *Ibid*., paras 26 and 27.
[20] *Ibid*., para 13.
[21] Resolution adopted by the General Assembly on 24 December 2021, Countering disinformation for the promotion and protection of human rights and fundamental freedoms, A/RES/76/227, 10 January 2022.
[22] *Ibid*., paras 7-11.
[23] Countering disinformation and promotion and protection of human rights and fundamental freedoms: resolution / adopted by the General Assembly, Vote summary, 24 December 2021.
[24] Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms, Report of the Third Committee, A/76/462/Add. 2, 1 December 2021, para 82.
[25] Human Rights Council, Role of States in countering the negative impact of disinformation on the enjoyment and realization of human rights, A/HRC/49/L.31/Rev.1, 30 March 2022.
[26] Disinformation and freedom of opinion and expression: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/47/25, 13 April 2021.
[27] *Ibid*., para 54.

are used without elaboration and assertions based on circular logic are made."[28] She called for States to work with the private sector to call for multi-stakeholder responses to disinformation in order to promote free, independent, and diverse media. The Special Rapporteur's report followed joint statements from the Special Procedures worldwide, including the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, expressing that "the human right to impart information and ideas is not limited to "correct" statements, that the right also protects information and ideas that may shock, offend and disturb, and that prohibitions on disinformation may violate international human rights standards."[29]

Other applicable regional standards reinforce these themes. For instance, the **Declaration of Principles on Freedom of Expression and Access to Information in Africa** requires states to "repeal laws that criminalise sedition, insult and publication of false news."[30] The Declaration advises the review of "all criminal restrictions of content," including criminal defamation and libel, to ensure they comply with international standards.[31]

Online content regulation

The above principles have been endorsed and further explained by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Special Rapporteur on FOE) in two reports in 2011.[32]

In the September 2011 report, the Special Rapporteur also clarified the scope of legitimate restrictions on different types of expression online.[33] He also identified three different types of expression for the purposes of online regulation:

- expression that constitutes an offence under international law and can be prosecuted criminally;
- expression that is not criminally punishable but may justify a restriction and a civil suit; and
- expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others.[34]

[28] *Ibid*. (Giving as an example the definition where "'a statement is false if it is false or misleading, whether wholly or in part, and whether on its own or in the context in which it appears.'")
[29] Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, adopted by the UN Special Rapporteur on Freedom of Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 3 March 2017.
[30] African Commission on Human and Peoples' Rights, Declaration of Principles on Freedom of Expression and Access to Information in Africa, November 2019, Principle 22(2).
[31] *Ibid*., Principles 22(1) and 22(3).
[32] Reports of the UN Special Rapporteur on Freedom of Expression, A17/27, 17 May 2011 and A/66/290, 10 August 2011.
[33] *Ibid*, para 18.
[34] *Ibid.*

In particular, the Special Rapporteur on FOE clarified that the only exceptional types of expression that States are required to prohibit under international law are i) child sexual abuse material ('child pornography' in the report); ii) direct and public incitement to commit genocide; iii) hate speech; and iv) incitement to terrorism. He further made clear that even legislation criminalizing these types of expression must be sufficiently precise, and there must be adequate and effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body.[35] In other words, these laws must also comply with the three-part test outlined above. For example, legislation enabling the use of blocking and filtering technologies to prohibit the dissemination of child sexual abuse material over the Internet through is not immune from those requirements.

Surveillance of communications

The right to privacy complements and reinforces the right to freedom of expression. The right to privacy is essential for ensuring that individuals are able to freely express themselves, including anonymously,[36] should they so choose. The mass-surveillance of online communications therefore poses significant concerns for both the right to privacy and the right to freedom of expression.

The right to private communications is strongly protected in international law through Article 17 of the ICCPR[37] which states, *inter alia*, that no one shall be subjected to arbitrary or unlawful interference with his privacy, family or correspondence. In **General Comment No. 16** on the right to privacy,[38] the HR Committee clarified that the term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorised by States can only take place when provided for by law, which itself must comply with the provisions, aims and objectives the ICCPR. It further stated that:

> [E]ven with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorised interference must be made only by that authority designated under the law, and on a case-by-case basis.[39]

The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has argued that like restrictions on the right to freedom of expression under Article 19, restrictions of the right to privacy under Article 17 of the ICCPR should be interpreted as subject to the three-part test:

[35] *Ibid*, para 22.
[36] *Ibid*, para 84.
[37] Article 17 states: "1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2) Everyone has the right to the protection of the law against such interference or attacks."
[38] HR Committee, General Comment No. 16, 23rd session, 1988, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994).
[39] *Ibid.*, para 8.

> Article 17 of the Covenant should also be interpreted as containing the said elements of a permissible limitations test. Restrictions that are not prescribed by law are "unlawful" in the meaning of article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute "arbitrary" interference with the rights provided under article 17.[40]

In terms of surveillance (within the context of terrorism in this instance), he defined the parameters of the scope of legitimate restrictions on the right to privacy in the following terms:

> States may make use of targeted surveillance measures, provided that it is case-specific interference, on the basis of a warrant issued by a judge on the showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack.[41]

The Special Rapporteur on FOE has also observed that:

> The right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of the administration of criminal justice, prevention of crime or combatting terrorism. However, such interference is permissible only if the criteria for permissible limitations under international human rights law are met. Hence, there must be a law that clearly outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality.[42]

Anonymity and encryption

The protection of anonymity is a vital component in protecting the right to freedom of expression as well as other human rights, in particular the right to privacy. A fundamental feature enabling anonymity online is encryption.[43] Without the authentication techniques derived from encryption, secure online transactions and communication would be impossible.

[40] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009, para 17.
[41] *Ibid.*, para 21.
[42] Report of the UN Special Rapporteur on Freedom of Expression, Frank LaRue, A17/27, 17 May 2011, para 59.
[43] Encryption is a mathematical "process of converting messages, information, or data into a form unreadable by anyone except the intended recipient" that protects the confidentiality of content against third-party access or manipulation; see e.g. SANS Institute, History of encryption, 2001.

The right to online anonymity has so far received limited recognition under international law. Traditionally, the protection of anonymity online has been linked to the protection of the right to privacy and personal data. In May 2015, the Special Rapporteur on FOE published his report on encryption and anonymity in the digital age.[44] The report highlighted the following issues in particular:

- Encryption and anonymity must be strongly protected and promoted because they provide the privacy and security necessary for the meaningful exercise of the right to freedom of expression and opinion in the digital age;[45]

- Anonymous speech is necessary for human rights defenders, journalists, and protestors. Any attempt to ban or intercept anonymous communications during protests is an unjustified restriction to the right to freedom of peaceful assembly under the UDHR and the ICCPR.[46] Legislation and regulations protecting human rights defenders and journalists should include provisions that enable access to and provide support for using technologies that would secure their communications;

- Restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law.[47] Laws and policies providing for restrictions to encryption or anonymity should be subject to public comment and only be adopted following a regular – rather than fast-track – legislative process. Strong procedural and judicial safeguards should be applied to guarantee the right to due process of any individual whose use of encryption or anonymity is subject to restriction.[48]

The Special Rapporteur's report also addressed compelled 'key disclosure' or 'decryption' orders whereby a government may "force corporations to cooperate with Governments, creating serious challenges that implicate individual users online."[49] The report stipulated that such orders should be

- based on publicly accessible law;
- clearly limited in scope focused on a specific target;
- implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets; and
- only adopted when necessary and when less intrusive means of investigation are not available.[50]

Cybercrime

[44] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye A/HRC/29/32, 22 May 2015.
[45] *Ibid,* paras 12,16 and 56.
[46] *Ibid,* para 53.
[47] *Ibid,* para 56.
[48] *Ibid,* paras 31-35.
[49] *Ibid*, para 45.
[50] *Ibid*.

No international standard on cybercrime exists. Out of the regional standards, the 2001 Council of Europe Convention on Cybercrime (the Cybercrime Convention) has been the most relevant standard.[51] Although the Gambia is not a signatory to the Convention, it provides a helpful model for states seeking to develop cybercrime legislation.

The Cybercrime Convention provides definitions for relevant terms, including definitions for computer data, computer systems, traffic data, and service providers. It requires State parties to create offences against the confidentiality, integrity and availability of computer systems and computer data; computer-related offences including forgery and fraud; and content-related offences such as the criminalisation of child sexual abuse material. The Cybercrime Convention then sets out a number of procedural requirements for the investigation and prosecution of cybercrimes, including preservation orders, production orders, and the search and seizure of computer data.

Finally, and importantly, the Cybercrime Convention makes clear that the above measures must respect the conditions and safeguards for the protection of human rights and liberties, consistent with the ICCPR and other applicable international human rights instruments.

Constitution of the Gambia

Articles 46 and 47 of the Gambia's Constitution protect the rights to freedom of expression, assembly, and media, respectively.[52] Specifically, Article 47 provides for protection against censorship, as well as protection from the disclosure of sources. It also provides that the State "shall not penalize any person for any opinion or view or the content of any broadcast, publication or dissemination."

[51] The Council of Europe Convention on Cybercrime, CETS No. 185, in force since July 2004. As of May 2015, 46 states have ratified the Convention and a further 8 states have signed the Convention but have not ratified it.
[52] Constitution of the Gambia (2020).

Analysis of the draft Cybercrime Bill

General Comments

Before laying down our specific concerns, ARTICLE 19 would like to make the following general comments about the draft Bill:

- **It primarily contains content-based offences criminalizing expression online:** We are primarily concerned that the draft Bill, despite its title, fails to narrowly focus on restricting cybercrime. It includes broad provisions that punish speech in several manners that have been explicitly rejected under international law, including by the HR Committee and special procedures. Concepts within the scope of criminalisation such as 'false information', 'cyberbullying', and 'pornography' are highly subjective and prone to abuse. Moreover, international human rights law protects information and ideas that may shock, offend and disturb.

- **It focuses on computer-enabled, rather than computer-dependent crimes:** Despite being titled a "cybercrime" bill, the bulk of the proposed offences actually concern conduct that does not actually require a computer to commit, but are merely traditional crimes conducted *using* a computer. The Bill even appears to admit that its criminal provisions are not cyber-dependent, devoting the heading of Article 6 to "computer related" offences. The inclusion of the word 'cyber' does not change this in substance—cyberbullying, for instance, is simply traditional harassment that occurs over a computer, rather than activity like hacking, which in contrast does not exist as a non-computer crime. Only Articles 8-14 purport to be computer-dependent (although even Article 12 punishes non-computer conduct). This goes well beyond the scope of criminalization of regional instruments such as the Budapest Convention.

- **It lacks meaningful intentionality or serious harm requirements:** As a general matter, the Bill does not contain substantive *mens rea* requirements as should ordinarily attach to criminal liability. Most of the proposed offences require that conduct be done "intentionally"; in some instances, an "intent to cause harm" is required. However, this is far from requiring "dishonest intent" or any specific intent to bring about a specifically articulated harm. Neither is "serious harm" required, which is particularly problematic given that some provisions lay out harms such as harm to "self-esteem" of officials or reputation.

- **It lacks procedural safeguards for human rights protections:** Procedural safeguards for human rights protections are markedly absent throughout the Bill. There is no reference in the Bill to the Gambia's obligations to uphold and protect the right to freedom of expression and other human rights protected by international law. The absence of any such provisions could threaten the entire Bill's compatibility with international standards and the enforcement of human rights in this area. This is particularly problematic given the breadth of law enforcement powers granted by the Bill.

Recommendations

Overall, ARTICLE 19 recommends withdrawing the Bill in its current state. If it progresses for further approval, it must be brought in line with international human rights standards. At minimum, the Bill:

- Must include explicit procedural protections respecting the Gambia's international human rights obligations.
- Must focus on a narrow set of cyber-dependent offences that do not go beyond those accepted in instruments such as the Budapest Convention.

Content-based offences

ARTICLE 19 observes that the draft Bill contains a plethora of content-based offences, which we detail below. As an initial matter, the inclusion of content-based offences are limitations on freedom of expression, and accordingly must be analysed under the three-part test as set forth by international law.

'False news' and disinformation

The draft Bill contains in Article 6 a criminalization of spreading "false news" or "information" against a person; Article 6(2) explicitly provides "no defence" if the speaker does not know the falsehood, instead requiring proving "reasonable measures" were taken to verify the accuracy of the information. This is a strict liability offence requiring no *mens rea*, as a publication of falsehood need not even be intentional. As a result, Article 6(2) serves to assume criminal liability upon publication and puts the burden on an individual to prove their innocence by showing they took "reasonable measures" to verify facts. This is incompatible with basic notions of fair trial and criminal due process.

Further, ARTICLE 19 reiterates that – as noted earlier – protecting persons from "false news" or other forms of disinformation is not, as such, a legitimate aim for justifying restrictions on the right to freedom of expression under Article 19(3) of the ICCPR. This is of particular concern given that the activist Madi Jobarteh was recently charged with publishing "false" information on account of criticizing the government.

As the four special mandates on freedom of expression cautioned in their 2017 Joint Declaration, the label of "fake news"/"false news" is increasingly being used by persons in positions of power to denigrate and intimidate the media and independent voices, increasing the risk of such persons to threats of violence, and undermining public trust in the media.[53] An important point of principle remains that "the human right to impart

[53] Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, adopted by the UN Special Rapporteur on Freedom of Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 3 March 2017.

information is not limited to 'correct statements', [and] that the right also protects information and ideas that may shock, offend or disturb." The four special mandates made clear that "general prohibitions on the dissemination of information based on vague and ambiguous ideas, including 'false news' or 'non-objective information', are incompatible with international standards for restrictions on freedom of expression."[54] While Article 6(1) states that it requires "intent to cause harm," it fails to articulate any specific harms. As such, it falls short of any permissible restrictions on expression.

Offences against reputation and 'cyberbullying'

The framing of the offence of 'cyberbullying' extends well beyond online harassment of the vulnerable, instead serving in reality as an extraordinarily broad criminal defamation law.

Specifically, Article 7 of the Draft Bill makes it an offence to use a computer system to "repeatedly cause fear, intimidation, humiliation or other damage or harm" to a person's "health, emotional well-being, self-esteem or reputation." We note that the notions of harm to "emotional well-being, self-esteem or reputation" are highly vague, subjective, and nowhere defined in the Bill or in international law. A similar provision appears in Article 6(1)(c), which prohibits using a computer to "bully, abuse or make derogatory statements against a person" (without a requirement of actually causing harm). Articles 6 and 7 appear to contain redundant provisions which may be therefore subject to separate and duplicate criminal penalties. It is worth emphasizing that there are absolutely no safeguards for public interest investigation or news reporting.

While 'cyberbullying' appears in the definitions section of Article 2, this 'definition' merely repeats the language of Article 7 in a circular manner, adding that anyone "assisting" or "encouraging" such conduct is also guilty of cyberbullying. It is unclear what it means to 'encourage' one to cause fear or harm to someone's reputation, and this captures a potentially limitless amount of conduct. Under this framing, a member of the public who is simply commenting or reposting a critical news article exposing the misdeeds of a government official could be deemed to be providing 'assistance' or 'encouragement' for bullying that official.

ARTICLE 19 notes that most investigative journalism that exposes misconduct of an official for the public benefit can be said to make "derogatory" statements or "harm" the reputation or "self-esteem" of the individual exposed. The problem with overcriminalization of these concepts is that they are inherently difficult to define, highly subjective, and extremely vulnerable to misuse. In the context of the Gambia's recent crackdowns on expression, critics and dissidents themselves may rightfully fear being accused of 'harassment'.

Additionally, broad criminal definitions of cyberbullying risk placing social media companies in a position of 'policing' speech on their platforms, which would tend to have a severe chilling effect on speech. Coupled with the broad criminal investigatory powers granted by the draft Bill, this sets an extremely low bar for invasions of privacy and police overreach.

[54] *Ibid.*

Finally, while some proponents of the Bill may wish to see action taken on the issue of cyberbullying, including this in a criminal measure is rarely a proportional response and is prone to backfire. ARTICLE 19 has provided legal analysis on how online harassment and abuse of women, particularly women journalists, has become more prominent in recent years, as well as best practices to address it.[55] ARTICLE 19 has also noted how bullying of women in the Gambia has impacted their ability to participate in political spaces.[56] It is important that societal responses to harassment be holistic and include a conversation with a variety of stakeholders including civil society and the private sector, particularly social media platforms where cyberbullying is most likely to occur. In our analysis, we lay out ways in which social media platforms can incorporate international legal standards, including the Guiding Principles on Business and Human Rights, to provide responsible and transparent approaches to cyberbullying and abuse that occurs in their platforms.[57]

Non-consensual sharing of intimate images and sexual content

Article 8 of the Draft Bill contains two separate categories of offences which must be analysed separately; the first are offences against privacy, and the second is an offence of sharing sexual content generally.

Non-consensual sharing of intimate images

First, Article 8(1) punishes using a computer to acquire "sexually explicit" photos, videos, or representations of another person without their consent or knowledge. The following provision further punishes using a computer to intimidate, coerce, or harass an individual by using that content. Provisions 8(4) and 8(5) provide for additional procedural protections for the confidentiality of victims, including preventing the publication of identifying information.

While this provision would appear intended to protect victims of non-consensual sharing of images (often referred to as 'revenge porn'), it is framed so broadly to actually potentially punish victims of abuse by perpetrators who are authority figures. For example, if a survivor of abuse has documented abuse of a sexual nature, transmitting evidence of such abuse in an effort to gain access to justice could be criminalized under the Bill. Criminalizing acts cannot be justified if their purpose or effect is to prevent legitimate criticism of public figures, the exposure of corruption, official wrongdoing, or to protect the reputation of heads of state or other public officials or public figures.[58] Worse, the 'privacy' and anonymity protections could be abused by officials or public figures to anonymously bring criminal claims against those who report on evidence of abuse. Article 8 provides no safeguards to protect against this scenario.

[55] ARTICLE 19, Online harassment and abuse against women journalists and major social media platforms, 2020.
[56] Cherno Omar Bobb, LG election: Female candidates face cyber bullying, others, The Point, 22 March 2023.
[57] *Ibid*., pp. 11-12.
[58] ARTICLE 19, The Global Principles on Protection of Freedom of Expression and Privacy, March 2017, Principles 3 and 13.

Article 8(1) is also overbroad in its definition of "sexually explicit content," which includes a "digital representation." This could include artistic expression and satire as forms of "representation," and provide a criminal cause of action for authority figures to respond to satire against them.

Criminalization of sexual content generally

Second, the draft Bill broadly criminalizes the sharing of sexual content generally, which is a distinct offence from the non-consensual sharing of intimate images. Article 8(3) makes it a crime to use a computer to "make available to the public" any "sexually explicit content of another person" *whether or not* it was obtained consensually. This would appear to make it a crime to share any sexual or intimate images online in the Gambia (or artistic or satirical representations), even where the subject consents. A related provision appears later in Article 12(7), which prohibits the electronic publication of "pornographic" or "prurient" content which has the effect to "deprave and corrupt persons."

ARTICLE 19 observes that outright bans on pornographic content are impermissible under international law. Sexual acts are not forms of expression that may be restricted. The Human Rights Committee has affirmed that restrictions on freedom of expression for the protection of public morals must be based on a broad understanding of what 'public morals' means. Historically, States have often been guilty of a form of paternalism in applying restrictions on sexually explicit material. Such paternalism is inconsistent with human rights guarantees, including freedom of expression, which presume that all adults are equal and responsible moral agents. It is not for a judge, or administrative officials, to decide what materials individuals should or should not be able to access, absent a real risk of actual harm.

As a result, the State bears the burden of demonstrating that any limitation to protect "public morals" is *essential* and strictly conducted in a manner of non-discrimination.[59] The Declaration of Principles on Freedom of Expression and Access to Information in Africa makes clear that "States shall not prohibit speech that merely lacks civility or which offends or disturbs."[60] That burden fails to be met here.

Incitement

Article 6(1)(b) of the draft Bill prohibits using a computer to "incite violence against a person." We note that there already exist clear international standards on incitement to genocide or incitement to discrimination, hostility or violence, and as such Article 6(1)(b) must be analysed under this framework. Specifically, incitement is defined under international law as "statements about national, racial or religious groups which create an **imminent** risk of discrimination, hostility or violence against persons belonging to those groups."

[59] Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, April 1985.
[60] Declaration of Principles on Freedom of Expression and Access to Information in Africa, Principle 23(3).

ARTICLE 19 has previously laid out a six-part factors test for evaluating incitement:

- Context of the expression;
- Speaker/proponent of the expression;
- Intent of the speaker/proponent of the expression to incite to discrimination, hostility or violence;
- Content of the expression;
- Extent and magnitude of the expression (including its public nature, its audience and means of dissemination);
- Likelihood of the advocated action occurring, including its imminence.[61]

Article 6(1)(b) as framed does not come close to meeting international standards; it fails to even include an imminence requirement, specificity to target individual vulnerable groups, or any nuance as to context.

Child exploitation materials

Article 5 of the draft Bill covers "child pornography" as defined in Article 2. ARTICLE 19 begins by observing that child sexual exploitation and the spread of child sexual abuse material (CSAM) are cyber-enabled offenses that engage multiple, complex human rights issues. Indeed, the Bill does not even list the offence under "computer related offences" despite the measure being titled a "cybercrime" law. For these reasons, a cybercrime treaty is not the right forum to discuss them. ARTICLE 19 urges States to uphold their obligations under international human rights law and adopt comprehensive approaches to addressing CSAM.

As drafted, Article 5 risks criminalizing content that may have scientific, educational, artistic, or literary value, notwithstanding the defence provided in Article 5(2)(a-c). It may also restrict the legitimate experience and expression of gender and sexuality of children and adolescents, as the definition in Article 2 only uses the phrase "sexually explicit conduct" with no further definition. We are particularly concerned about how criminalizing vaguely defined online content and activity will impact children seeking information about sexual and reproductive health and rights, sexual and gender diversity, discrimination and gender-based violence, and other topics that fall under the rubric of comprehensive sexuality education. Without further elaboration, the phrase "sexually explicit conduct" left undefined may be misused to criminalize the very vulnerable groups that the provision is intended to protect. We recall that the Committee on the Rights of the Child has advised that "States should avoid criminalizing adolescents of similar ages for factually consensual and non-exploitative sexual activity."[62] Further, such conduct may include "written material" and "writing." It is not clear the limits of what written material include, and whether this could give rise to the banning or sale of prominent, historically relevant books that are taught in universities.

[61] ARTICLE 19, Prohibiting incitement to discrimination, hostility or violence, 2012.

[62] Committee on the Rights of the Child, General comment No. 20 (2016) on the implementation of the rights of the child during adolescence, (CRC/C/GC/20), https://undocs.org/en/CRC/C/GC/20, para 40.

We note that the Bill contains some provisions providing 'defences' on account of "public good" or "reasonable grounds," and expressly includes the interest of "science, literature, or learning." However, an accused must "prove" this, and as such these merely shift the burden on individuals to defend the legitimacy of what may be permitted, when instead it is the burden of the government to justify restrictions on expression as *necessary* and proportionate to achieve a legitimate aim. As a result, providing a 'defence' provides insufficient protection and still threatens to have a severe chilling effect as it does not prevent underlying charges, forcing individuals to invest legal resources in defending themselves (which may be prohibitive for children or their families). This is of particular concern given that Article 5(3) includes in the definition of exploitation materials in written, visual, or audio formats that merely give the "impression" of being a child, and the only protection for children expressing themselves is to legally prove that they had "reasonable grounds" to do so.

Impersonation, blackmail, and threats

We note that Articles 6(1)(d)-(f) criminalize, respectively, impersonation, blackmail, and threats of criminal offences when using a computer. 'Impersonation', without any dishonest intent or specific intent to commit fraud, can easily cover forms of satire or performative art (i.e., if a comedian shares an impression on social media making fun of a public official). Further, blackmail and threats are not cyber-dependent offences and are inappropriate to address in a computer crimes law; here they fail to be articulated with any precision or sufficient *mens rea* requirement.

Recommendations:

- Articles 5-8 must be stricken entirely. They consistently fail the tripartite test of permissible restrictions of expression, particularly the test of legality in that they contain vague and overbroad prohibitions that have been routinely rejected under international standards. Many restrictions do not pursue a legitimate aim as explicitly enumerated in Article 19 para 3 of the ICCPR. Further, they constitute cyber-enabled, rather than cyber-dependent offences, and as such are inappropriate to include in a cybercrime law.

Liability of Media and Civil Society Organizations

Article 15 of the draft Bill contains an extremely problematic provision that attaches automatic criminal liability of actions taken by a corporation to its directors, managers, or those acting on the corporation's behalf. Specifically, Article 15(1) holds that any offence by a corporate body is "treated as committed" by any person listed in sub-parts (a) or (b) which include senior leadership or individuals acting as such. We are particularly concerned that this provision can be used to target the editors or leadership of media or civil society organizations for their statements, publications, or investigations online.

The liability is effectively automatic because for key officers of an organization to escape

liability, they have the burden to prove, under Article 15(2), that that they did not "consent" or have "knowledge" and also conducted "due diligence" to prevent a violation "as ought to have been exercised having regard to the nature of the person's functions and all the circumstances." This goes well beyond any permissible *mens rea* requirement for criminal liability, instead imposing a strict liability obligation for individuals to be actively investigating and preventing conduct of others, whether or not it is known to them.

In the context of media organizations, this can easily be used to criminally prosecute an editor-in-chief of a journalistic organization that is accused of publishing 'false news', as well as other key staff of the media outlet, if they do not conduct "due diligence" to prevent the story's publication. Most of the time, under Article 15's language, mere knowledge of a story would be enough to hold an editor criminally liable. The same might occur against the leadership of a human rights organization providing an investigation on government misconduct that has significant public interest value but is deemed objectionable under the draft Bill.

As a result, the provision on corporate liability effectively requires corporate entities to police themselves in order to escape liability.

Recommendations:

- Article 15 must be stricken as written; individual criminal liability for corporate actions should never automatically attach in a "guilty unless proven innocent" manner, but instead must require specific intent to cause an identifiable harm that is justified under international standards.

Cyber-dependent offences

ARTICLE 19 observes that the remainder of Articles 9 through 14 reference cyber-dependent offences, with the exception of Article 12, which punishes "pornographic" publications, or certain acts "in relation to a computer system." As a general matter, we note that several provisions, including Articles 12 and 13, create offences which do not appear in the Budapest Convention or are otherwise incompatible with international standards.

A common theme across these offences is that they generally do not contain requirements for specific, dishonest intent, or any requirement for actual or "serious harm." Further undermining intent requirements, numerous offences contain provisions explicitly stating that they do not require specific intent toward specific computers or computer data for a violation; these types of provisions are contained in Article 9(4) (unauthorized access), Article 10(3) (unauthorized interference), Article 11(2) (unauthorized interception), and Article 12(4) (unauthorized acts).

We comment further on specific problematic provisions below, although this list is non-exhaustive:

Criminalization of digital security technologies and research

Article 13 of the draft Bill provides strict liability for the manufacture, sale, receipt, or distribution of systems or data "without authorization" which are "designed primarily for the purpose of committing an offence." Articles 13(2)-(3) go further to indicate that the mere possession of such data, including a "document" recording the computer data, is itself an offence. These are punishable by up to three years imprisonment.

This provision is extremely dangerous; it completely re-writes "computer misuse" in Article 6 of the Budapest Convention into a strict liability offence criminalizing digital security technology. The key difference is that the Budapest Convention requires that production or sale be conducted *with the intent* to commit an offence, rather than simply that the device, program, or code is "designed" for an offence. We emphasize that Article 13 has no intent requirement.

Computer programs and data, by their nature, are typically use-agnostic (i.e., not necessarily designed with static end-uses in mind). Technologies are more often than not 'dual use', meaning that they may often be used for positive or negative purposes, just as a hammer might be used as either a tool or a weapon. This is the reason that the Budapest Convention includes not only an intentionality requirement, but also an explicit carve-out stating that criminal liability does not apply to instances where technologies are not acquired for committing of offences, such as for "authorized testing or protection of a computer system."

Indeed, Article 13 would threaten to criminalize not only legitimate security research, but also digital security tools that individuals may use to protect themselves from malicious cyber activities. Further, it would criminalize the use of privacy and anonymity tools; the dual-use nature of these tools may result in their users being accused of employing them for illicit activities. Journalists and human rights defenders routinely utilize encryption and anonymity tools in order to protect sources as well as their work and safety.

'Unauthorized acts' in relation to a computer system or data

The draft Bill punishes, in Article 12(1), any person who "does an unauthorized act" in relation to a computer system or data, where they "know" that it is unauthorized. Article 12(5) provides convoluted definitions including that a "reference to doing an act includes causing an act to be done," and that an "act" includes a "series of acts." Nowhere is it defined what an "act" entails, neither is the fact that an "act" must merely be in "relation" to a computer system clarified. There is no clarity at all on what conduct 12(1) criminalizes, and as such, it fails the test of legality.

Taking a broad reading, the breadth of such provisions as written might be abused to punish a journalist who publishes leaked text messages or incriminating photos of a government official, who then claims that it is an "unauthorized" use of their data.

Recommendations:

- Remove content-based offences, including in Article 12(7), which punishes

"pornographic" and "prurient" content.
- Strike Article 12 entirely, which fails the test of legality and is so broadly worded that it would criminalize public interest reporting.
- Strike Article 13 as written, which does not track any existing internationally or regionally accepted cybercrime, and would criminalize not only academic and security research but also the widespread use of digital security and anonymity tools by journalists and human rights defenders.
- Strike Articles 9(4), 10(3), 11(2), and 12(4), which explicitly eliminate the requirement for specific intent to impact computer systems or data. Instead, make clear that every cyber-dependent offence requires specific, dishonest intent.
- Include clear requirements of "serious harm" before criminal liability attaches.
- Include a public interest defence for cyber-dependent conduct that is beneficial to society.

Investigatory and Data-Sharing Provisions

The draft Bill contains a number of overbroad and problematic investigative provisions that are subject to widespread secrecy with next to no opportunity for service providers to challenge them. These provisions are not limited to the underlying offences of the Bill or cybercrime at all, but generally apply to any 'offence'. While this legal analysis does not comment on every aspect of investigative procedures, it does highlight some that have particular impacts on freedom of expression.

Compelled decryption

ARTICLE 19 is concerned that several provisions may be used to mandate forced decryption on private parties; this is explicitly contemplated by Article 16(2)(vii), which allows for application of warrants to "require a person in possession of decryption information" to grant "access to such decryption information necessary to decrypt data required for the warrant." Adjacent measures appear to allow to "extend the search or similar access" to computers or data outside the scope of the warrant, "as may be necessary" without a need for separate independent review. Failure to comply with these provisions is a separate offence constituting obstruction, and is punishable by up to two years imprisonment.

We note that encryption facilitates the exercise of the rights to free expression and privacy, and restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law. It is often the case that service providers do not even possess the technical capacity to decrypt end-to-end communications that pass through their systems; such providers should not face criminal penalty or contempt if this is the case.

Mandatory preservation, disclosure, and gag order

Article 19 of the draft Bill allows for any "authorised person" (which includes, pursuant to

Article 2, any member of law enforcement or an intelligence or cybersecurity agency meeting a requisite rank) to individually issue expedited preservation orders directly to any person or service provider. The recipient of such a preservation order, is, according to Article 19(4), subject to a gag order to keep the notice confidential and must comply under penalty of fine. While there is a requirement that the underlying data be required for an investigation and a risk that the data may be lost, there is also no independent review of whether that requirement is satisfied, or any opportunity for remedy by recipients to challenge the validity or implementation of the preservation order. Authorised persons are allowed to issue these notices at will without any need for a warrant.

Article 20 goes further to allow an authorised person to issue a written notice to a service provider, subject to the same confidentiality provisions, requiring the "expeditious" disclosure of traffic data as well as the path where it was transmitted. Judicial review is only mentioned via *application by the authorised person*; there is again no opportunity for independent review unless specifically sought by the law enforcement issuing the order. Neither is there an advance requirement for a warrant. Non-compliance with the traffic disclosure provision is also subject to fine.

These provisions raise numerous due process concerns, given that they allow law enforcement to issue orders that are subject to criminal penalty, without any requirement of (or right to) independent review. Further, vague terms such as a requirement of "expeditiously" responding or providing "sufficient" data, where non-compliance is subject to penalty, threatens to make service providers overshare in order to avoid sanctions.

International data sharing

Part IV of the draft Bill sets forth numerous aspects of information sharing, preservation, and access. These provisions are not limited to the offences of the Bill, but provide for a broad sharing protocol that extends well beyond cybercrime. Indeed, Article 22(2) provides that the Central Authority may request mutual legal assistance in "any criminal matter."

Of particular concern is that Article 24 authorizes proactive information disclosures without any consideration for the safeguards of sending or recipient states. This provision raises a particularly heightened threat to online anonymity to the degree it allows proactive disclosure of subscriber data.[63] There is also no requirement that proactively shared information be vetted by a recipient country's central authority in writing prior to being sent to law enforcement agencies.

Recommendations:

- Strike Article 16(2)(vii), which allows compelled decryption, undermining a necessary tool for the realization of the right to freedom of expression by journalists, human rights defenders, and the public at large.
- Provide for mandatory independent review of any preservation or production orders

[63] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, May 22, 2015, paras 47 et seq.

issued by law enforcement pursuant to Articles 19 and 20, and eliminate the automatic gag order for recipients as well as afford an opportunity to judicially challenge the validity of such an order.

- Define key terms such as what it means to “expeditiously” or “sufficiently” comply with orders, in order to provide legal certainty.
- Remove Part IV, which goes beyond the scope of a cybercrime bill, explicitly applies beyond the scope of the Bill, and seems more appropriately placed in separate mutual legal assistance or extradition legislation. At a minimum, require voluntary data sharing to be subject to safeguards under domestic law.

About ARTICLE 19

ARTICLE 19 is an international think–do organisation that propels the freedom of expression movement locally and globally to ensure all people realise the power of their voices.

Together with our partners, we develop cutting-edge research and legal and policy analysis to drive change worldwide, lead work on the frontlines of expression through our nine regional hubs across the globe, and propel change by sparking innovation in the global freedom of expression movement. We do this by working on five key themes: promoting media independence, increasing access to information, protecting journalists, expanding civic space, and placing human rights at the heart of developing digital spaces.

ARTICLE 19 advocates for the development of progressive standards on freedom of expression and freedom of information at the international and regional levels, and their implementation in domestic legal systems. We have produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, access to information and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the organisation publishes a number of legal analyses each year, comments on legislative proposals as well as existing laws that affect the right to freedom of expression. This analytical work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvements in proposed or existing domestic legislation. All of our analyses are available at http://www.article19.org/resources.php/legal.

If you would like to discuss this analysis further, or if you have a matter you would like to bring to the attention of the ARTICLE 19, you can contact us by e-mail at legal@article19.org. For more information about ARTICLE 19's work in The Gambia and West Africa, please contact us at:
E: senegal@article19.org; info@article19.org
W: www.article19ao.org; www.article19.org
Tw: @article19wafric; @article19org,
Fb: facebook.com/Article19wafric; facebook.com/article19org