ARTICLE 19

Senegal: Analysis of selected Internet regulation

March 2015

Legal analysis

Executive summary

In October 2014, ARTICLE 19 assessed the state of Internet freedoms in Senegal. In particular, we examined the compatibility of the Senegalese legal framework governing the Internet against international and comparative standards on the right to freedom of expression and freedom of information.

This analysis is published on March 2015 as a contribution to the current national debate on the reform of the legal framework on freedom of expression in the digital age.

In the analysis, ARTICLE 19 notes a number of positive aspects of the Senegalese legal framework pertaining to the Internet, in particular:

- Recognition of right to freedom of expression in relation to digital technologies in a number of laws and decrees,
- General lack of obligation for internet service providers to monitor the information they transmit or to search for illegal activities unless ordered to do so by judicial authorities,
- Positive proposals in the Draft Press Code including to abandon notice-and-take down provisions for Web-hosting providers and adopt a system requiring a judicial order.

However, there are a number of areas that fall significantly below the international standards and which could have a serious impact on freedom of expression in Senegal. Of particular concern is the Cybercrimes Law; which imposes a number of content limitations on freedom of expression that are vaguely worded and potentially very wide ranging. Similarly, the Decree on Encryption impose numerous requirements to seek permission from a commission before providing, importing, exporting and in some cases using encryption software. Additionally, the draft Press Code, whilst including a number of positive changes also tightens the definition of journalist would have the effect of excluding most bloggers and citizen journalists and continues to impose excessive liability for offences related to defamation, slander and insult.

Summary of recommendations

- Defamation should be fully decriminalised, including for online content. The provisions setting the penalties for insult, slander, defamation and similar offences should be removed.
- The definition of journalists (Article 168 of the Draft Press Code) should be modified to focus on the function of the individual and not an affiliating with a particular outlet;
- The notice-and-takedown system (Article 3 of the Law on Electronic Transactions) should be replaced with a system requiring a judicial order to remove content as suggested in Article 163 of the Draft Press Code;
- The notice-and-takedown system proposed in article 161 of the Draft Press Code for the liability of directors and co-directors of online press services should be replaced by a notice-to-notice system;
- Article 431-7 of the Cybercrime Law should be amended to include a broader category of grounds, including gender, age, political or other opinion, sexual orientation, gender identity or disability;
- The crime of incitement to violence, discrimination and hostility should require an intent;
- The word promote should be removed from the definition of racist and xenophobic material;

- Articles 431-60 and 431-61 should provide a definition of the term "secret information." In particular, it should distinguish between the various categories of classified information;
- Articles 431-60 and 431-61 should be re-drafted so that all offences require harm to national security or national defence.
- Articles 431-60 and 431-61 of the Cybercrimes Law should include an express public interest defence;
- Article 227 of the Draft Press Code permitting the authorities to suspend a press outlet for an attack on "good morals" should be removed;
- Article 159 para 5 of the Draft Press Code preventing editors of an online press service from publishing content susceptible to present violence in a favourable way should be removed;
- The limitation of free use of encryption software to those with keys of less than 128 bits in article 2 of the Decree on Encryption should be removed. The free use of encryption technology should be extended to all individuals not just those acting in a private capacity.

Table of contents

Introduction

In this legal analysis, ARTICLE 19 accesses the state of Internet freedom in Senegal. In particular, we examine the compatibility of the Senegalese legal framework governing the internet against international and comparative standards for the protection of freedom of expression and the right to information.

ARTICLE 19 has extensive experience of working on freedom of expression issues in Senegal, for example, we have previously analysed Senegalese legal provisions in this area including producing a memorandum on the Draft Press Code in 2010.[1] At the same time, we have analysed a number of laws pertaining to digital technology worldwide, including in Brazil, [2] Bolivia,[3] Venezuela,[4] Iran,[5] Pakistan[6] and Tunisia.[7] We believe, therefore, that we are particularly well-placed to assess the relevant laws governing freedom of expression on the Internet in Senegal.

Digital technology in Senegal is governed by a number of laws and decrees; these include but are not limited to:

- The provisions of the 2001 Constitution;
- The Law 96-04 of 2 February 1996 on the Organs of Social Communications, journalists and technician professions;
- The 1996 Press Code and the Draft Press Code of 2010;
- The Law 92-02 of 16 December 1991 on Creation the National Society of Radio and Television;
- The Law No. 2008-08 of 25 January 2008 on Electronic Transactions;
- The Law 2008-12 of 25 January 2008 on Protection of Reputation;
- The Law No 2008-41 of 20 August 2008 on Cryptology; and
- The Law No. 2008-11 of 25 January 2008 on Cyber-crime.[8]

For several years, there has been a movement to adopt an overarching press code that would include also the regulation of the content on the Internet. This has been a slow-moving process and the most recent draft of the Press Code was written in 2010, however discussion of the draft has continued particularly amongst civil-society. ARTICLE 19 hopes to contribute to this debate but also highlight other issue in relation to Senegalese laws and decrees in this area and ultimately to improve the protection of freedom of expression and information in relation to digital technology in the country.

---

[1] ARTICLE 19, Analysis of the Draft Press Code of Senegal, July 2010.
[2] ARTICLE 19, Draft Cybercrimes Law, February 2012.
[3] Bolivia: Law on Telecommunications and Information and Communication Technologies, February 2012
[4] Venezuela: Law on Social Responsibility of Radio, Television and Electronic Media, December 2011.
[5] ARTICLE 19, Computer Crimes Law of the Republic of Iran, December 2011.
[6] ARTICLE 19, Pakistan Telecommunications (Re-organisation) Act, 1996, January 2012.
[7] ARTICLE 19, Tunisia: Background paper on Internet Regulation, May 2013.
[8] The analysis is based on original French version of respective laws. The text of the laws is available upon the request at legal@article19.org.

International standards on freedom of expression

This section identifies international and regional standards for the protection of freedom of expression and information. These standards form the basis of our recommendations on how best to protect freedom of expression in relation to digital technologies on the Internet in Senegal, which are set out in the second section of this analysis.

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 bind states, including Senegal, in particular Article 19 of the Universal Declaration of Human Rights (UDHR)[9] and Article 19 of the International Covenant on Civil and Political Rights (ICCPR).[10]

In September 2011, the UN Human Rights Committee (HR Committee'), as treaty monitoring body for the ICCPR, issued General Comment No 34 in relation to Article 19.[11] General Comment No.34 constitutes an authoritative interpretation of the minimum standards guaranteed by Article 19 of ICCPR and is particularly instructive on a number of issues relative to freedom of expression on the Internet. Importantly, General Comment No 34 states that Article 19 ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and Internet-based modes of expression.[12] In other words, the protection of freedom of expression applies online in the same way as it applies offline.

At the same time, General Comment No 34 requires States party to the ICCPR 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.[13] In particular, the legal framework regulating the mass media should take into account the differences between the print and broadcast media and the Internet, while also noting the ways in which media converge.[14]

Similarly, the four special mandates on freedom of expression have highlighted in their 2011 Joint Declaration that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the Internet.[15] 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.[16] They

[9] UN General Assembly Resolution 217A(III), adopted 10 December 1948. The UDHR, as a UN General Assembly Resolution, is not directly binding on states. However, parts of it, including Article 19, are widely regarded as having acquired legal force as customary international law since its adoption in 1948
[10] GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc.
[11] UN Human Rights Committee General Comment No.34, CCPR/C/GC/43
[12] *Ibid*, para. 12
[13] *Ibid*., para. 17
[14] *Ibid*. para. 39.
[15] Joint Declaration on Freedom of Expression and the Internet, June 2011,
[16] *Ibid*.

also promote the use of self-regulation as an effective tool in redressing harmful speech.[17] As a state party to the ICCPR, Senegal must ensure that any of its laws attempting to regulate electronic and Internet-based modes of expression comply with Article 19 ICCPR as interpreted by the UN Human Rights Committee and that they are in line with the special mandates' recommendations.

Limitations on the right to freedom of expression

The right to freedom of expression is not guaranteed in absolute terms: Article 19(3) of the ICCPR permits the right to be restricted in the following respects:

> The exercise of the rights provided for in paragraph 2 of this Article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
> (a) For respect of the rights or reputations of others;
> (b) For the protection of national security or of public order, or of public health or morals.

Restrictions on the right to freedom of expression must be strictly and narrowly tailored and may not put in jeopardy the right itself. Determining whether a restriction is narrowly tailored is often articulated as a three-part test. Restrictions must:

- **Be provided by law**: Restrictions must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.[18] Ambiguous or overly broad restrictions on freedom of expression are impermissible under Article 19(3).

- **Pursue a legitimate aim**: as exhaustively enumerated in Article 19(3)(a) and (b) of the ICCPR. As such, it would be impermissible to prohibit information dissemination systems from publishing material solely on the basis that they cast a critical view of the government or the political social system espoused by the government.[19] Similarly, a restriction cannot be a pretext for protecting the government from embarrassment or exposure of wrongdoing, to conceal information about the functioning of its public institutions, or to entrench a particular ideology.

- **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 means that if a less intrusive measure is capable of achieving the same purpose as a more restrictive one, the least restrictive measure must be applied.

The same principles apply to electronic forms of communication or expression disseminated over the Internet.[20]

Additionally, Article 20 para 2 of the ICCPR places limitations on freedom of expression and requires states to prohibit certain forms of speech, namely "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence." Article 20

---

[17] *Ibid.*
[18] *Leonardus J.M. de Groot v. The Netherlands*, No. 578/1994, U.N. Doc. CCPR/C/54/D/578/1994 (1995).
[19] HR Committee Concluding observations on the Syrian Arab Republic, CCPR/CO/84/SYR,.
[20] General Comment 34, *op.cit*, para 43.

para 2 does not require states to prohibit all negative statements towards national groups, races and religions, but as soon as a statement advocates hatred in a way that it "constitutes incitement to discrimination, hostility or violence" it can be prohibited.

Online content regulation

With the exponential growth of digital technologies and increasing number of users, States have become increasingly uneasy about the availability of a wide variety of content, which they cannot control (e.g. sexually explicit content, content critical of the government or content unauthorised by intellectual property rights holders).

However, as the Special Rapporteur on freedom of expression rightly noted, these different types of content call for different legal and technological responses.[21] In his 2011 report, he 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.[22]

In particular, the Special Rapporteur clarified that the only exceptional types of expression that States are required to prohibit under international law are (a) child pornography; (b) direct and public incitement to commit genocide; (c) hate speech; and (d) incitement to terrorism.

He further made clear that even legislation criminalising 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.[23] In other words, these laws must also comply with the three-part test outlined above. For example, legislation prohibiting the dissemination of child pornography over the Internet through the use of blocking and filtering technologies is not immune from those requirements.

Similarly, hate speech laws targeting expression online must be unambiguous, pursue a legitimate purpose and respect the principles of necessity and proportionality. In this regard, the Special Rapporteur has highlighted his concern that a large number of domestic provisions seeking to outlaw hate speech are unduly vague, in breach of international standards for the protection of freedom of expression.

Finally, the Special Rapporteur has highlighted that all other types of expression, such as defamatory comments, should not be criminalised. Rather, States should promote the use of more speech to combat offensive speech.[24]

---

[21] The Report of the UN Special Rapporteur on Freedom of Expression, A/66/290, 10 August 2011, para. 18.
[22] Ibid.
[23] *Ibid*, para.22.
[24] UN Special Rapporteur on Freedom of Expression, A/HRC/17/27, 16 May 2011, para. 28.

The rights of citizen-journalists and bloggers

Digital technologies enable all individuals to self-publish their opinions and ideas on a blog or social media network. This raises the question of how "journalism" should be defined and what is 'media' in the digital age. Equally, the question arises whether and, if so, how 'citizen journalists' and 'bloggers' should be regulated.

Definition of journalism and new media

There is currently no set definition of journalism or what constitutes 'media' in the digital age on the international level. Nonetheless, the HR Committee and the Council of Europe have provided tentative responses. The General Comment No. 34 defined journalism as follows:

> Journalism is a function shared by a wide range of actors, including professional full-time reporters and analysts, as well as bloggers and others who engage in forms of self-publication in print, on the Internet or elsewhere, and general State systems of registration or licensing of journalists are incompatible with paragraph 3. Limited accreditation schemes are permissible only where necessary to provide journalists with privileged access to certain places and/or events. Such schemes should be applied in a manner that is non-discriminatory and compatible with Article 19 and other provisions of the Covenant, based on objective criteria and taking into account that journalism is a function shared by a wide range of actors.[25]

The HR Committee has thus taken a functional approach to the definition of journalism. In other words, journalism is an activity, which consists in the collection and dissemination of information to the public via any means of mass communication. The Committee of Ministers of the Council of Europe has taken a similar approach when it called the members states to:

- *Adopt a new, broad notion of media which encompasses all actors involved in the production and dissemination, to potentially large numbers of people, of content* (for example information, analysis, comment, opinion, education, culture, art and entertainment in text, audio, visual, audiovisual or other form) *and applications which are designed to facilitate interactive mass communication* (for example social networks) or other content-based large-scale interactive experiences (for example online games), *while retaining* (in all these cases) *editorial control or oversight of the contents;* [emphasis added]
- Review regulatory needs in respect of all actors delivering services or products in the media ecosystem so as to guarantee people's right to seek, receive and impart information… , *and to extend to those actors relevant safeguards against interference that might otherwise have an adverse effect on Article 10 rights, including as regards situations which risk leading to undue self-restraint or self-censorship;* [emphasis added.][26]

The Committee of Ministers further offered a number of criteria that should be taken into account when trying to determine whether a particular activity or actors should be considered as media, namely:

- intent to act as media;
- purpose and underlying objectives of media;
- editorial control;
- professional standards;

---

[25] General Comment No. 34, *op.cit.*, para 44.
[26] Recommendation CM/Rec (2011) 7 of the Committee of Ministers on a new notion of media, para. 7

- outreach and dissemination; and
- public expectation.

The Committee also provided a set of indicators in determining whether a particular criterion is fulfilled.

Regulation of bloggers and citizen journalists

Registration

The HR Committee's definition of journalism outlined above clearly shows that like professional journalists, bloggers should not be made subject to registration or licensing requirements. Similarly, they should be accredited only where necessary to get privileged access to certain places and/or events.

Limited editorial control

The Council of Europe recognised that different levels of editorial control call for different levels of editorial responsibility. In particular, it said that "Different levels of editorial control or editorial modalities (for example ex ante as compared with ex post moderation) call for differentiated responses and will almost certainly permit best to graduate the response."[27] This suggests that any legal framework affecting bloggers and citizen journalists should recognise that they have more limited duties and responsibilities when exercising their freedom of expression than professional journalists because they do not have the same resources and technical means as new

Civil and criminal liability

The law does not generally make any distinctions between journalists and the rest of the population for the purposes of civil or criminal liability. Accordingly, bloggers and citizen journalists are not immune to the application of such laws, e.g. defamation law. Nonetheless, the question arises whether bloggers and citizens should benefit from the same legal protections as journalists where they undertake the activity of journalism.

Legal protection

There are no set international legal standards concerning the legal protection to be afforded to citizen journalists and bloggers at present. However, in the same way that bloggers have a duty, like any other citizen, to obey the law, they can equally afford themselves of the defences available in the law.

The question whether bloggers and citizen journalists can avail themselves of legal principles governing the protection of sources is more controversial. As the Council of Europe said:

> [T]he protection of sources should extend to the identity of users who make content of public interest available on collective online shared spaces which are designed to facilitate interactive mass communication (or mass communication in aggregate); this includes content-sharing platforms and social networking services.[28]

However, it is not clear from the Recommendation whether a blogger or citizen journalist could avail himself or herself of the protection of sources in relation to information received from Internet users or others. Nonetheless, the Council of Europe has further recommended

[27] Recommendation CM/Rec (2011)7, *op.cit*, para.35.
[28] Ibid.

that some form of support and protection should be provided to media actors who do not fully qualify as media under a number of criteria, such as bloggers, but who at the same time 'participate in the media ecosystem'.[29]

Role of Internet intermediaries and intermediary liability

Intermediaries, such as ISPs, search engines, social media platforms and web hosts, play a crucial role in relation to access to the Internet and transmission of third party content.

Given the huge amount of information that is available on the Internet, and that could potentially be unlawful, e.g. copyright law, defamation laws, hate speech laws, criminal laws for the protection of children against child pornography, Internet intermediaries have had a strong interest in seeking immunity from liability on the Internet.

In several countries, intermediaries have been granted immunity for third-party content, whether as hosts, mere conduits, or for caching information.[30] They have also been exempted from monitoring content. [31] However, when acting as hosts, they have been made subject to 'notice and take-down' procedures, which require them to remove content once they are put on notice by private parties or law enforcement agencies that a particular content is unlawful. This system can be found for example in the E-commerce directive in the EU and the Digital Copyright Millennium Act 1998 (the so-called 'safe harbours') in the US.

A number of problems have been identified in relation to such 'notice and take-down' procedures. In particular, the Special Rapporteur on freedom of expression noted:

> [W]hile a notice-and-takedown system is one way to prevent intermediaries from actively engaging in or encouraging unlawful behaviour on their services, it is subject to abuse by both State and private actors. Users who are notified by the service provider that their content has been flagged as unlawful often have little recourse or few resources to challenge the takedown. **Moreover, given that intermediaries may still be held financially or in some cases criminally liable if they do not remove content upon receipt of notification by users regarding unlawful content, they are inclined to err on the side of safety by overcensoring potentially illegal content**. Lack of transparency in the intermediaries' decision-making process also often obscures discriminatory practices or political pressure affecting the companies' decisions. Furthermore, intermediaries, as private entities, are not best placed to make the determination of whether a particular content is illegal, which requires careful balancing of competing interests and consideration of defences. [Emphasis added][32]

---

[29] *Ibid*, para. 71

[30] See, e.g. the Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, the 'E-commerce directive' in the EU; or the US 1996 Communications Decency Act or The 2010 Singapore Electronic Transaction Act..

[31] See Article 15 of the E-commerce Directive. In *SABAM v. Scarlet Extended SA*, the CJEU considered that an injunction requiring an ISP to install a filtering system to make it absolutely impossible for its customers to send or receive files containing musical works using peer-to-peer software without the permission of the rights holders would oblige it to actively monitor all the data relating to each of its customers, which would be in breach of the right to privacy and the right to freedom to receive or impart information. The court noted that such an injunction could potentially undermine freedom of information since the suggested filtering system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications.

[32] The 2011 Report, *op.cit.*, para 42.

Accordingly, the four special mandates on freedom of expression recommended that:

> (i) No one should be liable for content produced by others when providing technical services, such as providing access, searching for, or transmission or caching of information;
> (ii) Liability should only be incurred if the intermediary has specifically intervened in the content, which is published online;
> (iii) ISPs and other intermediaries should only be required to take down content following a court order, contrary to the practice of notice and takedown.[33]

Assessing the restrictions of incitement to hatred

The HR Committee re-affirmed that there is a strong coherence between Articles 19 and 20 of the ICCPR when it stated that:

> 50. Articles 19 and 20 [of the ICCPR[are compatible with and complement each other. The acts that are addressed in Article 20 are all subject to restriction pursuant to Article 19, paragraph 3. As such, a limitation that is justified on the basis of Article 20 must also comply with Article 19, paragraph 3.45
>
> 51. What distinguishes the acts addressed in Article 20 from other acts that may be subject to restriction under Article 19, paragraph 3, is that for the acts addressed in Article 20, the Covenant indicates the specific response required from the State: their prohibition by law. It is only to this extent that Article 20 may be considered as *lex specialis* with regard to Article 19.
>
> 52. It is only with regard to the specific forms of expression indicated in Article 20 that States parties are obliged to have legal prohibitions. In every case in which the state restricts freedom of expression it is necessary to justify the prohibitions and their provisions in strict conformity with Article 19.[34]

ARTICLE 19 has developed a specific policy on prohibitions of incitement that elaborates on interpretation of Article 20(2) of the ICCPR in a greater detail;[35] in particular, we have recommended that:

- States should adopt uniform and clear definition of key terms of Article 20(2) of the ICCPR – "hatred," "discrimination," "violence," and "hostility"[36] and make sure that the interpretation is also consistent in jurisprudence by domestic courts;

---

[33] The 2011 Joint Declaration, *op.cit.*
[34] See, General Comment No. 34, *op.cit.*
[35] ARTICLE 19, Prohibiting incitement to discrimination, hostility or violence, 2012.
[36] ARTICLE 19 recommends that the definition of these terms should be as follows:
- Hatred is a state of mind characterised as "intense and irrational emotions of opprobrium, enmity and detestation towards the target group;
- Discrimination shall be understood as any distinction, exclusion, restriction or preference based on race, gender, ethnicity, religion or belief, disability, age, sexual orientation, language political or other opinion, national or social origin, nationality, property, birth or other status, colour which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life. This definition is adapted from those advanced by the Convention on the Elimination of All Forms of Discrimination against Women and the Convention on the Elimination of All Forms of Racial Discrimination.
- Violence shall be understood as the intentional use of physical force or power against another person, or against a group or community that either results in or has a high likelihood of resulting in injury, death, psychological

- Domestic legislation should includes specific and clear reference to "incitement to discrimination, hostility or violence" with references to Article 20(2) of the ICCPR and avoid broader or less specific language.

- The prohibition of incitement should conform to the three-part test of legality, proportionality and necessity under Article 19(3). This means that any prohibitions are provided for by law; pursue a legitimate aim; and be necessary in a democratic society, i.e. it must meet a pressing social need and meet the requirement of proportionality.

- Although Article 20(2) of the ICCPR only lists three characteristics which states are required to protect from incitement – nationality, race, and religion, the list should be read in light of Article 2(1) and Article 26 of the ICCPR and requires States to prohibit incitement also on the basis of "sexual orientation" and "gender identity" and disability. This interpretation would comply with evolution of the developments in protection of human rights since the adoption of the ICCPR in 1977.[37]

- The intent of the speaker to incite to hatred (that is to incite others to commit acts of discrimination, hostility or violence) should be considered a crucial and distinguishing element of incitement as prohibited by Article 20(2) of the ICCPR. Hence, ARTICLE 19 recommends that domestic legislation should always explicitly state that the crime of incitement to hatred is an intentional crime[38] and not a crime that can be committed through recklessness or negligence.[39]

Additionally, with a view to promoting a coherent international, regional, and national jurisprudence relating to the prohibition of incitement, ARTICLE 19 proposes that all incitement cases should be assessed under an uniform incitement test, consisting of a review of all the following elements:

- Context: of the expression in broader societal context of the speech.
- Intent: of the speaker to incite to discrimination, hostility or violence;
- Position and role of the speaker: in a position of authority and exercising that authority.
- Content: form and subject matter of expression, tone and style.
- Extent of the expression: public nature of the expression; the means of the dissemination;
- magnitude of the expression;
- Likelihood of imminent harm-: probability of discrimination, hostility or violence as a result of the expression.

---

harm, maldevelopment, or deprivation. The definition of violence is adapted from the definition of violence by the World Health Organisation in the report World Report on Violence and Health, 2002.

- Hostility shall be understood as a manifested action of an extreme state of mind. Although the term implies a state of mind, an action is required. Hence, hostility can be defined as the manifestation of hatred – that is the manifestation of "intense and irrational emotions of opprobrium enmity and detestation towards the target group." See ARTICLE 19, The Camden Principles on Freedom of Expression and Equality, 2009, Principle 12.1.

[37] The ICCPR was adopted before equality movements around the world made significant progress in promoting and securing human rights for all. However, it has since come to be interpreted and understood as supporting the principle of equality on a larger scale, applying to other grounds not expressly included in the treaty text, including sexual orientation, gender identity, and disability.

[38] In some jurisdictions, also acting "wilfully" or "purposefully".

[39] ARTICLE 19 notes that the legislation of many States already recognises intent or intention as one of the defining elements of incitement, for example, the UK, Ireland, Canada, Cyprus, Ireland, Malta, and Portugal.

Surveillance

Guaranteeing the right privacy in digital communications is essential for ensuring that individuals have the confidence to freely exercise their right to freedom of expression. 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 of private communications is strongly protected in international law, through Article 17 of the ICCPR, *inter alia*, state 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, the HR Committee clarified that the term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives the ICCPR. It also further stated that:

> 8. Even 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 authorized interference must be made only by the authority designated under the law, and on a case-by-case basis.

The Special Rapporteur human rights and countering terrorism has argued restrictions of the right to privacy should be interpreted as subject to the three-part test:

> [A]rticle 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]

He further defined the scope of legitimate restrictions on the right to privacy as follows:

> 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 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 there must be "on the basis of a warrant issued by a judge on 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 lack of ability of individuals to communicate privately substantially affects their freedom of expression rights. In 2011 report, the Special Rapporteur on freedom of expression expressed his concerns that:

> [T]he Internet also presents new tools and mechanisms through which both State and private actors can monitor and collect information about individuals' communications and activities on the Internet. Such practices can constitute a violation of the Internet users'

---

[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

[41] *Ibid.*, para. 21.

> right to privacy, and, by undermining people's confidence and security on the Internet, impede the free flow of information and ideas online.[42]
>
> [T]he right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of administration of criminal justice, prevention of crime or combating 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.[43]

The Special Rapporteur recommended that States should ensure that individuals can express themselves anonymously online and to refrain from adopting real-name registration systems.[44]

Cyber-security and human rights

International instruments and resolutions on cyber-security recognise the importance of balancing security imperatives with fundamental human rights, in particular the right to freedom of expression.

The Council of Europe Convention on Cybercrime (Cybercrime Convention) is the only binding international instrument in this area.[45] It is noteworthy in that it only provides for limited content-related offences, namely offences related to child pornography (Article 9) and offences related to copyright infringement (Article 10). Moreover, while law enforcement agencies are given broad investigative powers in relation to those crimes and other offences committed by means of a computer system, any such power and related procedures must conform to the requirements of the European Convention on Human Rights. Article 15 thus provides:

> 1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
> 2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
>
> 3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and

[42] The 2011 Report of the Special Rapporteur, *op.cit.*, para 52.
[43] *Ibid.*, para. 59.
[44] UN Special Rapporteur on Freedom of Expression Report of 10 August 2011, op.cit, para 84.
[45] The Council of Europe Convention on Cybercrime, CETS No. 185. It was adopted in 2001 and has been ratified by 42 countries, including the USA, Australia and Panama, and signed by another 11 countries.

> procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

In addition, the UN General Assembly Resolution on the "Creation of a global culture of cyber security"[46] states that "security should be implemented in a manner consistent with the values recognised by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency."

Access to digital technologies and network neutrality

Access to digital technologies

Digital technologies have become a basic requirement for the exercise of freedom of expression. It is also necessary for the meaningful exercise of other rights. States are therefore under a positive obligation to promote and facilitate access to digital technologies, including the Internet.

The Special Rapporteur on freedom of expression, thus recently stated:

> Given that the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States.[47]

Similarly, the four special mandates on freedom of expression have articulated a number of principles in relation to access to the Internet in their 2011 Joint Declaration on Freedom of Expression and the Internet. The declaration emphasises that states "are under a positive obligation to facilitate universal access to the internet."[48]

Network neutrality

The principle of net neutrality requires that all Internet traffic should be treated equally, i.e. without discrimination based on content, device, author, origin or destination of the content, service or application. The four special mandates adopted a set of principles in relation to network neutrality in their 2011 Joint Declaration. In particular, they declared the following:

> Network Neutrality
> a. There should be no discrimination in the treatment of Internet data and traffic, based on the device, content, author, origin and/or destination of the content, service or application.
>
> b. Internet intermediaries should be required to be transparent about any traffic or information management practices they employ, and relevant information on such practices should be made available in a form that is accessible to all stakeholders. [49]

---

[46] A/RES/57/239, 31 January 2003.
[47] Special Rapporteur on Freedom of Expression report of 10 August 2011, *op.cit*, para.85
[48] The 2011 Joint Declaration, *op.cit.*, para 6.
[49] *Ibid.*, para 5.

Digital freedoms in Senegal – analysis of selected laws

This section examines the current and proposed Senegalese provisions regulating aspects of freedom of expression and information in relation to digital technologies for compliance with the international standards set out above. It focuses on five major areas:

- Provisions protecting freedom of expression and information in relation to digital technologies;
- Proposed changes in Senegal to how digital media is regulated, with a focus on the draft Press Code;
- The regulation of bloggers and citizen journalists;
- Liability of ISP's, web-hosting providers and editors;
- Content restrictions and cyber-crimes; and
- Encryption.

The Constitution

The 2001 Constitution of Senegal[50] contains the following guarantees to the right of freedom of expression:

- Article 8 guarantees freedom of opinion, freedom of expression, press freedom, freedom of association, freedom to hold meetings, and the right to a plurality of information;
- Article 10 guarantees the right to freely express and disseminate opinions (subject to the honour and respect due to other persons and considerations of public order);
- Article 11 guarantees the free creation without prior authorisation of press bodies.

The Preamble of the Constitution does guarantee the right to seek, receive and impart information and the reference in Article 8 to the right to a verity of information. It is also enshrined in several of the international human rights instruments to which Senegal is a party.

Similarly, whilst the Constitution guarantees the freedom of opinion, it does not recognise the inviolability of this right, nor does it explicitly recognise that restrictions on freedom of expression must comply with the three-part test laid out in international law.

There is no reference in the Constitution to the right to freedom of expression and information using digital technology. Similarly the Constitution does not recognise the right to access to digital technologies.

Recommendations:

- The right to seek receive and impart information should be explicitly guaranteed by the Constitution and it should be recognised that the right can only be limited if, in compliance with a legitimate aim, disclosure threatens to cause substantial harm to that

[50] Constitution of the Republic of Senegal, 22 January 2001.

aim, the harm to the aim is greater than the public interest in having access to the information;
- The Constitution should recognise that the freedom to hold an opinion is guaranteed without any interference.
- The Constitution should recognise that the right to freedom of expression may only be subject to such restrictions as are provided by law and are strictly necessary and proportionate in a democratic society for the protection of national security, public order, public health or morals for the prevention of crime or for respect for the rights or reputations of others.
- Consideration should be given to specifying the right to freedom of expression through digital technologies and to including the right to access the Internet.

Other legal instruments

Several Senegalese laws and secondary regulation (decrees) covering the digital sphere recognise the right to freedom of expression. Moreover, such recognition is also included in several draft laws currently under consideration

Freedom of expression is guaranteed in:

- The Preamble of the Law on Organs of Social Communications, journalists and technician professions (LOSI) – which guarantees a "responsible" freedom of expression and creation of resources in all sectors of the information society;
- Article 5 of LOSI - which recognises that the principle of freedom aims to guarantee freedom of expression, namely the fundamental right of everyone to communicate and the right of every citizen to participate effectively in the information society and to participate in the creation and utilisation of online resources;
- The Preamble of the Draft Press Code - which states that the code aims to promote and guarantee freedom of expression and of opinion subject to respect for human dignity, the private life of citizens and the pluralistic expression of thoughts and opinions
- Article 3 of the LOSI - which recognises the right and freedom to create access utilize and share information and knowledge in accordance with the law
- Article 4 of the LOSI – which notes the right to access information is guaranteed by specific texts;
- The preamble of the Law on Electronic Transactions recognises the freedom of communication online.

Changes in how the digital media is regulated; the new Press Code

The current overarching press law (the LOSI), adopted in 1996, does not include references to digital media. Up till this point, therefore, the digital media has been governed by several different laws and decrees addressing distinct issues affecting the digital sphere (cyber-crime, electronic commerce etc).

For many years there has been a movement to update the overarching legislation governing the media in Senegal. One of the aims of this reform is to include digital media within the overarching framework. Therefore, the preamble of the Draft Press Code explicitly states that the code "includes, for the first time, online media," and Article 1 includes "online press" within the scope of application of the draft law.

Previous versions of the Draft Press Code have been analysed by ARTICLE 19. This analysis does not propose to repeat what has already been discussed in those comments. However this analysis will briefly mention some of the most important provisions which will affect both digital and non-digital media alike, as well as analysing sections of the Draft Code which deal with uniquely digital issues.

Aspects of the Draft Press Code effecting digital and non-digital media

ARTICLE 19 is concerned that the Draft Press Code imposes heavy fines for a number offences limiting certain types of speech which would have a serious chilling effect on freedom of expression, including online. The code proposes fines of between five hundred thousand and three million CFA for:

- Wilfully insulting the President (Article 254);
- Wilfully insulting foreign heads of state, government and ministers (Article 265);
- Contempt towards an ambassador, minister, envoy or similar (Article 266);
- Publishing, distributing, or reproducing "false news" (Article 255).

Similarly, the fines for defamation[51] range from five hundred thousand to two million CFA if directed at private individuals (Article 261) or from five hundred to four million CFA if directed against various official bodies including the army, the courts, the government (Articles 258-60).

ARTICLE 19 strongly believes these penalties constitute excessive sanctions which are contrary to several international instruments including Principle XII of the Principles of Freedom of Expression in Africa which states that sanctions should not be so severe as to inhibit freedom of expression.[52]

Recommendations:

- Defamation in Senegal should be decriminalised. The provisions setting the penalties for insult, slander, defamation and similar offences should be therefore removed.

Regulation of citizen journalists and bloggers

ARTICLE 19 is concerned by the restrictive definition of "journalism" in the legislation which excludes broad range of actors engaged in the function.

Restrictive definition of "journalism"

Under Article 23 of the LOSI, to be considered a journalist one must have either graduated from a journalism school and work in the domain of communication or work principally in an organ of social communication, journalism school or press service/ business.

The Draft Press Code severely tightens these requirements. According to Article 168, journalists must have either graduated from a journalism school and be actively involved in the distribution of information or to have a degree, three years of professional experience and be certified by a validation commission.

[51] Defined by Article 258 as any imputation or allegation of fact that damages the honour or respect of the person or of the body to which the fact is attributed.
[52] For further analysis of the problems posed by such provisions see the Memorandum, op.cit.

ARTICLE 19 notes that restrictions on who may enter the journalistic profession or be employed by the media sector have long been considered to breech the international guarantee of freedom of expression. Mandatory qualification requirements fail to recognize that the right to express oneself through the mass media belongs to everyone not only those who are considered particularly qualified or suitable.

With regards to digital media, the provision is likely to be particularly problematic as it will exclude the majority of bloggers and "citizen journalists." ARTICLE 19 strongly advocates the adoption of a "functional" definition of journalism in compliance with the recommendations of the HR Committee which defined journalism in its General Comment No 34 as

> A function shared by a wide range of actors, including professional full-time reporters and analysts, as well as bloggers and others who engage in forms of self-publication in print, on the Internet or elsewhere.[53]

Similarly, other bodies have instead been careful to formulate a very wide definition of 'journalist', covering anyone who serves as a conduit of information to the public, regardless of whether they would normally be perceived as journalists. The Recommendation adopted by the Council of Europe Committee of Ministers provides:

> The term "journalist" means any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication. [54]

Editorial control

ARTICLE 19 believes that bloggers and citizen journalists should not be made subject to the same laws of editorial control as journalists. It is well-established under international law that people exercising their freedom of expression have certain "duties and responsibilities." However, the scope of such duties and responsibilities must always take account of a person's situation, including their resources and the technical means available to them.[55] For example, it would be unfair to require someone who blogs in their spare time to meet the standards of fact-checking and editing that can be reasonably expected from a journalist working for a major media company.

For comparative purposes, we note that the Council of Europe has adopted a similar approach by calling on States to adopt differentiated responses to different level of editorial responsibility. Therefore, whilst ARTICLE 19 recommends a functional definition of journalist encompassing bloggers and citizen journalists, we consider that their duties and responsibilities should be limited to the duty of all citizens to respect and obey the law.

---

[53] General Comment No. 34, *op.cit.*, para 44.
[54] Recommendation No. R (2000)7 of the Committee of Ministers to Member States on the right of journalists not to disclose their sources of information, adopted 8 March 2000.
[55] See, for example, European Court of Human Rights, *Stoll v Switzerland*, [GC] no.69698/01, para.102, 10 December 2007

Specific regulation

ARTICLE 19 is not aware of any particular legal framework regulating citizen journalists and bloggers in Senegal, which is to be welcomed. We believe that bloggers should not be regulated apart of the same civil and criminal liability laws that apply to others.[56]

However, ARTICLE 19 is concerned by the provisions related to accreditation - the awarding of press cards to journalists - which constitutes a de facto registration system. Under Article 40 of the LOSI, journalists can apply for a press card. However only those in possession of such a card can benefit from the rights or advantages accorded to journalists by other articles of the law. This system is retained in the draft Press Code.[57]

ARTICLE 19 finds that this procedure amounts to an obligatory system of registration in order for an individual to exercise the job of journalist. As mentioned above, this is contrary to international norms which recognise that the right to express oneself through the mass media is universal and does not belong only to those considered qualified or appropriate. Cards for journalists should be treated as a matter of self-regulation for media agencies.

Recommendations;

- The legislation should recognise that the right to express oneself through mass media belongs to everyone and should define journalists broadly. The definition of journalists (Article 168 of the Draft Press Code) should be modified to focus on the function of the individual and not an affiliating with a particular outlet;
- Journalists, including bloggers and citizen journalists; should not be required to register or obtain a licence;
- The previsions in the Draft Code related to press cards should be removed.

Intermediary liability

Liability for content

ARTICLE 19 welcomes the move in the Draft Press Code to replace the current notice-and-take-down regime[58] for web hosting providers with a system requiring a court order to remove content.

Articles 3 paras 2 and 3 of the Law on Electronic Transactions set up a notice-and-takedown regime for web hosting providers. Web hosting providers are, therefore, not liable for illegal content provided that upon receiving notice of the existence of such content they act promptly to remove it or make it impossible to access. Article 3 para 4 sets out the conditions under which they are considered notified.

ARTICLE 19 has long argued that notice and take-down provisions breach freedom of expression as they do not provide procedural safeguards[59] and web hosting providers tend to err on the safe side and, therefore, remove material that was not in fact illegal. Thus, we

[56] General Comment No. 34, *op.cit*, para.32
[57] Article 187 of the draft Press Code.
[58] Notice and take-down procedures require intermediaries to remove content once they are put on notice by private parties or law enforcement agencies that a particular content is unlawful.
[59] For example the individual posting the content is often not informed or given a chance to respond to the allegation of illegality before the content is removed.

welcome the proposal in Article163 of the Draft Press Code which states that web hosting providers are not liable for illegal content unless they have been asked to remove it by the judicial authorities.

However, for the reasons mentioned above, ARTICLE 19 is concerned by the proposal in the Draft Code to set up a notice and take-down procedure for directors and co-directors of online publication. Article 161 states that directors and co-directors of online publication are not criminally liable for illegal content if they did not have effective knowledge its existence and acted promptly to remove the content upon receiving notice. ARTICLE 19 recognises that a system requiring judicial orders for removal of any content on all levels may be too burdensome and costly. However alternatives such as notice-to-notice systems can be implemented which provide a better protection for freedom of expression.[60]

Recommendations;

- Article 163 of the Draft Press Code which requires a judicial order before web hosting providers are required to remove or block access to material should be retained;
- The notice and takedown procedure in Article 161 of the Draft Code should be replaced with a notice-to-notice system.

Blocking and filtering

The regulations governing internet blocking and filtering are laid out in Article 3 of the Law on Electronic Transactions.

---

[60] See ARTICLE 19, Internet Intermediaries: Dilemma of Liability, 2013. Notice-to-notice allow aggrieved parties to send a notice of complaint to the host. In order to comply with international standards and best practice, notice-to-notice systems should meet the following conditions:

- The notice sent by an aggrieved party should include minimum requirements, including:
  - the name of the complainant;
  - the statement concerned with an explanation as to why it should be considered unlawful, including the provision of a legal basis for the claim;
  - the location of the material; and
  - an indication of the time and date when the alleged wrongdoing was committed. If the notice complies with these requirements, and upon payment of a fee, the host will then be required to forward the notice electronically as soon as is practicable (e.g. within 72 hours) to the person identified as the wrongdoer. They could be identified either directly by the complainant or via their IP address. The claimant will then be informed that the notice had been forwarded or, if not, why this was not possible.
- The alleged wrongdoer will then have a choice of either removing the content and informing the complainant (directly or via the host) or of filing a counter-notice within a sufficient time period (e.g. 14 days of receipt of the notice). The host will then forward the counter-notice within a set time (e.g. 72 hours) to the complainant, who will have another period of time (e.g. 14 days upon receipt of the counter-notice) to decide whether or not to take the matter to a court or other independent body with adjudicatory powers to determine the matter. Depending on the content at issue and the complexity of the complaint, consideration will be given to fast-track and low-cost procedures.
- If the alleged wrongdoer wishes to remain anonymous and refuses to give their contact details when filing the counter-notice, the complainant would have to seek a disclosure order from the court in order to bring the matter before the courts. This would at least stem the tide of abusive claims by adding the additional hurdle of convincing a court that disclosure was necessary. In this scenario, the only remedy available to claimants against online service providers would be statutory damages for failing to comply with their 'notice-to-notice' obligations.
- If the alleged wrongdoer fails to respond or file a counter-notice within the required time limit, the host will lose its immunity from liability. In other words, the host will have a choice. It can either take the material down or decide not to remove it, in which case it may be held liable for the content at issue if the complainant wishes to take the matter to a court or other independent adjudicatory body.

ARTICLE 19 welcomes the provisions laid out in Article 3 which broadly conforms to the international standards. Under Article 3 para 1, ISP's must inform their users the existence of any technical means permitting them to restrict access to, or select certain services. This is an important requirement as Internet users should be made aware of measures utilised by internet intermediaries which may restrict their access to information.

According to Article 3 para 5, ISPs and web hosting providers are not subject to a general obligation to monitor the information they transmit or to search for illegal activities unless ordered to do so by a court. This broad freedom is limited by Article 3 para 5 which requires ISP's and web hosting providers to "contribute" to the fight against the advocacy of crimes against humanity, the incitement of racial hatred and child pornography. In this capacity, ISP's and hosts are required to put in place mechanisms to enable individuals to report the content mentioned above. When informed of the existence of such content they must inform public authorities. They must also make public the methods they use to fight against these illegal activities. In ARTICLE 19's view these provisions comply with the current international standards.

However ARTICLE 19 is concerned by the broadening of these provisions by the 2008 Decree on Electronic Communications. The Decree requires that ISP inform the competent authorities of any "manifestly illicit content" and explicitly states that this is "in conformity with (the requirements under) article 3 (5) of the law.[61] However the definition of "manifestly illicit content" contained in the decree is far wider than the content included within the law. It therefore includes content where the "illegal character in indisputable, notably content of a pornographic character or…(content)…clearly attacking the public order or good morals."

Recommendations;

- Article 2 (2) of the Decree on Electronic Communications should be revised to include only the content referenced in Article 3 (5) of the Law on Electronic Transactions.

Content restrictions and cybercrimes

"Hate speech "

ARTICLE 19 is concerned by the definition of "racist and xenophobic material" laid out in the Cyber-crimes Law. Article 431-7 of the Cybercrimes Law, defines "racist or xenophobic material" for the purpose of the law as "all writing, images or other representations of ideas or theories that advocate or promote hatred, discrimination or violence against any individual or group of individuals based on race, colour, descent or national or ethnic origin as well as religion if used as a pretext for any of these factors."

ARTICLE 19 recognises that this language is directly taken from the Article 2 para 1 of the Council of Europe Additional Protocol to the Convention on Cybercrime. However, we believe that this wording fails to provide sufficient protection for freedom of expression in two ways.

- Firstly, as outlined in the section on international standards, ARTICLE 19 advocates for broader interpretation of grounds for prohibition of incitement, including grounds such as "sexual orientation" and "gender identity" and disability. This is in line with the

[61] Article 9 of the 2008 Decree on Electronic Communications.

Human Rights Committee's interpretation of the guarantees against discrimination contained in Article 2 (1) and Article 26 of the ICCPR.[62]

- Secondly, there is no requirement of intent. As noted above, ARTICLE 19 argues that incitement should always be an intentional crime to meet requirements of the ICCPR

- Thirdly, it is over-inclusive as the language could fall below the requirements laid out by international standards. The term "promotion," included in the Senegalese legislation is broader and thus contravenes international standards.

In addition, ARTICLE 19 notes that it is very important that the judiciary and law enforcement authorities are provided with comprehensive and regular trainings on incitement standards, including the interpretation of incitement as per ARTICLE 19's recommendations.

Recommendations;

- Article 431-7 of the Cybercrime Law should be amended to include a broader category of grounds, including gender, age, political or other opinion, sexual orientation, gender identity or disability;
- The crime of incitement to violence, discrimination and hostility should require an intent;
- The word promote should be removed from the definition of racist and xenophobic material.

Favourable presentation of violence

ARTICLE 19 is concerned by Article 159 of the Draft Press Code which states that content published by the editor of an online press service must not be susceptible to "present violence in a favourable way."

ARTICLE 19 notes that whilst it is legitimate to limit freedom of speech to protect public order, such limitations must still comply with the three part test set out in Article 19 para 3 of the ICCPR. In ARTICLE 19's view, this provision fails all three stages of that test. The phrase "presentation of violence in a favourable way" is vague and cannot be considered proscribed by law. The Article does not explicitly link the depiction of violence with an aim which may legitimately by used to limit freedom of expression (e.g. public order). Finally such a wide limitation cannot be seen as proportionate.

Furthermore, this paragraph generally seeks to impose additional limitations on editors with regards to the types of material they can publish. ARTICLE 19 believes there should not be specific laws limiting the freedom of an editor to publish material. Instead editors should be covered by general laws covering any individual publishing or producing material.

Recommendations:

- Article 159 (5) of the Draft Press Code should be abandoned.

---

[62] On sexual orientation see: HR Committee, *Toonen v Australia*, Com. No. 488/199, CCPR/C/50/D/488/1992; on disability see HR Committee, General Comment no. 25 of 1996 on the right to take part in the conduct of public affairs, the right to vote and to be elected, and the right to equal access to public services (Article 25) at para.10 and Concluding Observations on Ireland, 24 July 2000, A/55/40, paras 422-451, at para.29 (e).

National security

The provisions governing national security and online information are found in Articles 431-60 and 431-61 of the 2008 Cybercrimes Law. According to those Articles:

- Senegalese nationals who pass information, documents, data or similar which "should be kept secret in the interests of national defence" to a foreign power are culpable of treason and face a life sentence;
- Senegalese or foreign nationals who amass information with the intention to deliver it to a third state where the information is harmful to national defence can be sentenced to forced labour;
- All holders or depositaries, in title or in practice, of information objects or similar which should be kept secret in the interest of national defence are liable if they (without the intention to spy or commit treason) destroy, reproduce or give knowledge of this information to an unqualified person or the public and can face between 10-20 years in prison;
- If the holder or depositary acted in carelessness, negligence or disregard for regulations they face a reduced sentence of between 5 – 10 years.

ARTICLE 19 is concerned by three aspects of these provisions.

- Vague and overbroad provisions: Firstly, the prohibitions are extremely vague and there are no definitions of the information which "should be kept secret in the interests of national defence." ARTICLE 19 believes that Article 431-60 and 431-61 interfere with the freedom to obtain and exchange information that may be in the public interest. They must, therefore, comply with the three –part test under international law. In particular, they must be 'provided by law', i.e. they must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly. We note, however, that information which "should be kept secret in the interests of national defence" is not defined in the law itself or by explicit reference to other provisions. This term could cover a broad range of information including information with only a minimal impact on national defence. Furthermore, secret information is usually divided into categories of "top secret", "confidential", "restricted" etc. - depending on the information's perceived national security importance. However the law fails to take these distinctions into account.

- Lack of intent to harm requirement: ARTICLE 19 is concerned that some of the provisions do not require proof of harm as an element of the offence. In General Comment No. 34, the Human Rights Committee explicitly stated that:

> Extreme care must be taken by State parties to ensure that treason laws and similar provisions relating to national security, whether described as official secrets or sedition laws or otherwise, are crafted and applied in a manner that conforms to the strict requirements of paragraph 3. It is not compatible with paragraph 3, for instance, to invoke such laws to **suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists**, researchers, environmental activists, human rights defenders, or others, for having disseminated such information. [vi] [emphasis added]

  Whilst application of paragraph 1 of Article 431-61 is limited to information which is of a nature to harm national defence, the other offences set out in article 431-60 and paragraph 2 of 431-61 do not contain this requirement.

- Lack of public interest defence: ARTICLE 19 is concerned by the lack of public interest defence for the aforementioned Articles of the Cybercrimes Law. It is crucial that the public interest of all information, including that related to national security and national defence, be considered. As recognised in the Johannesburg Principle 15(2) legal defences must safeguard disclosures of information where the public interest of that act outweighs the potential harm caused to national security.

Recommendations:

- Articles 431-60 and 431-61 should provide a definition of the term "secret information." In particular, it should distinguish between the various categories of classified information.
- Articles 431-60 and 431-61 should be re-drafted so that all offences require harm to national security or national defence.
- Articles 431-60 and 431-61 of the Cybercrimes Law should include an express public interest defence.

Good morals

ARTICLE 19 is concerned by the limitations to freedom of expression and information in relation to digital technology in order to protect "good morals."

A number of the Senegalese legal provisions governing freedom of expression and information in relation to digital technology include such a provision; for example;

- Article 2 of the Decree on Electronic Communications: content considered as manifestly illegal includes content which clearly offends public morality;
- Article 431-59 the Law on Cybercrime: anyone who makes, imports, sells, distributes, etc all writings images, photos etc which are contrary to good morals can face imprisonment of between 6 months and 7 years and/or a fine of between five hundred thousand to ten million CFA;
- Article 13 of LOSI: individuals, when exercising their rights are required to respect good morals;
- Article 227 of the Draft Press Code: allows the administrative authority to suspend an organ of the press (including an online organ) if there is an attack on good moral standards (this decision must be confirmed within 24 hours by the President of the regional tribunal).

ARTICLE 19 notes that the protection of public morals constitutes a legitimate limitation to freedom of expression according to Article 19 para 3(b) of the ICCPR. However, such limitations must still comply with the three part test; in particular

- Restrictions must be accessible and foreseeable so that people know in advance what is prohibited and may regulate their conduct accordingly. The Senegalese laws and decrees refer to "good morals" but give no further guidance on its meaning. This is unacceptably vague and cannot be regarded as "prescribed by law."

- ARTICLE 19 notes that public or good moral standards must reflect the diversity of communities and interests – freedom of expression, therefore, extends to expression

which "offends shock or disturb the state or any other sectors of the population." [63] International and regional bodies have also stressed that "public morality" arguments are only acceptable when some real and specific harm to society can be shown. The Senegalese provisions do not recognise these concepts.

Furthermore, ARTICLE 19 is gravely concerned by Article 227 of the Draft Press Code which allows the authorities to suspend an organ of the press for an attack on good morals. In our view the suspension of a press organ because it attacks good moral standards cannot be necessary or proportionate given that there are other responses (such as removing the offending articles or information) available.

Recommendations;

- The reference to good moral standards should be revised to give clarity and enable individuals to guide their conduct.
- Provisions referencing good moral standards should recognise that public morals must reflect diversity of communities and interests and that limitations on the basis of public morality can only be used to prevent or put an end to a real and specific harm to society
- The references to good morals in Article 227 of the Draft Code should be removed.

Encryption

ARTICLE 19 is concerned by limitations to the utilisation and importation of encryption technology laid out in the Law on Encryption.

Encryption, which enables individuals to assure the privacy of communications, is essential to enable individuals to feel confident to express themselves freely. It also provides a vital protection for human rights actors, journalists, bloggers, whistleblowers and others and is an integral part of e-commerce. Encryption code itself has also been seen as a form of speech.[64]

The Special Rapporteur on freedom of expression has recognised the importance of encryption for freedom of expression noting that "individuals should be free to use whatever technologies they choose to secure their communications, and that states should not interfere with the use of encryption technologies, nor compel the provision of encryption keys." [65]

However, the Senegalese laws impose restrictions on encryption. Article 12 paragraph 1 of the Law on Encryption sets out the principle of free use of encryption. However paragraph 2 significantly limits this freedom by requiring the supply, import and export of all means of encryption except those aimed at authentification or control of data integrity to be declared to the National Commission of Cryptology.[66] The Commission is not independent but rather nine of the fourteen members are representatives of government ministries.[67] Breach of the requirements to declare or seek authorisation from the Commission can incur severe penalties. For example, importing or supplying means of encryption without a required

[63] European Court of Human Rights, Handyside v. the UK, App. No. 5493/72, 7 December 1976, para. 49.
[64] See, for example *Daniel J. Berntsein v United States department of State et al*, 192 F.3d 1308 (9th Cir. 1999)
[65] UN Special Rapporteur on Freedom of Expression, A/HRC/23/40, 17 April 2013, para.89.
66 Article 12 para 3 and article 14 of the Law on Encryption
67 Article 6 of the Law on Encryption

declaration can lead to penalties ranging from imprisonment from 6 months to 5 years or fines of between four hundred thousand to five million CFA.[68]

Article 2 para 4 of the 2012 Decree on Encryption allows free private use of encryption software for physical persons provided the key is less than or equal to 128 bits. No definition of "private use" is provided but it is unlikely that this would extend to journalists acting in their professional capacity. The use of larger keys is subject to authorisation by the Commission.[69]

These provisions constitute a threat to freedom of expression and privacy on the Internet and do not comply with the international standards in this area. It is not clear why the limitations on encryption are limited. We believe that restricting the use of encryption will allow for the routine surveillance of all internet users.

Recommendations:

- The limitation to encryption keys of less than or equal to 128 bits should be removed.
- The free use of encryption software should be extended to all individuals. If the law provides for the disclosure of encryption keys to police officers or other government agencies, such agencies are required to obtain a judicial warrant in order to obtain encryption keys to the extent that these requests fulfil the conditions of necessity and proportionality stated in Article 19 para of the ICCPR.
- The Commission should be reformed to ensure its independence.

Access to the Internet and net neutrality

ARTICLE 19 has already recommended that access to the Internet should be recognised as a right (see section on the Constitution above). In addition, the special mandates for the protection of freedom of expression have suggested policies to foster universal access to the Internet. We therefore encourage the Senegalese Government to pay close attention to these proposals, which are reproduced above.

ARTICLE 19 is not aware of any provisions recognising the principle of net neutrality in Senegal. ARTICLE 19 therefore strongly encourages the inclusion of this principle in the legislation.

68 Chapter VII – penal sanctions, Article 2 of the Law on Encryption,
[69] The 2012 Decree on Encryption, Article 4 para 3.

About ARTICLE 19

The 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. The Law Programme has 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 Law Programme, you can contact us by e-mail at legal@article19.org. For more information about the ARTICLE 19's work in Senegal, please contact Fatou Jagne Senghor, Director of ARTICLE 19 Senegal and West Africa, at fatouj@article19.org.

This analysis has been made possible by the support of Swedish International Development Cooperation, Sida. Sida does not necessarily share the opinions here within expressed. ARTICLE 19 bears the sole responsibility for the content of the analysis.