ARTICLE 19

Ethiopia: Proclamation on Telecom Fraud Offences

August 2012

Legal analysis

Executive summary

In this analysis, ARTICLE 19 finds the recently adopted Proclamation 761/2012 on Telecom Fraud Offences ("the Proclamation") to be fundamentally flawed from a freedom of expression and information perspective, and recommends its immediate repeal.

The Ethiopia House of Peoples' Representatives passed the Proclamation on 11 July 2012. It creates new offences related to the use and provision of telecommunications services, and increases sentences for a number of existing offences. It also extends the Anti-Terrorism Proclamation and the Criminal Code to electronic communications. The Proclamation will gain legal effect once published in the Federal Negarit Gazett.

ARTICLE 19 finds that the purposes of the Proclamation, to protect the state monopoly over telecommunications and safeguard national security, do not comply with international standards on the right to freedom of expression and information. In particular, the lack of a definition for "national security" gives the law uncertain scope and may encourage limitations on legitimate expression. The Proclamation is therefore likely to undermine rather than advance its stated aims of promoting "peace, democratisation and development" in Ethiopia.

The most concerning aspect of the Proclamation is the extension of the Anti-Terrorism Proclamation 2009 (already criticized by ARTICLE 19 in the past) and the Criminal Code of 2004 to electronic communications in Sec. 6. In particular, the Anti-Terrorism Proclamation has attracted broad condemnation from a number of international human rights bodies for violating the right to freedom of expression and information; its extension in the Proclamation shows a flagrant disregard for these rights. The Criminal Code of 2004 contains provisions that do not comply with international standards on the right to freedom of expression and information, including prohibitions on "obscene" communications, criminal defamation, and prohibitions on expression specifically engineered to protect public officials from criticism. The extension of these provisions to electronic communications is also a significant cause for concern.

It is also concerning that the Proclamation increases sentences for pre-existing telecommunication offences, including the prohibition on call back services and telephone or fax services over the Internet. Despite assurances given by the Ethiopian government to the contrary, ARTICLE 19 is unable to conclude that these provisions do not threaten to impose criminal liability for the provision or use of services such as Skype or Google-Talk. The lack of clarity over the scope of this prohibition is likely to have a significant chilling effect on the use of such technologies in the country, and thereby limit the free flow of information.

Further, the Proclamation imposes criminal penalties for individuals who fail to obtain a license for various commercial and non-commercial activities surrounding telecommunication usage. These provisions are ambiguous in scope and impose unnecessary obstacles for individuals to access information dissemination systems in Ethiopia.

Recommendations

- The Proclamation on Telecom Fraud Offences must be repealed in its entirety.
- The Ethiopian government must reform the telecommunications sector and prioritise promoting universal access to the Internet.
- The Anti-Terrorism Proclamation and the Criminal Code must not be extended to cover telecommunications, but must be amended to protect the right to freedom of expression.

Table of Contents

About the Article 19 Law Programme

The ARTICLE 19 Law Programme advocates for the development of progressive standards on freedom of expression and access to information at the international level, 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 Law Programme 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 online 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 work of ARTICLE 19 in Kenya, please contact Henry Maina, Director of ARTICLE 19 Kenya and East Africa at henry@article19.org

Introduction

Proclamation 761/2012 on Telecom Fraud Offences ("the Proclamation") was passed by the Ethiopian House of Peoples' Representatives on 11 July 2012;[1] and will gain legal effect when published in the Federal Negarit Gazzet.[2] The Proclamation creates new offences related to the use and provision of telecommunications services, and increases sentences for a number of existing offences. The Proclamation also extends aspects of the Anti-Terrorism Proclamation and the Criminal Code to electronic communications.

ARTICLE 19 has extensive experience of working on freedom of expression and information issues in Ethiopia. We recently condemned the application of the Anti-Terrorism Proclamation 2009 to imprison 6 prominent government critics to periods of imprisonment between 15 years and life, joining calls from numerous governments, international human rights bodies and other civil society organisations.[3] ARTICLE 19 has previously issued an analysis listing its concerns with the Anti-Terrorism Proclamation 2009 from a freedom of expression and information perspective, recommending reforms to bring the Proclamation into compliance with international human rights standards.[4] We have also issued analyses on laws pertaining to information communication technologies and freedom of expression in Iran, Iraq, and Brazil.[5]

In this analysis, ARTICLE 19 assesses the Proclamation for its compliance with international standards on the right to freedom of expression and information. It sets out international and regional standards on the right in the context of telecommunications regulation, and then analyses the Proclamation according to those standards. The analysis also gives context to these comments by explaining how the Proclamation fits into the existing legislative framework for telecommunications regulation in Ethiopia.

The Ethiopian government claims that the creation of new telecommunication offences is essential for the protection of national security "beyond the economic losses" telecom fraud causes the government, and for advancing "peace, democratisation and development" in the country. ARTICLE 19 finds the Proclamation to be irretrievably flawed from a freedom of expression and information perspective, and urges the Government of Ethiopia to repeal this law in its entirety and conduct a wholesale review of telecommunications regulation in the country.

---

[1] The analysis is based on the Draft Proclamation submitted to Parliament on 24 May 2012. The Standing Committee for Science, Communication and Technology annexed amendments to be made to the Proclamation in an agenda paper submitted to Parliament alongside the Proclamation for the 11 July 2012 vote. The amended version of the Proclamation will not be available until published in the Federal Negarit Gazett. The agenda paper is referenced where necessary to our analysis.

[2] Since 15 days have passed since the House of Peoples' Representatives vote, the Proclamation gains automatic Executive approval without requiring the signature of the Prime Minister; see: Constitution of the Federal Republic of Ethiopia (1995), Article 57.

[3] ARTICLE 19, "Ethiopia: Six journalists convicted for 'terrorism'", 13 July 2012; available at: http://www.article19.org/resources.php/resource/3372/en/ethiopia:-six-journalists-convicted-for-%E2%80%9Cterrorism%E2%80%9D

[4] ARTICLE 19, "Comment on the Anti-Terrorism Proclamation 2009", 30 March 2010; available at: http://www.article19.org/resources.php/resource/589/en/ethiopia:-comment-on-anti-terrorism-proclamation-2009

[5] All ARTICLE 19 legal analyses are available at: http://www.article19.org/resources.php/legal/

The most problematic features of this Proclamation include the extension of the Anti-Terrorism Proclamation 2009 and the Criminal Code of 2004 to electronic communications, including the Internet (Sec. 6).

The Anti-Terrorism Proclamation 2009 has been used extensively to imprison government critics on the pretence of protecting national security. This legislation adopts an overly ambiguous definition of "terrorist-acts" that encompasses a range of non-threatening expressive conduct, as well as offences related to the "encouraging" of such acts. The Criminal Code of 2004 contains provisions that do not comply with international standards on freedom of expression and information, including prohibitions on "obscene" communications, criminal defamation, including provisions engineered to protect public officials from criticism. The extension of these provisions to electronic forms of communications is a significant cause for concern. All of these offences are ambiguously defined and confer considerable discretion on law enforcement authorities to restrict criticism of the government.

A number of provisions in the Proclamation severely increase the sanctions available for existing telecommunication offences, including the prohibition on call back services and telephone or fax services over the Internet. In an agenda paper outlining amendments to the Draft Proclamation, to be incorporated when the Proclamation is published in the Federal Negarit Gazett, it is asserted that the 2002 prohibition on the private use of VoIP is to be voided, and that services such as Skype and Google-Talk are therefore legalised. However, this assurance is not reflected in the substance of Proclamation 761/2012. ARTICLE 19 is therefore unable to conclude that these provisions do not threaten to impose criminal liability for the provision or use of services such as Skype or Google-Talk. The lack of clarity over the scope of this prohibition is also likely to have a significant chilling effect on the use of such technologies in the country, and thereby limit the free flow of information.

Furthermore, the Proclamation imposes criminal penalties for individuals who fail to obtain a license for various commercial and non-commercial activities surrounding telecommunication usage. These provisions are ambiguous in scope and impose unnecessary obstacles for individuals to access information dissemination systems in Ethiopia.

ARTICLE 19 finds the Proclamation to be irretrievably flawed from a freedom of expression and information perspective. We therefore recommend that the Proclamation be repealed as part of a comprehensive reform agenda to restore the right to freedom of expression and information in Ethiopia.

International Standards on Freedom of Expression and Information

Rapid developments in information communication technologies (ICTs) in the past decade have transformed the media and significantly enhanced the way in which billions of people around the world seek, receive and impart information. More so than ever, the right to freedom of expression and information is fundamental to the promotion and protection of all human rights in a democratic society. International human rights law has clearly established that the right to freedom of expression and information applies on-line, and that any restrictions on the enjoyment of ICTs must comply with the same rules as restrictions on traditional media.

Universal Declaration of Human Rights

Article 19 of the Universal Declaration of Human Rights ("the UDHR")[6] recognises access to information as integral to the right to freedom of expression:

> Everyone has the right to freedom of opinion and expression; this right includes the right to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers.

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.[7]

International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights ("the ICCPR") elaborates upon and gives legal force to many of the rights articulated in the UDHR. The ICCPR binds its 167 states party to respect its provisions and implement its framework at the national level.[8] Ethiopia acceded to the ICCPR on 11 June 1993 and is therefore legally bound to respect and ensure the right to freedom of expression and information as contained in Article 19 of the ICCPR:

> 1. Everyone shall have the right to freedom of opinion
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media of his choice.

While the right to freedom of expression and information is a fundamental right, it is not guaranteed in absolute terms.

Article 19(3) of the ICCPR provides that the right carries with it "special duties and responsibilities", but that any restriction on the right must be "provided by law" and

---

[6] UN General Assembly Resolution 217A(III), adopted 10 December 1948.

[7] *Filartiga v. Pena-Irala*, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2nd circuit).

[8] Article 2 of the ICCPR, GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc. A/6316 (1966); 999 UNTS 171; 6 ILM 368 (1967).

"necessary" for (a) the respect of the rights or reputations of others, or (b) for the protection of national security or of public order, public health or morals. Restrictions 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. It is required that restrictions are i) provided by law, ii) pursue a legitimate aim; and iii) that they conform to the strict tests of necessity and proportionality.[9]

The HR Committee, the treaty monitoring body for the ICCPR, criticised the inappropriate application of counter-terrorism legislation to restrict the right to freedom of expression and information in its Concluding Observations to Ethiopia's initial report.[10] Following its Universal Periodic Review at the Human Rights Council on 9 December 2009,[11] Ethiopia agreed to take steps to uphold the right to freedom of expression and freedom from arbitrary arrest and detention, and to ensure that its counter-terrorism efforts comply with these rights. However, it refused to agree to a visit by thematic UN Special Rapporteurs on these issues, and refused to amend the Anti-Terrorism Proclamation to bring it into conformity with international human rights standards. The Proclamation at issue in this analysis extends the Anti-Terrorism Proclamation further.

African Charter on Human and Peoples' Rights

As a state party to the African Union, Ethiopia is bound by the freedom of information obligations imposed by the African Charter on Human and Peoples' Rights (the Charter),[12] and the Declaration of Principles on Freedom of Expression in Africa (the Declaration).[13] Article 9 of the Charter states:

1. Every individual shall have the right to receive information.
2. Every individual shall have the right to express and disseminate his opinions within the law.

The Declaration elaborates upon the right to freedom of expression and information. In its preamble the African Commission on Human and Peoples' Rights notes the "important contribution" that can be made to the realisation of the right to freedom of expression by new information and communication technologies.

Part XIII states that criminal restrictions on the right to freedom of expression must "serve a legitimate interest in a democratic society". Freedom of expression should not be restricted on public order or national security grounds unless there is a real risk of harm to a legitimate interest and there is a close causal link between the risk of harm and the expression".

At its 51st Ordinary Session, the Commission adopted Resolution 218 "on the human rights

---

[9] *Velichkin v. Belarus*, Communication No. 1022/2001, U.N. Doc. CCPR/C/85/D/1022/2001 (2005).

[10] The report is available at: http://www.ccprcentre.org/country/ethiopia/

[11] Human Rights Council, Thirteenth Session, Report of the Working Group on the Universal Periodic Review, Ethiopia, 4 January 2010, A/HRC/13/17; available at: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/101/47/PDF/G1010147.pdf?OpenElement

[12] African Commission on Human and Peoples' Rights, African [Banjul] Charter on Human and Peoples' Rights, adopted 27 June 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entered into force 21October 1986, available at http://www.achpr.org/english/_info/charter_en.html.

[13] African Commission on Human and Peoples' Rights, Declaration of Principles on Freedom of Expression in Africa, adopted by Resolution of the Commission at the 32nd Ordinary Session, 2002, available at http://www.achpr.org/sessions/32nd/resolutions/62/.

situation in the Democratic Republic of Ethiopia".[14] In the preamble to Resolution 218, the Commission notes that it is "gravely alarmed by the arrests and prosecutions of journalists and political opposition members, charged with terrorism and other offences including treason, for exercising their peaceful and legitimate rights to freedom of expression and freedom of association." Resolution 218 calls upon the government of Ethiopia to remove restrictions on freedom of expression imposed through a number of laws, including the Anti-terrorism Proclamation (2009).

The Internet and the right to freedom of expression and information

In recent years numerous international human rights bodies have recognised the principle that freedom of expression must be promoted and protected in the digital sphere no less than in the public sphere. Technological developments in recent years have led to the recognition of access to the Internet and other forms of electronic communication as integral to the right to freedom of expression.

On 29 June 2012, the HRC adopted by consensus a landmark Resolution "on the promotion, protection and enjoyment of human rights on the Internet", affirming the importance of the Internet for securing the right to freedom of expression and information.[15] The Resolution reflects the Joint Declaration made by the four Special Mandates on freedom of expression and information in June 2011,[16] and the report of UN Special Rapporteur for freedom of opinion and expression presented at the 17th Session of the HRC the previous month.[17] In General Comment No. 34, also issued in June 2011, the HR Committee stressed that Article 19 of the ICCPR protects all forms of expression *and their means of dissemination*, including all forms of electronic and Internet-based modes of expression.[18]

Together, these resolutions, declarations and comments have established the following principles in relation to freedom of expression and information online:

- Enjoyment of the right to freedom of expression and information on-line is essential to the attainment of other human rights, including the right to political participation, the right to health care, and the right to education among others.[19]
- The global and open nature of the Internet is a driving force for accelerating progress towards development.[20]

---

[14] Resolution on the human rights situation in the Democratic Republic of Ethiopia, ACHPR/Res 218, 2012; available at: http://www.achpr.org/sessions/51st/resolutions/218/

[15] A/HRC/20/L.13, 29 June 2012; available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx

[16] Joint Declaration on Freedom of Expression and the Internet, 1 June 2011; available at: http://www.article19.org/data/files/pdfs/press/international-mechanisms-for-promoting-freedom-of-expression.pdf

[17] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27, 16 May 2011; available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[18] HR Committee, General Comment No. 34, 21 June 2011, CCPR/C/GC/34; available at: http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

[19] See: the Joint Declaration 2011, at Paragraph 6.a;

[20] See: the HRC Resolution, at Paragraph 2, and the London Declaration for Transparency, the Free Flow of Information and Development, 25 August 2010; available at:

- States are under an obligation to take into account the extent to which developments in information technology have substantially changed communication practices around the world.[21]

- States are under an obligation to take necessary steps to promote and facilitate universal access to the Internet and other forms of new media, both domestically and through international cooperation.[22]

- Any restriction on the right to freedom of expression and information or the use of information dissemination systems must comply with Article 19 (3) of the ICCPR.[23]

- Generic bans on access to the Internet, or use of particular systems, and blanket prohibitions on certain forms of content, are never proportionate. Any imposition of criminal penalties for offences must take into account the overall public interest in protecting online forms of expression.[24]

- Intermediaries who provide technical Internet services should not be liable for content generated by others which is disseminated using those services.[25]

Telecommunications and the protection of national security

In General Comment No. 34, the HR Committee caution that extreme care must be taken in crafting and applying laws that purport to restrict expression to protect national security. Whether characterised as treason laws, official secrets laws or sedition laws they must conform to the strict requirements of Article 19 (3) of the ICCPR.

In their Joint Declaration of 2011, the four Special Mandates noted that even when done in good faith, efforts by governments to regulate for cyber security too often fail to take into account the special characteristics of the Internet and consequently restrict freedom of expression online unduly. The UN General Assembly Resolution on the "Creation of a global culture of cyber security" 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."[26]

---

http://www.article19.org/data/files/medialibrary/1798/London-Declaration.pdf

[21] See: General Comment No. 34, at Paragraph 15;

[22] See: the HRC Resolution, at Paragraph 3; the Joint Declaration 2011 at Paragraph 6.a and 6.e; General Comment No.34, at Paragraph 15; and the African Platform on Access to Information, adopted by the Pan African Conference on Access to Information, September 2011; available at: http://www.article19.org/resources.php/resource/2740/en/pan-africa:-landmark-regional-declaration-paves-way-for-access-to-information.

[23] See: General Comment No.34, at Paragraph 43;

[24] See: the Joint Declaration 2011, at Paragraph 3.a and 6.d; General Comment No.34, at Paragraph 43.

[25] See: the Joint Declaration, at Paragraph 2.

[26] See A/RES/57/239, Jan. 31, 2003; available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.

The Johannesburg Principles on National Security, Freedom of Expression and Access to Information[27] ("the Johannesburg Principles") make clear at Principle 2 that restrictions sought to be justified on the ground of national security are illegitimate unless their genuine purpose and demonstrable effect is to protect the country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force. The 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.

From a comparative perspective, the preamble to the Council of Europe Convention on Cybercrime (2001) states that parties must be

> [M]indful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights ... which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy.[28]

This is supported by Article 15 of the Convention, which states that the powers and procedures provided for within the Convention "shall provide for the adequate protection of human rights and liberties", including references to the ICCPR. Article 27(4)(a) of the Convention allows states to refuse assistance to other state parties where they believe the request for assistance relates to a "political offence".

Telecommunications and network neutrality

The principle of "net neutrality" protects the consumers' right to access the content, applications, services and hardware of their choice. It requires that any party with control over the Internet infrastructure should not exploit that control to block content, or prioritise or slow down access to certain applications or services, such as Voice Over Internet Protocol (VOIP). Underpinning net neutrality are the principles that: (i) network-managing practices must be transparent; (ii) parties with control over the Internet infrastructure must not block lawful sites and services; and (iii) fixed broadband providers cannot unreasonably discriminate against lawful network traffic.

Net neutrality is increasingly being recognised as an essential condition for safeguarding the right of all people to access the Internet, and for securing human rights on-line. In their 2011 Joint Declaration, the four Special Mandates stated that 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.[29]

From a comparative perspective, the Committee of Ministers for the Council of Europe adopted a Declaration on net neutrality on 29 September 2010.[30] At paragraph 4 it provides:

---

[27] Adopted on 1 October 1995. These Principles have been endorsed by the UN Special Rapporteur on Freedom of Opinion and Expression and have been referred to by the United Nations Commission on Human Rights in each of their annual resolutions on freedom of expression since 1996.

[28] Convention on Cybercrime, Budapest, 23.XI.2001; available at http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.

[29] See the Joint Declaration, at Paragraph 5.

[30] Declaration of the Committee of Ministers on network neutrality, Adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies; available at:

> Users should have the greatest possible access to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice. Such a general principle, commonly referred to as network neutrality, should apply irrespective of the infrastructure or the network used for Internet connectivity. Access to infrastructure is a prerequisite for the realisation of this objective.

From a comparative perspective, both the European Union[31] and the Netherlands[32] have legislated on the issue of network neutrality to safeguard the right to freedom of expression and information online.

Telecommunications and the protection of surveillance and privacy

Guaranteeing the right to privacy in online 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.

From a comparative perspective, the European Union has grappled with the issue of protecting the privacy of communications online in its E-Privacy Directive.[33] Article 15 of this Directive provides that any infringement of privacy rights must be "necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC [Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data]."

In the Resolution on Surveillance of Communications and Freedom of Expression (5 June 2009) a coalition of international freedom of expression organisations stated that there is no pressing need in a democratic society for telecommunication providers to routinely collect information regarding their customers' activities. Governments should therefore not require that persons to pre-register or identify themselves to use telecommunications networks.[34]

---

https://wcd.coe.int/ViewDoc.jsp?id=1678287&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

[31] See Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, Article 1, Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[32] "Netherlands first country in Europe with Net Neutrality", Bits of Freedom, 8 May 2012; available at: https://www.bof.nl/2012/05/08/netherlands-first-country-in-europe-with-net-neutrality/

[33] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT

[34] Available at: http://www.ifex.org/international/2009/06/05/ja_gm/

Analysis of the Telecom Fraud Offences Proclamation

This section provides a brief background to the Proclamation, including the legislative process leading to the adoption of the Proclamation and the relationship between the Proclamation and existing domestic laws. The purposes for the Proclamation are then reviewed, followed by an assessment of the substantive provisions of the Proclamation for their compliance with international standards on the right to freedom of expression and information.

The legislative process

The Proclamation was approved by vote of the House of People's Representatives on 11 July 2012.[35]

A Draft Proclamation was submitted to the House of Peoples' Representatives on 24 May 2012. The Science, Communication and Technology Standing Committee considered amendments to the Draft Proclamation and raised a number of concerns, mostly relating to implementation but also on the issue of prohibitions on VoIP services such as Skype of Google-talk. These concerns were raised in an agenda paper submitted to the House of Peoples' Representatives, alongside a series of amendments to the text that would be incorporated to the Proclamation following an affirmative vote. The interpretation given to the Proclamation in the agenda paper has legal effect, in addition to the textual amendments that affect the substance of the law. The final version of the Proclamation is not available until it is officially published.

The Proclamation contains 18 sections divided between three parts: 'general', 'telecom fraud offences', and 'miscellaneous provisions'. An additional section to the Proclamation, added through the agenda paper, requires the Council of Ministers to issue a regulation for the implementation of the Proclamation. It is unclear whether these regulations are required or not before the Proclamation can be enforced, or when these regulations will be issued.

Relationship to existing law

The Constitution of the Federal Democratic Republic of Ethiopia ("the Constitution")[36] is the supreme law of Ethiopia and incorporates international legal instruments ratified by Ethiopia (Article 9). The right to freedom of expression is protected at Article 29 (2) – (6), and the Proclamation must therefore be interpreted in light of this guarantee.

[35] It should be borne in mind that 99.6% of seats in the House of Peoples' Representatives are held by ruling Ethiopian People's Revolutionary Democratic Front.

[36] Constitution of the Federal Democratic Republic of Ethiopia, 21 August 1995; available at: http://www.unhcr.org/refworld/docid/3ae6b5a84.html

Telecommunications regulation in Ethiopia is governed by the Telecommunications Proclamation No. 49/1996 ("the Telecommunication Proclamation 1996"), which was substantially amended by the Telecommunications Amendment Proclamation No.281/2002 ("the Telecommunication Amendment Proclamation 2002"). However, the Proclamation directs that no law, regulations, directives or practices that are inconsistent with this Proclamation will continue to have legal effect with respect to matters regulated by the Proclamation (Sec. 17.2).

A number of criminal offences related to the use and provision of telecommunication services precede the Proclamation. Sec. 24 of the Telecommunications Proclamation 1996 (as amended in 2002) criminalises the following conduct: (i) the use or provision of call back services;[37] (ii) the use or provision of voice communication or fax services through the Internet; and (iii) using the telecommunication service provider network, or bypassing the same to engage in private or commercial Telecommunication Services without a license. However, the sentencing provisions for these offences are repealed by the Proclamation in Sec. 17.1.[38] The Proclamation re-articulates these offences and provides heightened sanctions for their violation, in addition to creating a number of new telecommunication offences – including the extension of the Anti-Terrorism Proclamation (2009) and the Criminal Code (2004) to electronic communications.

The regulatory body for telecommunications in Ethiopia is the Ethiopian Telecommunications Agency ("the ETA") – which was established pursuant to Proclamation No. 49/1996 ("the Telecommunication Proclamation") with the objective of promoting the development of high quality, efficient, reliable and affordable Telecommunication Services in the country.[39] The ETA is not independent, as it is largely controlled by and is accountable to the Ministry of Transport and Communication. The Proclamation does not amend this regulatory framework.

The Ethiopian Telecommunications Corporation ("the ETC") was established by the Council of Ministers Regulations No. 10/1996. In the Telecommunications Amendment Proclamation No. 281/2002, the ETC is referred to as the "sole telecommunications service provider".[40] Since its establishment, the ETC, now known as Ethio Telecom,[41] has exercised a complete monopoly over telecommunications services in Ethiopia and remains entirely government

[37] "Call back services" are defined in the Proclamation as "the use of dial tone of a foreign telecommunication operator for international connections without the knowledge of the domestic telecommunication operator".

[38] The repealed provisions are Sec. 25 (1), (2), and (3) of the Telecommunication Proclamation 1996 (as amended in 2002). The offences that these sentences relate to are contained The offences themselves, to the extent that they are not inconsistent with the Proclamation, remain unchanged in Sec. 24 of the Telecommunication Proclamation 1996.

[39] Telecommunications Proclamation No. 49/1996, 28 November 1996; available at: http://www.eta.gov.et/Scan/Telecom%20Proc%2049_1996%20NG1.pdf

[40] Telecommunications (Amendment) Proclamation No. 281/2002, 2 July 2002; available at: http://www.eta.gov.et/Scan/Telecom%20Proc%20281_2002%20(amendment)%20NG.pdf

[41] In December 2010, as part of the Ministry of Finance and Economic Development's five year "Growth and Transformation Plan" (GTP), France Telecom, mostly known for its international brand, "Orange", took over management of the ETC as part of a two year €30 million contract. The change in management was marked by the rebranding of the ETC as "Ethio Telecom", although the entity remains an entirely state owned corporation with a monopoly over all telecommunication services. The five-year plan does not indicate any intention to liberalise government control over the telecommunications infrastructure or service delivery. Ethio Telecom's monopoly therefore looks likely to endure. The GTP also indicates that government control over information flows will be maintained if not tightened – one of its "key targets" is "to prevent and fully control illegal activities and thereby ensure the security of the ICT system."

owned. While no other telecommunications service provider has been awarded a license under the Telecommunications Proclamation, in recent years there has been an increase in small-scale private contracting and limited private resale of services. Protecting the telecommunications monopoly from economic losses is listed among the purposes of the Proclamation.

Purposes

The Proclamation identifies "telecom fraud offences" as a "serious threat to national security beyond economic losses", and asserts that existing laws are not adequate to combat these threats. Telecom fraud is further blamed with "encumbering" the telecommunications industry to play an "essential" role in the implementation of peace, democratisation and development programs.

ARTICLE 19 believes that the creation of new telecommunications offence that restrict the right to freedom of expression and information without good cause will not advance "peace, democratisation and development" in Ethiopia but will directly undermine these causes. We recall that the Human Rights Council, the Joint Declaration by the four Special Mandates on Freedom of Expression, and the London Declaration each recognise that the global and open nature of the Internet is a driving force for accelerating progress towards development. Further restricting enjoyment of electronic communications goes directly against the international movement towards recognising the importance of online freedoms.

Protecting the state's telecommunications monopoly from "economic losses" is not a legitimate basis for restricting the right to freedom of expression and information under either Article 19 of the ICCPR or Article 9 of the ACHPR. No legitimate basis or clear need has been given by the Ethiopian government to justify this legislation. No evidence has been advanced to demonstrate that "telecom fraud" is obstructing the development of the telecommunications sector, particularly given the country's poor Internet and telephone penetration levels. The Ethiopian government itself notes that only 62.14% of the population are within a 5km distance of the nearest telephone connection. The International Telecommunication Union ("the ITU") estimate that only 1.1% of the Ethiopian population are Internet users.[42] The ITU further link these low penetration levels and relatively high prices for mobile telephone services are the consequence of a lack of competition and a failure to liberalise the telecommunications sector.[43] The case for liberalisation therefore appears more compelling than the case for promulgating new criminal offences for telecommunication use.

Moreover, restrictions on the right to freedom of expression and information cannot be based on an over-broad understanding of "national security." The genuine purpose and demonstrable effect of such restrictions must be to protect the country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force. The lack of a definition for "national security" in the Proclamation is particularly concerning, as it confers too much discretion on law enforcement authorities to suppress legitimate forms of expression. Principle 7 of the Johannesburg Principles provides

[42] International Telecommunication Union, information and communication technology statistics for 2011; available at: http://www.itu.int/ITU-D/ict/

[43] *Ibid*, FN30.

specific guidance on the forms of expression that should be protected by measures designed to safeguard national security.

ARTICLE 19 is further concerned that the protection of national security is present as connected to, if not reinforcing, the need to protect the state monopoly over telecommunications. This understanding of national security finds no support in international human rights law, and indicates that the government intends to use the protection of "national security" as a pretext for stifling legitimate forms of expression.

The Proclamation is therefore fundamentally flawed at its inception, and further endangers the right to freedom of expression and information in the country. ARTICLE 19 urges the Ethiopian Government to repeal this law immediately. This should be accompanied with a programme of reform towards ensuring universal access to the Internet, and the enjoyment of such technologies in line with international standards on the right to freedom of expression and information.

Recommendations:

- The Ethiopian Government must repeal the Proclamation.
- Parliament must urge the government to focus on securing universal access to the Internet and other forms of electronic communication, and insist that the right to freedom of expression and information is protected in this process.

Extension of the Anti-Terrorism Proclamation and the Criminal Code

ARTICLE 19 is very concerned at the creation of two new offences in Sec. 6 of the Proclamation that significantly expand the scope of the Anti-Terrorism Proclamation and the Criminal Code to cover electronic communications.

Sec. 6(1) criminalises the use or causing the use "of any telecommunications network or apparatus to disseminate any terrorizing message connected with a crime punishable under the Anti-terrorism Proclamation No. 652/2009 or obscene message punishable under the Criminal Code". The provision allows for the imposition of imprisonment between 3 to 8 years and fines from Birr 30,000 to Birr 80,000.

ARTICLE 19 issued a comprehensive analysis of the Anti-Terrorism Proclamation in March 2010, finding it to be a serious threat to the right to freedom of expression and information in Ethiopia.[44] The analysis recommended that the definition of "terrorist acts" be narrowed. Sec. 3 of the Proclamation defines "terrorist acts" as the intention to "advance a political, religious or ideological cause by coercing the government, intimidating the public or section of the public, or destabilising or destroying the fundamental political, constitutional or, economic or social institutions of the country." Any "serious interference or disruption of any public service" is also defined as a "terrorist act". This ambiguous provision grants the government ample discretion with which to target legitimate forms of expression that poses no threat to national security. The analysis also recommended that specific provisions should ensure the protection of journalists and their sources, and vague prohibitions on the "encouragement of terrorism" should be replaced with narrower prohibitions on incitement. The Anti-Terrorism Proclamation 2009 has been criticised by the UN High Commissioner for

[44] The full analysis if available at: http://www.article19.org/resources.php/resource/589/en/ethiopia:-comment-on-anti-terrorism-proclamation-2009

Human Rights,[45] the HR Committee,[46] and the African Commission[47] for its failure to comply with international standards on the right to freedom of expression and information.

ARTICLE 19 is extremely concerned that Sec. 6(1) of the Proclamation will not only extend the reach of the Anti-Terrorism Proclamation 2009 to electronic communications, but will broaden the offences contained therein significantly. The text of Sec. 6(1) prohibits "terrorizing messages" "connected with a crime punishable under the Anti-terrorism Proclamation". "Terrorizing messages" is not defined, but it seems that the mere association of an electronic message to the broad range of activities prohibited in the Anti-terrorism Proclamation would be sufficient to incur criminal liability under this provision.

W recall that the Criminal Code (Proclamation No. 414 of 2004) contains numerous illegitimate restrictions on the right to freedom of expression and information. At Section IV, the Criminal Code lists "crimes tending to corrupt morals".[48] Sec. 6(1) of the Proclamation explicitly extends these prohibitions into the electronic sphere. The offences include: Article 639 "public indecency and outrages against morals"; Article 640 "obscene or indecent publications"; Article 641, "obscene or indecent performances", and Article 643 "indecent publicity and advertisements". Article 642 does not define obscenity or indecency directly, but provides that "objects purely artistic, literary or scientific in character" are not obscene or indecent if they are not "calculated to inflame exotic feelings or lust."

The extension of illegitimate restrictions on the right to freedom of expression to electronic communications demonstrates Ethiopia's lack of regard for Article 19 (3) of the ICCPR or Part II of the African Declaration.

Firstly, the prohibitions are not 'provided by law'; the terms "terrorism acts" and "obscene" lack the precision required for an individual to regulate his or her conduct or to constrain the discretion of law enforcement. Secondly, the restrictions are not narrowly tailored to protect 'national security' or 'public morals' as understood in international law. The offences in the Anti-Terrorism Proclamation are not necessary to protect the country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force. In relation to public morals, it is recalled that the right to freedom of expression encompasses expression considered deeply offensive,[49] and it must be appreciated that the concept of morals "derives from many social, philosophical and religious traditions; consequently, limitations... for the purposes of protecting morals must be based on principles not deriving exclusively from one tradition." With these considerations, the sentences imposed cannot be considered proportionate.

Sec. 6(2) of the Proclamation is broader still, prohibiting using or causing to be used "the telecommunication service or infrastructure provided by the telecommunication service provider for any other illegal purpose". It is not clear what purpose such a blanket extension

---

[45] See: http://www.un.org/apps/news/story.asp?NewsID=42498&Cr=Ethiopia&Cr1=

[46] HR Committee, Concluding Observation on Ethiopia, CCPR/C/ETH/CO/1, 25 July 2011, At Paragraph 15.

[47] Resolution on the human rights situation in the Democratic Republic of Ethiopia, ACHPR/Res 218, 2012; available at: http://www.achpr.org/sessions/51st/resolutions/218/

[48] Criminal Code of the Federal Democratic Republic of Ethiopia, Proclamation No. 414 of 2004, available at: http://www.unhcr.org/refworld/docid/49216b572.html

[49] See communication No. 736/97, Ross v. Canada, Views adopted on 18 October 2000.

of Ethiopian criminal law serves, as its breadth essentially renders Sec. 6(1) redundant. The Criminal Code contains offences for various forms of defamation (Sec. 613, 615) including heightened protections for public officials (Sec. 618). There are also provisions protecting the state and other national symbols from insult (Sec. 244, 264, 265, 266) and broad restrictions on the protection of state secrets (Sec. 248, 249, 250, 396, 397, 399). It is beyond the scope of this analysis to engage in a detailed assessment of these provisions, other than to state that their extension through Sec. 6(2) of the Proclamation is a deeply concerning development that poses a serious threat to freedom of expression in Ethiopia.

Recommendations:

- The Anti-Terrorism Proclamation and the Criminal Code must be substantially amended to comply with international standards on the right to freedom of expression and information.

Increased penalties for the provision and use of call back services

It is recalled that Sec. 24 of the Telecommunications Proclamation 1996 (as amended) prohibited the use or provision of call back services (also known as "collect calls" or "reverse charges calls"). Either providing or using this service could attract sentences of imprisonment between 2 and 5 years and a fine of up to Birr 10,000 (approximately 362 GBP).

Sec. 8 of the Proclamation concerns "offences related to call-back services"; it covers the provision of call back services in subsection (1) and the use of these services in subsection (2). The substance of the offence is not changed, but sentences for the provision of these services is increased significantly, while sentences for the use of those services shift from a custodial focus to greater economic sanctions.

Sec. 8.1 now provides sentences of between 5 and 10 years and fines equivalent to five times the revenue estimated to have been generated by their illegal conduct. Sec. 8.2 provides that any individual who "obtains" a call back service will be sentenced to imprisonment of between 3 months and 2 years and a fine of between Birr 2,500 and Birr 20,000 (approximately 724 GBP).

ARTICLE 19 opposes the imposition of criminal penalties for providing or using call back services, particularly where the purpose of such penalties is to safeguard a state monopoly over telecommunications. As has already been emphasised, preventing economic loss to Ethio Telecom is not a legitimate basis for imposing criminal liability on individuals for using legitimate forms of communication. Rather than prohibit call back services, the Ethiopian government should explore ways of making international telephone calls more affordable so that revenue is not lost to overseas operators who are able to offer a more competitive service.

Increased penalties for the provision and use of telephone calls or fax services through the Internet

The provision and use of telephone calls or fax services through the Internet has been prohibited in Ethiopia since 2002, when Sec. 24 of the Telecommunications Proclamation 1996 was amended by the Telecommunications (Amendment) Proclamation. Either providing or using these services could attract sentences of imprisonment between 2 and 5 years and a fine of up to Birr 10,000 (approximately 362 GBP) under those provisions. There are no

records of these provisions ever being enforced against users of services that may fall within the ambiguous meaning of "telephone or fax services".

Sec. 10.3 and 10.4 of the Proclamation now prohibits the provision and use of these services in largely the same terms. The particulars of the offences are not detailed, again referencing "telephone and fax services", seeming conferring discretion upon law enforcement officers to interpret this as including VoIP services such as Skype or Google Talk, which substantively offer the same experience as a telephone call and allow documents to be transferred in a functionally equivalent manner to a fax.

The agenda paper does not amend the substance of Sec. 10.3 or 10.4, nor does it formally add a provision repealing the prohibition as contained in Sec. 24 of the Telecommunications Proclamation 1996 (as amended). However, Sec. 17.2 of the Proclamation repeals provisions of any inconsistent law. According to sources in Ethiopia with access to the agenda paper, the prohibition on VoIP was a concern raised during discussions in the Science, Communication and Technology Standing Committee. The agenda paper is reported to assert that "the new legislation legalises the use of VoIP services and it voids the prohibition on private use of VoIP services by the 2002 Telecom Legislation" [based on an unofficial translation].

ARTICLE 19 is concerned that the legality of VoIP services, or any other service that may be considered a "telephone call or fax service", remains ambiguous. If the agenda paper has legal effect and binds the judiciary in their interpretation of the Proclamation, it is noted that it only lifts the restriction in relation to private usage, and that provision of any telecommunication service without a license remains an offence. It is unclear why the text of Sec. 10.3 and Sec. 10.4 has not been amended to reflect these assurances. ARTICLE 19 believes that the assurances alone are not sufficient to provide legal certainty. The conflict between Sec. 10.3 and Sec. 10.4 and the agenda paper violates Article 19 (3) of the ICCPR as the restriction cannot be considered "provided by law" under the tests of certainty or accessibility. The analysis focuses on the text of Sec. 10.3 and Sec. 10.4.

Sec. 10.3 provides increased sentences for the provision of telephone or fax services over the Internet. Imprisonment of between 3 and 8 years is now available, and a fine equivalent to five times the revenue estimated to have been generated by the illegal conduct. Sec. 10.4 reduces custodial sentences for those using these services to between 3 months and 2 years, but increases available fines to between 2,500 Birr and 20,000 Birr (approximately 724 GBP).

ARTICLE 19 strongly opposes the imposition of criminal liability for the provision or use of telephone or fax services over the Internet, whether or not that prohibition is restricted to private or commercial uses. We urge the Ethiopian Government to repeal these provisions.

We recall that the right to freedom of expression and information applies to all forms of expression and their means of dissemination, including all forms of electronic and Internet-based modes of expression. The prohibition on telephone and fax services through the Internet violates Article 19 of the ICCPR, and demonstrates the failure of the Ethiopian government to take into account the extent to which developments in information technology have substantially changed communication practices around the world and the overall public interest in allowing expression through these new technologies. Restricting the use of these technologies also violates the obligation incumbent on Ethiopia to promote and facilitate

universal access to the Internet and other forms of new media, both domestically and through international cooperation.[50]

Sec. 10.3 and 10.4 also grant the Ethiopian government substantial discretion to target critics of the regime on the pre-text of the technology those persons use, thus avoiding drawing attention to the content of the expression that is the true target of the sanction. Reliance on pre-textual justifications for stifling criticism would violate the right to freedom of expression and information, and the targeting of specific forms of communication on-line would violate the principle of net neutrality.

Sec. 10.3 and 10.4 also violate the principle of "net neutrality". We recall that the principle of "net neutrality" protects the consumers' right to access the content, applications, services and hardware of their choice. In their 2011 Joint Declaration, the four Special Mandates stated that 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.[51] The HR Committee have similarly expressed that generic bans on particular online systems are a disproportionate restriction on the right to freedom of expression and information.

ARTICLE 19 therefore finds that Sec. 10.3 and 10.4 violate international standards on the right to freedom of expression and information.

Offences related to the provision of telecommunication service or operators

Under Sec. 24 of the Telecommunications Proclamation 1996 (as amended) it was already an offence to use "the telecommunication service provider network, or bypassing [the] same" to "engage in private or commercial Telecommunication Services" without a license. The Proclamation does not repeal this provision but substitutes it with two similar provisions in Sec. 4 and Sec. 9.

Sec. 4 of the Proclamation makes it a criminal offence to provide telecommunication services without having a valid license in accordance with the appropriate laws. Severe penalties are available under Sec. 4 in comparison with those provided under the 1996 provisions. Imprisonment of between 7 years and 15 years is now available under Sec. 4, as opposed to sentences between 3 years and 5 years, and fines are increased from the equivalent of double the unauthorised income earned during the commission of the crime to the equivalent of triple that income.

Sec. 9.1 similarly prohibits (a) the establishment of any telecommunication infrastructure other than that established by Ethio Telecom and (b) bypassing the telecommunication infrastructure and providing domestic or international telecommunication services. Imprisonment under Sec. 9.1 is increased to between 10 years and 20 years, with a fine equivalent to ten times the revenue estimated to have been earned from the illegal activity. Sec. 9.2 prohibits the use of telecommunications provided in breach of Sec. 9.1.a. Sentences range from 3 months to 2 years imprisonment, and fines between Birr 2,500 to Birr 20,000.

---

[50] See: the HRC Resolution, at Paragraph 3; the Joint Declaration 2011 at Paragraph 6.a and 6.e,

[51] See the Joint Declaration, at Paragraph 5.

ARTICLE 19 finds that both Sec. 4 and Sec. 9 of the Proclamation are too ambiguous, and potentially allow the government substantial discretion to imprison telecommunication users on the basis of vague technicalities and stifle innovation in the telecommunications and ancillary industries. This is due in part to the broad definition of "telecommunication service" in Sec. 2.1 of the Proclamation. For example, in relation to Sec. 4 of the Proclamation, it would be possible for a person to face severe sentences for performing unlicensed maintenance work on a telecommunications device.

Offences related to the fraudulent use of telecommunications

Despite the Proclamation being named after "telecom fraud", fraudulent behaviour is only central to the offences contained in Sec. 7 and Sec. 10.1 - 10.2.

Sec. 7 concerns "fraud of charges" and makes it an offence to fraudulently obtain any telecommunications service without payment of a lawful charge, or by fraudulently charging one's payment to another person. Sentences of imprisonment between 5 and 10 years are available, in addition to a fine equivalent to three times the charge avoided by the illegal act.

Sec. 10.1 concerns the illegal manipulation, duplication of SIM cards, credit cards, subscriber identification numbers or data or sales or otherwise distributing illegally duplicated SIM cards, credit cards or subscriber identification numbers or data. The offence may be punished with imprisonment between 10 and 17 years and a fine between Birr 100,000 to Birr 150,000.

Sec. 10.2.a makes it an offence to connect equipment to a public pay telephone to obtain services not normally available through the public pay telephone. This may be punished with imprisonment from 3 to 8 years and a fine from Birr 30,000 to Birr 80,000.

ARTICLE 19 does not have any comment on these aspects of the Proclamation, other than to express concern at the extremely harsh sentences available for offences that seemingly cause minimal harm to the public.

Sec. 10.2.b makes it an offence to obtain or cause others to obtain telecommunication services from Ethio Telecom by presenting false or forged service agreements, or by fraudulently using the identity code of another person or any other fraudulent means. This may be punished with imprisonment from 3 to 8 years and a fine from Birr 30,000 to Birr 80,000.

ARTICLE 19 does not believe that there exists a pressing need in a democratic society for telecommunication providers to routinely collect information regarding their customers' activities. Governments should therefore not require that persons pre-register or identify themselves to be permitted to use telecommunications networks. These standards are referenced in the Resolution on Surveillance of Communications and Freedom of Expression, 5 June 2009, signed by 30 International Freedom of Expression Organisations, including ARTICLE 19. Registration requirements for the use of telecommunications should therefore be abolished, and any offences related to a failure to properly register for the use of telecommunication services should also be repealed.

Offences related to the unauthorised import or possession of telecommunications equipment

Sec. 3 of the Proclamation prohibits in subsection (1) the manufacture, assembly, import or offers for sale of any telecommunications equipment without a permit from the Ministry of Information and Communication Technology Development. Sentences of between 10 and 15 years imprisonment and fines from Birr 100,000 to Birr 150,000 are available. Subsection (2) further prohibits the use or possession of such equipment, with prison sentences between 1 and 4 years and a fine from Birr 10,000 to Birr 40,000. Subsection (3) allows the Ministry to prescribe the types of technologies that will not require permits, and set their technical standards; however the issuance of such regulations do not appear to be necessary for the enforcement of this provision.

ARTICLE 19 does not believe that there is a pressing social need to require the manufacture, assembly, import or offers for sale of telecommunications equipment to be subject to any specialised regulation. Targeting individuals who purchase or possess such equipment is particularly disproportionate, especially since these individuals are unlikely to know whether the equipment has come to them through legitimate channels or not, and many individuals are unlikely to be able to afford replacement technology if it were confiscated or cut-off. ARTICLE 19 is especially concerned that these provisions may be used as a pretext for depriving critics of the incumbent government of equipment essential to the exercise of the right to freedom of expression or information.

Interception and unauthorised access

Sec. 5 of the Proclamation concerns the interception and unauthorised access to telecommunications services. Sec. 5.1 prohibits obstructing or interfering with "telecommunication networks, services or system"; Sec. 5.2 prohibits the interception or illegal access to any telecommunication system, and Sec. 5.3 prohibits the interception, alteration, destruction or damage of telecommunication calls or other forms of personal information. Sentences of 10 to 15 years are available, and fines from Birr 100,000 to Birr 150,000.

ARTICLE 19 recalls that Ethiopia is obligated to protect the privacy of individuals from invasion by public or private parties. Guaranteeing the right to privacy in communications is essential for ensuring that individuals have the confidence to freely exercise their right to freedom of expression. However, key terms in Sec. 5 are not defined, including what it means to obstruct, interfere, or illegally access telecommunications systems. With this ambiguity, it is unclear how these offences will protect the privacy rights of individuals, and the extent to which government authorities can violate these laws and with what safeguards against abuse.