Ethiopia: Computer Crime Proclamation

July 2016

Legal analysis

Executive summary

In June 2016, Ethiopia's House of People's Representatives adopted the Computer Crime Proclamation 2016 (the Proclamation). The Proclamation deals with a host of issues, ranging from illegal access to computer systems (also known as 'hacking') to disseminating spam and combating child pornography. However, it also creates a number of new criminal offences that are likely to impact heavily on the enjoyment of the right to freedom of expression and other human rights, by extending the reach of criminal defamation and creating various new criminal offences, such as "inciting fear" online, all punishable by imprisonment. It also provides for far-reaching investigatory powers, including surveillance by law enforcement agencies. In a country that has in recent years seen the imprisonment of various bloggers, journalists and human rights activists in apparent contravention of international human rights law, this creates a serious concern as to the future protection in Ethiopia of the right to freedom of expression online.

This legal analysis of the Proclamation analyses its provisions against international human rights law and makes a number of recommendations for reform.

Summary of recommendations

General provisions

- A clause should be inserted requiring that the Proclamation be interpreted in accordance with human rights standards, in particular the rights to privacy and freedom of expression.

Computer crimes

- Articles 3-7 should be completely redrafted, incorporating the following principles:
  - a requirement of dishonest intent should be introduced;
  - a public interest defence should be provided for, covering the accessing or intercepting of data for journalistic purposes and in the public interest;
  - the offence should not be made out unless serious harm or damage was done or likely to be done, particularly for data interference and system interference offences; and
  - the imposition of financial penalties as an alternative to imprisonment should be provided for in order to provide a proportionate penalty for minor infractions.
- The offence of criminal defamation should be removed; or at the very least, the penalty of imprisonment abolished;
- Provided the offences of "making threats", "stalking" and "incitement to violence" already exist in the Criminal Code, Articles 13 and 14 should be removed as unnecessary; any offline equivalent offences should be reviewed and replaced with appropriately narrowly defined offences of 'stalking' and 'inciting violence or hatred', in line with the requirements of international human rights law;
- The drafting of Article 12(2) should be reviewed to provide a definition of 'erotic', as well as of the terms "entice" and "solicit";
- Article 16 should be removed. Instead, service providers should be granted immunity from liability in line with the Manila Principles on Intermediary Liability; any liability should be civil rather than criminal; and
- If our recommendations about Articles 13 and 14 are followed, Article 19 should be removed as redundant; if not, at the very least, instead of providing that different laws can apply concurrently, Article 19 of the Proclamation should provide that only one law can apply.

Preventive and investigative measures

- Data retention requirements should be reviewed in line with international standards on privacy;
- Reference to the Minister in Article 24 (2) should be struck out and replaced by "court";
- An independent body should oversee the implementation of the surveillance regime established under the Proclamation;
- There should be annual reports on the number of surveillance operations, providing as much detail as is possible without undermining any ongoing investigations;
- Individuals who suspect that they have been subject to surveillance should have access to redress, either through court or to a specialised tribunal;
- The power to conduct raids without obtaining any independent authorisation in Article 25 should be repealed; and
- The duty to report cybercrimes under Article 26 should be repealed.

Evidentiary and procedural provisions

- Articles 29-31 should be completely redrafted, incorporating the following principles:
  - Investigative powers should be required to only be used as necessary and proportionate;
  - Investigative authorities should be required to obtain a court order for any intrusive searches, seizures or other orders, and courts should apply due process and proportionality principles in deciding on applications;
  - Investigative authorities should not be allowed to delete content or render it inaccessible;
  - The burden of proof should rest firmly with the prosecution.

Miscellaneous

- The Information Network Security Agency, as a pivotal body in the investigation of computer crimes, should be subject to strict parliamentary scrutiny;
- The Ministry of Justice should be required to refuse to cooperate with any requests for international cooperation likely to violate human rights standards.

Table of contents

Introduction 5
International standards 6
The protection of freedom of expression under international law 6
Limitations on the right to freedom of expression 6
Regulating freedom of expression online 7
Role of Internet intermediaries and intermediary liability 9
Cybercrime 10
Surveillance of communications 11
Analysis of the Proclamation 13
General provisions and definitions 13
Computer Crimes 14
"Crimes against computer systems and computer data" 14
"Illegal content data" 16
"Other offences" 18
Preventive and investigative measures 19
Evidentiary and procedural provisions 21
Roles of government entities and "miscellaneous provisions" (Parts 5 & 6) 22
Annex: A Proclamation to provide for Computer Crimes 23

Introduction

On 7 June 2016, Ethiopia's House of People's Representative adopted the Computer Crime Proclamation 2016.[1] According to its Preamble, the Proclamation aims to protect Ethiopia's economic and political stability. Noting that "information and communication technology plays a vital role in the economic, social and political development of the country", and warning that "unless appropriate protection and security measures are taken, the utilization of information communication technology is vulnerable to various computer crimes … that can impede the overall development of the country and endanger individual rights"[2], the Proclamation explains that Ethiopia's existing legal framework is "not adequately tuned with the technological changes" and insufficient "to prevent, control, investigate and prosecute the suspects of computer crimes."[3]

The Proclamation ostensibly aims to remedy this by creating new criminal offences related to computer crime, providing strong investigatory powers to law enforcement agencies, laying down rules of evidence and clarifying the roles of various government agencies involved with the prevention and detection of computer crime. These new criminal offences range from illegal access to computer systems (also known as 'hacking') to disseminating child pornography, but worryingly – from the perspective of protecting the right to freedom of expression and the enjoyment of other human rights online – the Proclamation also creates a number of new criminal offences that are likely to impact heavily on the enjoyment of these rights. Section Three of the Proclamation, entitled "Illegal content data", creates various criminal offences, including "causing fear" to a person;[4] "inciting fear" among the population;[5] and committing defamation online, all punishable with imprisonment.[6] These new offences will heavily impact on the enjoyment of human rights online.

Given the recent history in the country of the imprisonment of bloggers and human rights and democracy activists for the legitimate exercise of their right to freedom of expression, there is great scope for the abuse of broadly worded new offences such as created by the Proclamation. Furthermore, in Part Three of the Proclamation, far-reaching surveillance is authorised and Part Four of the Proclamation grants access to computer data. Ethiopia's Information Network Security Agency, created in 2011,[7] is mandated to establish an "online computer crimes investigation system" and empowered to conduct "sudden searches" when it suspects computer crime.
This legal analysis of the Proclamation compares its provisions against international human rights law, focusing on human rights treaties ratified by Ethiopia at both the United Nations and African Union levels, as well as against recommendations made by intergovernmental bodies such as the United Nations Special Rapporteur on Freedom of Expression. These international standards are set out in the next section; the following section contains a detailed legal analysis of the Proclamation along with recommendations for reform.

[1] Attached as Annex to this analysis. This analysis has been conducted on the basis of an English translation of the Proclamation.
[2] Preamble, Paragraphs 1 and 2.
[3] Preamble, Paragraph 3.
[4] Proclamation, Article 13(2).
[5] Proclamation, Article 14.
[6] Proclamation, Article 13(3).
[7] For more information about INSA, see its website: http://www.insa.gov.et/web/en/home.

International standards

The protection of freedom of expression under international law

The right to freedom of expression is protected by a number of international human rights instruments. These include in particular Article 19 of the Universal Declaration of Human Rights (UDHR)[8] and Article 19 of the International Covenant on Civil and Political Rights (ICCPR);[9] as well as, at the regional level, Article 9 of the African Charter on Human and Peoples' Rights (ACHPR).[10] The ICCPR and ACHPR are binding international treaties ratified by Ethiopia;[11] the freedom of expression guarantee in the UDHR is binding on Ethiopia as a rule of customary international law.[12]

Various important recommendations and declarations elaborating on the meaning of the right to freedom of expression have been issued by the intergovernmental bodies tasked with supervising international human rights treaties, and these constitute authoritative interpretations of binding treaty law. The most important ones among these are statements by the UN Human Rights Committee, which supervises the implementation of the ICCPR and which has issued a lengthy General Comment on the Right to Freedom of Expression,[13] and the African Commission on Human and Peoples' Rights, which supervises the implementation of the ACHPR and which in 2002 issued a Declaration of Principles on Freedom of Expression in Africa (African Declaration).[14] In addition, statements and recommendations made by the UN and African Union Special Rapporteurs on the right to freedom of expression are similarly crucial in understanding how the right to freedom of expression applies in different contexts. Collectively, these form a body of law[15] that is crucial to interpreting the meaning of the right to freedom of expression.

Limitations on the right to freedom of expression

While the right to freedom of expression is a fundamental right, it is not an absolute right; in certain, narrowly defined circumstances, restrictions may be imposed on it. However, any restrictions must be strictly necessary, be narrowly tailored and may not put in jeopardy the right itself. In accordance with international law, restrictions must:

- *be prescribed by law*: this means that a norm must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.[16] Ambiguous, vague or overly broad restrictions on freedom of expression are impermissible;
- *pursue a legitimate aim*, exhaustively enumerated in Article 19(3) of the ICCPR as respect of the rights or reputations of others, protection of national security, public order, public health or morals. As such, it would be impermissible to prohibit expression or information solely on

[8] UN General Assembly Resolution 217A(III), adopted 10 December 1948.
[9] Adopted by UN General Assembly Resolution 2200A(XXI) of 16 December 1966, in force 23 March 1976.
[10] African 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 21 October 1986.
[11] Ethiopia acceded to the ICCPR on 11 June 1993, and to the ACHPR on 15 June 1998.
[12] Whilst not a binding document at its adoption, core parts of the UDHR, including the right to freedom of expression, are widely recognized to have acquired the force of customary international law. See e.g. *Filartiga v. Pena-Irala*, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2nd circuit).
[13] UN Human Rights Committee General Comment 34, CCPR/C/GC/3, adopted on 12 September 2011.
[14] Adopted at the 32nd Session of the African Commission on Human and Peoples' Rights, 17-23 October 2002.
[15] Usually referred to as 'soft law', indicating that while they lack the binding force of law of a treaty, they are nevertheless authoritative and persuasive statements that are a strong guide to how the corresponding treaty should be interpreted.
[16] E.g. *Leonardus J.M. de Groot v. The Netherlands*, No. 578/1994, U.N. Doc. CCPR/C/54/D/578/1994 (1995).

the basis that they cast a critical view of the government or the political social system espoused by the government;

- *be "necessary" to secure the legitimate aim.* Necessity requires that restrictions are proportionate to the legitimate aim pursued, and that there is a pressing social need for them. The State invoking the restriction must show a direct and immediate connection between the expression and the protected interest. Proportionality requires that a restriction on expression is not over-broad and that it is appropriate to achieve its protective function. It must be shown that the restriction is specific and individual to attaining that protective outcome and is no more intrusive than other instruments capable of achieving the same limited result.[17]

Article 20(2) of the ICCPR requires States to prohibit any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited. However, any restrictions on freedom of expression that are imposed pursuant to this provision should also comply with the three-part test outlined above. States should never prohibit all negative statements towards national groups, races and religions; the requirement of Article 20(2) is restricted to prohibit the advocacy of hatred that constitutes incitement to discrimination, hostility or violence.

Regulating freedom of expression online

General Comment No 34,[18] adopted by the UN Human Rights Committee in September 2011, explicitly recognises 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.[19] In other words, the protection of freedom of expression applies online in the same way as it applies offline. State parties to the ICCPR are also required to consider the extent to which developments in information technology, such as Internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world.[20] 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.[21]

Similarly, the four special mandates for the protection of freedom of expression, including the African Special Rapporteur on Freedom of Expression and Access to Information, have highlighted in their Joint Declaration on Freedom of Expression and the Internet of June 2011 that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the Internet.[22] In particular, they recommend the development of tailored approaches for responding to illegal content online, while pointing out that specific restrictions for material disseminated over the Internet are unnecessary. They also promote the use of self-regulation as an effective tool in redressing harmful speech.

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression elaborated on the regulation of online speech in two reports in 2011.[23] In his

---

[17] E.g. *Velichkin v. Belarus*, Communication No. 1022/2001, U.N. Doc. CCPR/C/85/D/1022/2001 (2005).
[18] *Op. cit.*
[19] *Ibid.*, para. 12.
[20] *Ibid.*, para. 17.
[21] *Ibid.*, para. 39.
[22] Joint Declaration on Freedom of Expression and the Internet, Declaration signed by the UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information on 1 June 2011: http://www.osce.org/fom/78309.
[23] Report of the UN Special Rapporteur on Freedom of Expression, A17/27, 17 May 2011 and Report of the UN Special Rapporteur on Freedom of Expression, A/66/290, 10 August 2011.

September 2011 report, the Special Rapporteur clarified the scope of legitimate restrictions on different types of expression online and 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.[24]

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 legislation criminalizing these types of expression must still comply with the 'three part test': it should be sufficiently precise; necessary and proportionate; 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.[25]

This means, for example, that legislation prohibiting hate speech or the dissemination of child pornography over the Internet must be unambiguous in its wording, must be limited to the legitimate aims provided in Article 19 ICCPR, and must respect the principles of necessity and proportionality. The Special Rapporteur has specifically 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. This includes expressions such as combating "incitement to religious unrest", "promoting division between believers and non-believers", "defamation of religion", inciting to violation", "instigating hatred and disrespect against the ruling regime", "inciting subversion of state power" and "offences that damage public tranquillity".[26]

The Special Rapporteur has also clarified which online restrictions are, in his view, impermissible under international law. In particular, he has called upon States to provide full details about the necessity and justification for blocking a particular website, stressing that the "determination of what content should be blocked should be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences to ensure that blocking is not used as a means of censorship."[27]

Finally, the Special Rapporteur has highlighted that all other types of expression, such as defamatory comments, should not be criminalised. Instead, States should promote the use of counter speech to combat offensive speech. In this regard, it is worth mentioning that with new Web 2.0 types of applications, including the comment section on newspapers' websites, blogs, online chat rooms etc., it is now possible to respond to derogatory comments online almost immediately and at no cost. For this reason, the Special Rapporteur has remarked that the sanctions available for offline defamation and similar offences may well be unnecessary and disproportionate online.[28]

---

[24] *Ibid*, para. 18.
[25] *Ibid*, para. 22.
[26] Joint submission by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the Special Rapporteur on freedom of religion or belief and the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance is available from http://www2.ohchr.org/english/issues/opinion/articles1920_iccpr/docs/experts_papers.htm
[27] 2011 Report of the UN Special Rapporteur, *op. cit.*, para 38.
[28] 2011 Report of the UN Special Rapporteur, *op. cit.*, para 28.

Role of Internet intermediaries and intermediary liability

Intermediaries, such as Internet Service Providers (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. They have come to be seen as the gateways to the Internet without which most people would not be able to gain access to information online. Because of this crucial position, many countries have granted Internet intermediaries complete or conditional immunity for third-party content.[29] They have also been exempted from monitoring content.[30]

At the same time, in most conditional liability regimes Internet intermediaries are subject to notice and take-down procedures whereby they are given an incentive to remove allegedly unlawful content upon notice from private parties or law enforcement agencies lest they face liability. Such notice and takedown procedures have been sharply criticised by the UN Special rapporteur on freedom of expression, including for their lack of clear legal basis and basic fairness. In particular, he noted:[31]

> [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)

Accordingly, the four special rapporteurs on freedom of expression recommended in their 2011 Joint Declaration on Freedom of Expression and the Internet that:

- 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;
- Liability should only be incurred if the intermediary has specifically intervened in the content, which is published online;
- ISPs and other intermediaries should only be required to take down content following a court order, contrary to the practice of notice and takedown.[32]

---

[29] See for example, the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, the 'E-commerce directive' in the EU. See also the Communications Decency Act 1996 in the US, and in Singapore, the Electronic Transaction Act 2010 which gives strong protection to innocent providers.

[30] See Article 15 of the E-commerce directive. In the case of *SABAM v. Scarlet Extended SA*, the Court of Justice of the European Union 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.

[31] UN Special Rapporteur on Freedom of Expression report, *op. cit.,* para. 42.

[32] The 2011 Joint Declaration, *op. cit.*

Cybercrime

Increasingly, countries attempt to regulate internet content through so-called "cybercrime legislation". At present, there is no universal definition of the term "cybercrime",[33] the term is usually used to describe any traditionally defined crime that is committed using a computer network or the internet. It typically covers a wide range of criminal offences from terrorist activities and espionage conducted with the help of the internet and illegal hacking into computer systems, to running boot nets[34] for the purpose of spreading spam emails and credit card fraud, phishing, theft and manipulation of data, and cyber-stalking, to name just a few.

Many of the recently adopted laws are, however, vague and overly broad and are therefore open to arbitrary and subjective interpretation, threatening the protection of the right to freedom of expression. This has lead the UN Special Rapporteur on freedom of expression to voice his strong concern:

> [L]egitimate online expression is being criminalized in contravention of States' international human rights obligations, whether it is through the application of existing criminal laws to online expression, or through the creation of new laws specifically designed to criminalize expression on the internet. Such laws are often justified on the basis of protecting an individual's reputation, national security or countering terrorism, but in practice are used to censor content that the Government and other powerful entities do not like or agree with.[35]

International standards on cybercrime do recognise the importance of balancing security imperatives with fundamental human rights, in particular the right to freedom of expression. In particular, 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.[36]

It is noteworthy that this convention contains no content-based restrictions other than those relating to child pornography. It should also be mentioned that the convention recognises the potential for domestic cybercrime laws to target political dissent and allows states to refuse assistance to other states if that request is perceived to relate to a politically motivated prosecution.[37]

The African Union Convention on Cyber Security and Personal Data Protection provides that cybercrime laws should, "ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by

---

[33] For example, the Council of Europe Convention on Cybercrime, adopted 23 November 2001 (see at http://bit.ly/2aulqQG) does not include a definition on cybercrime but lists offences to be criminalized by member states. The UN Manual on the Prevention and Control of Computer Related Crime (see at http://bit.ly/29UKRZT) includes fraud, forgery, and unauthorized access in its definition of computer(-related) crimes. The NATO Parliamentary Assembly equates cyber-attacks with cybercrime, cyber terror, or cyber war, depending on the involved type of actors and motivations: NATO Parliamentary Assembly, 2009 Annual Session Committee Report, 173 DSCFC 09 E BIS – NATO and Cyber Defence, at http://bit.ly/2a0tHO2.

[34] "Boot net" is term used for booting (or "jumpstart") over the network, that is a process or set of operations that loads and starts the operating system.

[35] The 2011 Report of the UN Special Rapporteur, *op. cit.*, para 34.

[36] Council of Europe Convention on Cybercrime, *op. cit.*, Preamble.

[37] *Ibid.*, Article 27(4)(a).

international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, amongst others."[38]

It is therefore abundantly clear that international human rights law and best practice requires that legislation aimed at countering cybercrime has to be crafted in such a way that it is compatible with human rights law and international freedom of expression standards and that it must not be used to silence legitimate speech or to pursue critical citizens, human rights defenders, bloggers and journalists. Cybercrime legislation should respect the proportionality principle that is fundamental to human rights protection and should meet the following criteria:

- Any legislation should provide for narrowly defined, clear and adequate definitions of key legal and technical terms covered by the offence;
- Any legislation should not contain content-based offences other than those related to child pornography;
- Legislation should require proof about the likelihood of harm arising from the criminal activity, including in relation to offences involving the obtaining or dissemination of classified information;
- Legislation should require the nature of the threat to national security resulting from any criminal activity to be identified;
- Legislation should provide for a public interest defence in relation to the obtaining and dissemination of information classified as secret;
- Legislation should refrain from imposing prison sentences for expression-related offences, except for those permitted by international legal standards and with adequate safeguards against abuse.[39]

Surveillance of communications

The right of private communications is strongly protected in international law through Article 17 of the ICCPR,[40] that 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 UN Human Rights 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:

> 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 UN Special Rapporteur on promotion and protection of human rights and fundamental freedoms while countering terrorism has argued that like restrictions on the right to freedom of expression under Article 19, restrictions of the right to privacy under Article 17 of the ICCPR should be interpreted as subject to the three-part test: [41]

---

[38] African Union Convention on Cyber Security and Personal Data Protection, adopted 27 June 2014, not yet entered into force, Article 25(3).

[39] See ARTICLE 19, *Freedom of expression and ICTs: Overview of international standards*, 2013, at http://bit.ly/29NwJ5C.

[40] Article 17 states: 1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2) Everyone has the right to the protection of the law against such interference or attacks.

[41] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms

> [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.

The UN Special Rapporteur on Freedom of Expression has similarly observed that:

> [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.[42]

---

while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009.

[42] *C.f.* Report of the UN Special Rapporteur on Freedom of Opinion and Expression, 16 May 2011, *op.cit.*

Analysis of the Proclamation

This section analysis the provisions of the Proclamation against the international human rights law standards set out in the preceding section. The Proclamation consists of six parts:

1. Part One, containing general provisions and definitions;
2. Part Two, dealing with "computer crimes";
3. Part Three, detailing "preventive and investigative measures";
4. Part Four, providing evidentiary and procedural provisions;
5. Part Five, detailing the various government entities that have a role in the prevention, detection and investigation of computer crime; and
6. Part Six, providing a set of "miscellaneous provisions".

We will analyse these in turn.

General provisions and definitions

Article 1 provides the Proclamation's formal short title: "Computer Crime Proclamation No. —/2016". In this Analysis, it will be referred to as "the Proclamation."

Article 2 of the Proclamation provides a number of definitions. These are important as they govern the Proclamation's scope. For example, ""computer or computer system" is defined very broadly to encompass any software and the microchips technology based device, or any device that is capable of performing logical functions, and any accessories to that device. "Data" is similarly broadly defined, as are the terms "access"; "interception" and "service provider", to name but a few. These definitions impact on the interpretation of other provisions in the Act and rather than critique them in isolation, we will discuss them as part of our critique of the operative provisions of the Proclamation, where relevant.

What is lacking in these introductory provisions, or in the Proclamation's Preamble, is an overarching requirement that the Proclamation be interpreted and implemented with due respect for human rights, in particular the rights to privacy and freedom of expression. While constitutional law purists might argue that this is not strictly speaking necessary because the Ethiopian constitution already protects the rights to freedom of expression and privacy,[43] there would nevertheless be strong interpretative value in inserting a clause stating this given the impact of the Proclamation on the enjoyment of human rights. This would also give effect to the African Union Convention on Cyber Security and Personal Data Protection,[44] which requires all states Parties to ensure that measures implemented for the protection of cyber security do not infringe human rights,[45] and help bring the Proclamation in line with the international human rights law standards discussed in the preceding section by stating that in case of doubt, the Proclamation should be interpreted in line with human rights standards. This would also be consistent with best practice in this area, notably the COE Convention on Cybercrime.[46]

Recommendations:

- A clause should be inserted requiring that the Proclamation be interpreted in accordance with human rights standards, in particular the rights to privacy and freedom of expression.

[43] The Ethiopian Constitution, Articles 29 and 26, respectively; at http://bit.ly/2a0ugYn.
[44] As adopted June 27, 2014, not yet entered into force; at http://bit.ly/2achRPE.
[45] At Article 25(3), "Rights of Citizens".
[46] See Article 15.

Computer Crimes

Part Two of the Proclamation consists of four separate sections, establishing various different computer crimes.[47] Section One establishes "Crimes against computer systems and computer data"; Section Two establishes crimes concerning to computer-related forgery, fraud and theft; Section Three establishes categories of "illegal content data"; and Section Four lays down various "other" offences. We will analyse, Sections One, Three and Four, which are more closely linked to freedom of expression.

"Crimes against computer systems and computer data"

Articles 3 and 4 establish the crimes of illegally "accessing" and "intercepting" computer data or computer systems, without authorisation or "in excess of authorisation". They provide prison sentences of three and five years respectively, or up to 15 years if the computer systems are deemed "critical" (defined as causing "considerable damage on public safety and the national interest"[48]). No defences are provided, for instance for the protection of the public interest.

Articles 5 and 6 create criminal offences of, respectively, "interference with computer systems", punishable with a fine or "rigorous" imprisonment from three to five years, and "causing damage to computer data", punishable with a fine or "rigorous" imprisonment for up three years. Prison sentences of a minimum of three years are prescribed if the computer system or data belonged to a legal person (i.e. a corporation or an organisation), and a minimum of five years if the interference or damage has affected critical infrastructure.

Article 7 creates a number of offences that are ancillary to the preceding articles: paragraphs 1 and 2 criminalise the 'intentional transmission' of a computer program that can cause damage, or the sale of computer equipment or software designed or adapted to commit an offence under articles 3-6; paragraph 3 criminalises possession of any such hardware or software; and paragraph 4 criminalises disclosing the passwords for computer systems. All these ancillary offences are punishable with imprisonment and a fine, with the exception of paragraphs 1 and 3 which provide for a fine as an alternative to imprisonment.

Under Article 8, it is an aggravating factor if any of the offences created in the preceding provisions concern computer systems or data designated as "top secret by the concerned body for military interest or international relation, and while the country is at a state of emergency or threat"; in this scenario, a prison sentence of 15 to 25 years is imposed.

Read together with the definitions in Article 2, Articles 3-7 create a series of offences that are very broad and likely to capture acts that are perfectly legitimate under international human rights law. The impact of these provisions on the enjoyment of the right to freedom of expression and the exercise of journalism is significant and is likely to have a substantial chilling effect.

- Overbroad offences and the chilling effect: Articles 3 and 4 would discourage any whistleblowers, who may have evidence of gross corruption or human rights violations, from coming forward; and it would also discourage journalists from publishing any such evidence in the media. For example, a bank employee who notices suspicious banking transactions involving large sums of money being channelled into the personal bank accounts of public officials would not even be able to provide a screenshot without risking a penalty of

[47] It should be noted that many of these have been developed from Sections 706-711 of the Ethiopian Criminal Code, see: http://bit.ly/2acjf58, and Proclamation No. 761/2012 (the Telecom Fraud Offence Proclamation), at http://bit.ly/2ab8z9T. Both sets of provisions are repealed in Part Six of the Proclamation.
[48] Article 2(10).

imprisonment; and a journalist who might wish to publish a story based on this information would similarly risk imprisonment because of the broad definitions of "accessing" computer data and the absence of any public interest defence. Any prosecution in such circumstances would be a clear violation of the right to freedom of expression. These provisions should be redrafted to allow for a public interest defence, impose much lighter minimum sentences and require that harm be done.

- Lack of serious harm requirement and disproportionate sentences: Articles 5 and 6 similarly establish widely drafted criminal offences punishable with hard sentences of up to twenty years imprisonment. Article 5 does not require any serious harm to occur, yet imposes a prison sentence of a minimum of three years for anyone who "intentionally hinders, impairs, interrupts or disrupts the proper functioning of the whole or any part of computer system". This would be grossly disproportionate for a minor offence causing only slight disruption to the functioning of any computer system, even a home network. Article 6 is similarly disproportionate, imposing a prison sentence of up to three years as well as a fine for any damage to computer data. Because of the very wide definition of "computer data" in Article 2, this would mean that even the deletion of an innocuous email becomes subject to a sentence of imprisonment. Both provisions should be redrafted to provide that no offence is committed unless serious harm is caused, and should allow for the imposition of monetary fines as an alternative to imprisonment.
- Lack of dishonest intent: A further problem with these provisions is that as drafted, the requirement of 'intent' relates only to the act of gaining access, interference or interception – and not to the damage that may be caused as a result of the act, or to illegally obtaining data. It would be preferable if, in line with Article 2 of the Cybercrime Convention, these provisions required "dishonest intent" or analogous wording.
- Other issues: The offences created under Article 7 are similarly problematic. First, because the offences created under paragraphs (1)-(4) are linked to the broadly framed offences of Articles 3-6, they cast a similarly wide net and could easily criminalise legitimate journalistic undertakings. For example, the secure drop websites that have been created in various countries to allow whistle-blowers securely to provide information to journalists[49] would be deemed criminal under Article 7(2) and the providers of these websites – deemed legitimate in democratic countries around the world – would face arrest if they landed in Addis Abeba. Providing software that can break Digital Rights Management systems would also be criminalised, despite the fact that DRM systems are themselves highly controversial – for example, they can prevent individuals from using copyrighted works in a way that is ordinarily protected by the defence of "fair use" or from transferring content that has been lawfully obtained from one device to another. The provisions in Article 7 are problematic in other respects as well. For example, paragraph (3) criminalises mere possession of a computer programme which may be used to commit an offence under Articles 3-6, regardless of whether an offence is actually committed; while paragraph (4) imposes a harsh prison sentence on anyone who discloses a password regardless of whether that disclosure has caused any harm (paragraph 5 only remedies this somewhat by stating that if the disclosure was unintentional, the prison sentence shall not exceed one year, which is disproportionately harsh for the unintentional disclosure of a password which caused no harm whatsoever).

Recommendations:

- Articles 3-7 should be completely redrafted, incorporating the following principles:
  - a requirement of dishonest intent should be introduced;

[49] Wikileaks is the best known, but there are various others, including GlobaLeaks (https://www.globaleaks.org/), PubLeaks (https://publeaks.nl/), for Dutch media; https://whistleblowing.jp/ (which can be accessed only via Tor); and IRPILeaks (https://irpi.eu/irpileaks/, also accessible via Tor only).

- a public interest defence should be provided for, covering the accessing or intercepting of data for journalistic purposes and in the public interest;
- the offence should not be made out unless serious harm was done or likely to be done, particularly for data interference and system interference offences; and
- the imposition of financial penalties as an alternative to imprisonment should be provided for in order to provide a proportionate penalty for minor infractions.

"Illegal content data"

Section Three of the Proclamation establishes a number of offences related to 'content', separated into 'obscene or indecent crimes against minors'; 'crimes against liberty and the reputation of persons'; 'crimes against public security'; and the 'dissemination of spam':

- Article 12 criminalises the depiction of minors, or persons appearing to be minors, engaged in explicit sexual conduct; as well as the so-called 'grooming' of minors by sending erotic content;
- Article 13 provides a series of offences criminalizing "intimidation" by sending any content; "causing fear, threat or psychological strain" by continuously sending emails or posting messages about someone or by "keeping their computer communication under surveillance"; and publishing any defamatory writing – all punishable with imprisonment except for spreading defamatory content, which is punishable with imprisonment or a fine;
- Article 14 criminalizes writing any messages that "incite fear, violence, chaos or conflict among people", punishable with rigorous imprisonment; and
- Article 15 criminalises sending of spam email, punishable with imprisonment and a fine unless consent has been obtained.

Article 16 deals with the liability of service provides, and states that they are criminally liable for the offences created under Articles 12-14 (but not 15) if they are directly involved in the dissemination or editing of the content, or if they fail to remove or disable access to data upon obtaining actual knowledge of its illegality or receiving notice from the 'competent administrative authorities'. This links with Article 26, which requires service providers to report to the authorities any computer crime committed through its systems that it becomes aware of. It should be noted in this regard that the definition of service provider is extremely broad, and would encompass a university that provides access to students as well as a company or media outlet that provides a computer system for its employees.[50]

Making threats, stalking, defamation and incitement to violence

From a human rights perspective, the offences created under Articles 13 and 14 are highly problematic and violate the human rights guarantees laid down in the Ethiopian constitution as well as in international human rights law, in particular the right to freedom of expression. None comply with the basic criteria, outlined in the preceding section of this legal analysis that criminal offences should be carefully and narrowly worded and be proportionate to the pursuit of a legitimate aim. For example:

- Article 13(1) of the Proclamation criminalizes posting any material online that might be perceived as 'intimidating' and imposes a prison sentence for any such postings. There is no definition of 'intimidating' in the proclamation and in practice, this could include anything from posting evidence of corruption – which would certainly be intimidating to the person

[50] Service provider is defined as "a person who provides technical data processing or communication service or alternative infrastructure to users by means of computer system".

accused of being corrupt – to evidence of large scale damage to the environment, which could be perceived as 'intimidating' or even 'threatening' to people affected by it;
- Article 13(2) probably seeks to criminalize so-called 'stalking' but defines this so broadly as to include legitimate journalism. For example, a journalist who reports on government corruption or mismanagement and publishes a series of reports concerning the corrupt behaviour of a particular public official may well be seen to be "causing psychological strain" by "repeatedly" publishing stories. This would render good journalism punishable by imprisonment;
- Article 13(3) re-creates the offence of criminal defamation in a digital context, punishable by imprisonment or a fine. The imposition of imprisonment for criminal defamation has been condemned by international human rights courts including the African Court of Human and Peoples' Rights,[51] and the African Commission has called on all African States to abolish criminal defamation.[52] To include this in new legislation is a very regressive step;
- Article 14, criminalizing the publication of any content that incites chaos, fear, violence or conflict, would result in the potential imprisonment of journalists who report on environmental disasters or war. Such reporting may well incite "fear" among the public, particularly those sections of the public directly affected by the event reported on, but it would still be legitimate reporting. To the extent that Article 14 seeks to criminalize the incitement of hatred or war, it should comply with the guarantees laid down in Articles 19 and 20 ICCPR and be tightly drafted as to criminalize only such material the publication of which has a real likelihood of resulting in hatred or war.

In any event, we note that it is highly likely that the offences under Articles 13 (1) (making threats), 13 (2) (stalking) and 14 (incitement to violence) are already criminalised in the Penal Code. As such, the creation of equivalent online offences is unnecessary. As such, Articles 13 (1), 13 (2) and 14 should be removed. At the same time, the Ethiopian Parliament should ensure that the existing "offline" offences of "making threats", "stalking" and "incitement to violence" comply with international standards on freedom of expression. We further note that Article 13 (2), which criminalises defamation, and any offline equivalent offence, are incompatible with international standards on freedom of expression and should be removed entirely from Ethiopia's statute book.

Child pornography

Although the main offences created in Article 12, of making, possessing or distributing child pornography, are in line with international human rights law, we note that there is no definition of "erotic" in Article 12(2). As a result, there is a danger that even sending educational materials or content related to sexual health could be interpreted as 'erotic'. Because 'enticing' or 'soliciting' is similarly undefined, this creates the danger of criminalizing sexual education or similarly legitimate work. The drafting should be revisited to prevent this.

Intermediary liability

Article 16, on the liability of service providers, is problematic in several respects.

- Liability, if any, should be civil rather than criminal: to begin with, we note that imposing criminal liability on service providers is out of step with best practice in this area. Instead, service providers should be granted immunity from liability in line with the Manila Principles

[51] E.g. *Lohé Issa Konaté v. The Republic of Burkina Faso*, African Court on Human and Peoples' Rights, App. No. 004/2013, 5 December 2014.
[52] ACHPR/Res169(XLVIII)2010: Resolution on Repealing Criminal Defamation Laws in Africa

on Intermediary Liability.[53] To the extent that service providers may be held liable for third-party content in limited circumstances, any liability should only be civil rather than criminal.

- Lack of definitions and safeguards: secondly, and in any event, the wording used in Article 16 is vague and several key terms are left undefined. For example, intermediaries are criminally liable if it can be proven that they were "directly involved" in the dissemination of spam, but the Proclamation fails to define direct involvement. Similarly, the term "actual knowledge" is undefined – and this, as experience in other countries shows, is a key term, as are the "competent administrative authorities" (we note that in different contexts, different authorities may have competence and this should be clarified, particularly bearing in mind the potentially very heavy penalties, including imprisonment). Moreover, we note that the definition of "service provider" is very broad, with the liability regime under Article 16 failing to distinguish between the different kinds of activities intermediaries are engaged in for the purposes of liability (mere conduit, caching, hosting). This means that a potentially very high number of service providers could fall within the scope of Article 16 so long as they process data. The Proclamation also fails expressly to prohibit general monitoring of their networks and content by service providers

Recommendations:

- The offence of criminal defamation should be removed; or at the very least, the penalty of imprisonment abolished;
- Provided the offences of "making threat", "stalking" and "incitement to violence" already exist in the Criminal Code, Articles 13 and 14 should be removed as unnecessary; any offline equivalent offence should be reviewed and replaced as the case may be with appropriately narrowly defined offences of 'stalking' and inciting violence or hatred, in line with the requirements of international human rights law;
- The drafting of Article 12(2) should be reviewed to provide a definition of 'erotic', as well as of the terms "entice" and "solicit"; and
- Article 16 should be removed: service providers should not be held criminally liable for content produced by others; instead, they should be granted immunity from liability in line with the Manila Principles on Intermediary Liability, and any liability should be civil rather than criminal.

"Other offences"

Section Four of the Proclamation establishes a number of other offences and clarifies the applicable punishment of legal persons such as corporations. Article 17 lays down penalties, including imprisonment, for failing to cooperate with or hindering investigations under the Proclamation; Article 18 provides that when crimes are committed with the means of a computer for offences not provided for in the Proclamation, the relevant other law shall apply; and Article 19 provides that when conduct is committed that constitutes an offence under the Proclamation as well as under other law, then both laws shall apply concurrently. Article 20 substitutes imprisonment for fines if an offence is committed by a juridical person, such as a corporation.

The offences for hindering or failing to cooperate with an investigation are harsh and problematic primarily because of the broad scope of the offences created under the Act (see, for example, the preceding section critiquing Articles 13 and 14). To the extent that an offence created under this Proclamation clearly violates international human rights law, the ancillary offence of hindering an investigation or failing to cooperate with it would similarly violate international human rights law.

[53] https://www.manilaprinciples.org/

This underscores the urgency of reforming the Proclamation and bringing it in line with international human rights law.

Article 19 creates uncertainty by providing that different provisions can apply concurrently to offences, potentially setting different thresholds for liability, different defences and different levels of punishment. As noted earlier, it is both unnecessary and highly undesirable, in our view, to create specific online offences where an offline equivalent offence already exists (see our analysis above in relation to Articles 13 and 14). This is especially so given that online offences are usually punished more harshly than their offline equivalent contrary to international standards on freedom of expression.[54] At the very least, we believe that cybercrime laws such as the Proclamation should create certainty by providing either that they apply, as *lex specialis* or *lex posterior*, or that another law applies.

Recommendation:

- If our earlier recommendations about Articles 13 and 14 are followed, Article 19 should be removed as redundant;
- If not, at the very least, instead of providing that different laws can apply concurrently, Article 19 of the Proclamation should provide that only one law can apply.

Preventive and investigative measures

Part Three of the Proclamation provides the preventative and investigative measures that can be invoked for the investigation or prevention of offences under the Proclamation. Article 21 provides that all computer crime is investigated in accordance with the provisions of the Proclamation. Under Article 22, the police and prosecutors' office have joint responsibility, with the prosecutor taking the lead in investigations. Both will be supported in their tasks by the Information Network Security Agency.

Articles 23 and 24 provide important requirements on data retention and surveillance. Under Article 23, service providers must retain all computer data passing through its systems for at least one year, and must disclose this on the order of a court or a public prosecutor. Article 24 provides that police and prosecutors may, by warrant of a court, intercept communications if this is deemed "necessary". Such surveillance may be instigated only as a means of last resort. In urgent cases, and when damage to critical infrastructure may occur as a result of computer crime, surveillance may be authorized by the President of the Federal High Court, on the recommendation of a minister, instead of a court. Data collected through surveillance that is not necessary for the investigation must be destroyed immediately, "upon the decision of the Minister". Service providers are required to cooperate with these surveillance operations.

Article 25 authorises the Information Network Security Agency to conduct "sudden searches" of computer systems deemed to be at risk or at the source of an attack when there are reasonable grounds to believe that a computer crime is to be committed and it is necessary to prevent and control this, to provide early warning to citizens, or to minimize the risks for the effectiveness of an ongoing investigation. Article 26 imposes a duty on service providers to report the commission of the crimes stipulated in the Proclamation or dissemination of any illegal content data by third parties of which they have knowledge. They must also take appropriate measures, which are undefined. Article 27 provides that where there are reasonable grounds to believe that a computer crime is (being) committed, the police may arrest suspects, in accordance with the provisions of the Criminal Procedure Code.

[54] A/HRC/20/L.13

The problems with these provisions are twofold:

- Underlying crimes fail to comply with international human rights law: The first set of problems relate to the fact that they are linked with the investigation and prevention of 'crimes' that themselves contravene international human rights law. As set out in preceding sections of this analysis, many forms of legitimate journalism will be criminalized under provisions of the Proclamation, in particular Articles 13 and 14. It is entirely likely that a media outlet reporting on government corruption or ethnic conflict would commit an "Offence against public security". Not only would this in itself violate international human rights law, but any action taken against that media outlet under Articles 24 or 25, such as a search or interception of communications, would also violate international human rights law. Again, this illustrates the urgency of repealing and reforming the affected parts of the Proclamation, as argued in preceding sections of this legal analysis.
- Investigatory powers fail to provide for sufficient safeguards: The second set of problems lies within the provisions of Part Three of the Proclamation. As set out in the section on standards, international human rights law requires safeguards to prevent the abuse of powers such as those provided in Part Three. These safeguards consist of requirements of legality, proportionality and necessity, as well as transparency, accountability and due process. However, they have been implemented in the Proclamation only in part:
    - *Data retention requirements:* the data retention requirements under Article 23 are disproportionate and inconsistent with best practice in this area.[55] In particular, the Proclamation fails to provide for an upper limit on the period of time during which the data may be retained. Moreover, and in any event, Article 23 provides for the blanket retention of data without any regard for the kind of data that may be necessary for a given purpose.
    - *Real-time collection of computer data and undue role of the Minister:* the role of the Minister in the procedure involving real-time collection of computer data in non-urgent cases under Article 24 (2) is unclear. In our view, the Minister should not be involved at all in such cases.
    - *Lack of independent oversight and redress for surveillance operations:* there is no transparency of any operations undertaken under the Proclamation. In most democratic countries, legislation providing for surveillance powers establish an independent oversight body. Moreover, the Proclamation fails to provide for any means of redress for individuals affected by surveillance or sudden searches. Revelations such as the Snowden leaks have shown that governments have in the past abused powers of surveillance, and the only way to prevent this is by transparency and providing redress to those affected.
    - *Searches without warrant:* Article 25 raises the spectre of sudden searches and seizures without being authorised by a court. This is an extreme measure and as currently provided, there is every likelihood that this will be abused to raid the premises of independent media outlets or bloggers that are critical of the government, or political opponents. Unless the substantive offences provided in Articles 13 and 14 are repealed and/or reformed, Article 25 should be repealed in its entirety.
    - *Duty to report:* the duty to report under Article 26 is both unnecessary and highly inappropriate. In particular, it is unclear how service providers are supposed to obtain "knowledge" of illegality, which they are not otherwise qualified to assess. Article 26 seems to proceed on the assumption that service providers should monitor their networks so as to obtain knowledge of criminality. This would be contrary to international standards on freedom of expression, which prohibit general monitoring.

Recommendations:

[55] See e.g. CJEU, C-293/12, *Digital Rights Ireland*, 08 April 2014

- Data retention requirements should be reviewed in line with international standards on privacy;
- Reference to the Minister in Article 24 (2) should be struck out and replaced by "court";
- An independent body should oversee the implementation of the surveillance regime established under the Proclamation;
- There should be annual reports on the number of surveillance operations, providing as much detail as is possible without undermining any ongoing investigations;
- Individuals who suspect that they have been subject to surveillance should have access to redress, either through court or to a specialised tribunal;
- The power to conduct raids without obtaining any independent authorisation in Article 25 should be repealed; and
- The duty to report cybercrimes under Article 26 should be repealed.

Evidentiary and procedural provisions

Part Four of the Act provides rules of evidence with relation to computer crimes under the Proclamation, and also provides for an additional regime of search and seizure. Articles 29-31 provide for any computer data to be seized by order of court; and Article 32 provides rules on the admissibility of computer-related materials, such as printouts of emails, as evidence. Article 33 provides that the person adducing evidence has the burden of proving its authenticity (for example, than a print-out of an email is genuine), and Article 34 provides further detail on proving the authenticity of electronic documents. Article 36, finally, provides that the burden of proof generally falls on the prosecution, but that, once basic facts have been established, the court may shift this burden to the defence.

As with the provisions of Part Three, the chief problem with the provisions of Part Four is that they provide for investigative powers in relation to 'crimes' that are so broadly defined that they include ordinary journalism. Again, this underscores the urgency of reforming the crimes created under the Proclamation; together with the various investigatory powers, they essentially lay down the framework for an extraordinary range of controls and powers, which are fundamentally inconsistent with international human rights standards.

As regards the detail of the provisions, they give broad investigatory powers to police, prosecutors and other agencies, who may issue orders requiring computer data to be preserved, regardless of whether the target of such an order is him or herself a suspect; courts are required to issue orders for the production of computer data without due process; and search warrants once issued in relation to one computer system may be 'recycled' to search other computer systems (Article 32(2)). Furthermore, investigative bodies may not only access data; they are also granted a power to make any data inaccessible, as well as require that passwords are handed over. These are all highly intrusive powers which, when used in tandem with the powers to raid media outlets and other entities suspected of 'computer crimes' are likely to violate international human rights law standards.

Finally, we note that under Article 36, the burden of proof may shift to the defence. This may violate international human rights standards on due process and we recommend that normal criminal procedure should not be departed from.

Recommendations:

- Articles 29-31 should be completely redrafted, incorporating the following principles:
  - Investigative powers should be required to only be used as proportionate;
  - Investigative authorities should be required to obtain a court order for any intrusive searches, seizures or other orders, and courts should apply due process principles in deciding on applications;

- Investigative authorities should not be allowed to delete content or render it inaccessible;
- The burden of proof should rest firmly with the prosecution.

Roles of government entities and **"miscellaneous provisions"** (Parts 5 & 6)

Part Five of the Proclamation details the various agencies involved in the prevention and detection of computer crime. Police and public prosecutors are empowered to establish specialist units, and the Information Network Security Agency is required to establish an online computer crimes investigation system and "provide other necessary investigation technologies". Furthermore, a National Executing Task Force comprising the heads of the Ministry of Justice, the Federal Police Commission and other relevant bodies will be established in order to prevent and control computer crimes, to be led by the Minister of Justice. All crimes are to be prosecuted before the Federal High Court, indicating the high level of priority given to the prosecution of computer crimes.

Part Six provides various miscellaneous provisions. Article 41 empowers the Ministry of Justice to enter into international agreements in matters concerning computer crime, including for the exchange of information, joint investigations, extradition and similar matters. Article 42 provides that in sentencing, a court may order the suspension, confiscation or removal of any computer system, data or device or blockage of data processing service used in the perpetration of the offence and property may be confiscated. Article 43 repeals various previous legislative provisions, including the chapter of the criminal code that hitherto dealt with computer crime.

Most of the provisions in Parts Five and Six are procedural and we will not analyse them in depth. We note, however, that the Information Network Security Agency is likely to be a pivotal body in the investigation of offences, particularly through the powers it is given to not only provide 'back-up' but also carry out raids. We have already critiqued the operative provisions of the Proclamation in this regard and will not repeat that criticism here. We would note, however, that the Agency should be subject to specific transparency requirements and it should account to the relevant parliamentary bodies, including through annual reports as well as any oral evidence it may be called to give on the use of its powers.

We also note that the Ministry of Justice is empowered to engage in international cooperation. The Proclamation should explicitly require it to refuse to cooperate with any requests likely to violate human rights standards (for example, a request to cooperate in a prosecution that is politically motivated).

Recommendations

- The Information Network Security Agency, as a pivotal body in the investigation of computer crimes, should be subject to strict parliamentary scrutiny
- The Ministry of Justice should be required to refuse to cooperate with any requests for international cooperation likely to violate human rights standards

Annex: A Proclamation to provide for Computer Crimes

WHEREAS information and communication technology plays a vital role in the economic, social and political development of the country;

WHEREAS unless appropriate protection and security measures are taken, the utilization of information communication technology is vulnerable to various computer crimes and other security threats that can impede the overall development of the country and endanger individual rights;

WHEREAS the existing laws are not adequately tuned with the technological changes and are not sufficient to prevent, control, investigate and prosecute the suspects of computer crimes;

WHEREAS it has become necessary to incorporate new legal mechanisms and procedures in order to prevent, control, investigate and prosecute computer crimes and facilitate the collection of electronic evidences;

NOW, THEREFORE, in accordance with Article 55(1) of the Constitution of the Federal Democratic Republic of Ethiopia, it is hereby proclaimed as follows:

PART ONE – GENERAL

1. Short Title
This Proclamation may be cited as the "Computer Crime Proclamation No. —/2016".

2. Definitions
In this Proclamation unless the context otherwise requires:
1/ "data processing service" means the service of reception, storage, processing, emission, routing or transmission of data by means of computer system and includes networking services;
2/ "computer or computer system" means any software and the microchips technology based data processing, storage, analysis, dissemination and communication device or any device that is capable of performing logical, arithmetic or routing function and includes accessories of that device;
3/ "computer data" means any content data, traffic data, computer program, or any other subscriber information in a form suitable for processing by means of a computer system;
4/ "computer program" means a set of instructions or commands expressed in words, codes or schemes which are capable of causing a computer system to perform or achieve a particular task or result;
5/ "traffic data" means any computer generated data relating to a chain of communication by means of a computer system indicating the communication's origin, destination, route, time, date, duration, size or types of underlying service;
6/ "content data" means any computer data found in the form of audio, video, picture, arithmetic formula or any other form that conveys the essence, substance, meaning or purpose of a stored or transmitted computer data or computer communication;
7/ "network" means the interconnection of two or more computer systems by which data processing service can be provided or received;
8/ "computer data security" means the protection of a computer data from deleting, changing, and accessing by unauthorized person, compromising its confidentiality or any other damage;

9/ "access" means to communicate with, to enter in, store in, store data in, retrieve, or obtain data from, to view, to receive, move or copy data from a computer system, or otherwise make use of any data processing service thereof;
10/ "critical infrastructure" means a computer system, network or data where any of the crimes stipulated under article 3 to 6 of this proclamation, is committed against it, would have a considerable damage on public safety and the national interest;
11/ "interception" means real-time surveillance, recording, listening, acquisition, viewing, controlling or any other similar act of data processing service or computer data;
12/ "spam" means unsolicited e-mails transmitted to multiple electronic accounts at a time;
13/ "service provider" means a person who provides technical data processing or communication service or alternative infrastructure to users by means of computer system;
14/ "Ministry" or "Minister" means the Ministry or Minister of Justice, respectively;
15/ "Public Prosecution Department" means federal public prosecutor department legally vested with the power and function of prosecution or delegated regional state public prosecutor departments;
16/ "investigatory organ" mean a person legally invested with the power of investigation;
17/"regional state" means any state referred to in Article 47(1) of the Constitution of the Federal Democratic Republic of Ethiopia and for the purpose this Proclamation it includes Addis Ababa and Dire Dawa city administrations;
18/ "police" mean Federal Police or Regional State Police to whom the power of the Federal Police is delegated;
19/ "Agency" mean Information Network Security Agency;
20/ "person" means a physical or juridical person;
21/ any expression in the masculine gender includes the feminine.

PART TWO – COMPUTER CRIMES

SECTION ONE – CRIMES AGAINST COMPUTER SYSTEM AND COMPUTER DATA

3. Illegal Access

1/ Whosoever, without authorization or in excess of authorization, intentionally secures access to the whole or any part of computer system, computer data or network shall be punishable with simple imprisonment not exceeding three years or fine from Birr 30,000 to 50, 000 or both.
2/ Where the crime stipulated under sub-article (1) of this Article is committed against:
a) a computer system, computer data or network that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from three to five years and fine from Birr 30,000 to 50,000;
b) a critical infrastructure, the punishment shall be rigorous imprisonment from five to 10 years and fine from Birr 50,000 to 100,000.

4. Illegal Interception

1/ Whosoever, without authorization or in excess of authorization, intentionally intercepts non-public computer data or data processing service shall be punishable with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000.
2/ Where the crime stipulated under sub-article (1) of this Article is committed against:
a) a computer data or data processing service that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from five to 10 years and fine from Birr 50,000 to 100,000.
b) a critical infrastructure, the punishment shall be rigorous imprisonment from 10 to 15 years and fine from Birr 100,000 to 200,000.

5. Interference with Computer System
1/ Whosoever, without authorization or in excess of authorization, intentionally hinders, impairs, interrupts or disrupts the proper functioning of the whole or any part of computer system by inputting, transmitting, deleting or altering computer data shall be punishable with rigorous imprisonment from three years to five years and fine not exceeding Birr 50,000.
2/ where the crime stipulated under sub-article (1) of this Article is committed against:
a) a computer system that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from five to 10 years and fine from Birr 50,000 to 100,000;
b) a critical infrastructure, the punishment shall be rigorous imprisonment from 10 years to 20 years.

6. Causing Damage to Computer Data
1/ Whosoever, without authorization or in excess of authorization, intentionally alters, deletes, suppresses a computer data, renders it meaningless, useless or inaccessible to authorized users shall be punishable with rigorous imprisonment not exceeding three years and fine not exceeding Birr 30,000.
2/ Where the crime stipulated under sub-article (1) of this Article is committed against:
a) a computer data that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from three years to five years and fine from Birr 30,000 to 50,000;
b) a critical infrastructure, the punishment shall be rigorous imprisonment from five to 10 years and fine from Birr 50,000 to 100,000.

7. Criminal Acts Related to Usage of Computer Devices and Data
1/ Whosoever, knowing that it can cause damage to computer system, computer data or network, intentionally transmits any computer program exclusively designed or adapted for this purpose shall be punishable with simple imprisonment not exceeding five years or fine not exceeding Birr 50,000.
2/ Whosoever, knowing that it is to be used for the commission of unlawful act specified under Articles 3 to 6 of this Proclamation, intentionally imports, produces, offers for sale, distributes or makes available any computer device or computer program designed or adapted exclusively for the purpose of committing such crimes shall be punishable with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000.
3/ Whosoever possesses any computer devices or data specified under sub-article (1) or (2) of this Article with the intention to further the commission of any of the crimes specified under Articles 3 to 6 of this Proclamation shall be punishable with simple imprisonment not exceeding three years or fine from Birr 5,000 to 30, 000.
4/ Whosoever, without authorization or in excess of authorization, intentionally discloses or transfers any computer program, secret code, key, password or any other similar data for gaining access to a computer system, computer data or network shall be punishable with simple imprisonment not exceeding five years or in serious cases with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000.
5/ Where the crime stipulated under sub-article (4) of this Article is committed negligently, the punishment shall be simple imprisonment not exceeding one year and fine.

8. Aggravated Cases
Where the crime stipulated under Article 3 to 6 of this Proclamation is committed against a computer data or a computer system or network which is designated as top secret by the concerned body for military interest or international relation, and while the country is at a state of emergency or threat, the punishment shall be rigorous imprisonment from 15 to 25 years.

SECTION TWO – COMPUTER RELATED FORGERY, FRAUD AND THEFT

9. Computer Related Forgery
Whosoever falsifies a computer data, makes false computer data or makes use of such data to injure the rights or interests of another or to procure for himself or for another person any undue right or advantage shall be punishable with simple imprisonment not exceeding three years and fine not exceeding Birr 30,000 or in a serious cases with rigorous imprisonment not exceeding 10 years and fine from Birr 10,000 to 100,000.

10. Computer Related Fraud
1/ Whosoever fraudulently causes a person to act in a manner prejudicial to his rights or those of third person by distributing misleading computer data, misrepresenting his status, concealing facts which he had a duty to reveal or taking advantage of the person's erroneous beliefs, shall be punishable with rigorous imprisonment not exceeding five years and fine not exceeding Birr 50,000.
2/ Whosoever, with fraudulent intent of procuring any benefit for himself or for another person, causes economic loss to another person by any change, deletion or any other damage of computer data shall be punishable with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000 or in serious cases with rigorous imprisonment not exceeding 10 years and fine from Birr 10,000 to 100,000.

11. Electronic Identity Theft
Whosoever, with intent to commit criminal act specified under Article 10 of this Proclamation or for any other purpose produces, obtains, sales, possesses or transfers any data identifying electronic identity of another person without authorization of that person shall be punishable with simple imprisonment not exceeding five years or fine not exceeding Birr 50,000.

SECTION THREE – ILLEGAL CONTENT DATA

12. Obscene or Indecent Crimes Committed Against Minors
1/ Whosoever intentionally produces, transmits, sales, distributes, makes available or possesses without authorization any picture, poster, video or image through a computer system that depicts:
a) a minor engaged in sexually explicit conduct; or
b) a person appearing to be a minor engaged in sexually explicit conduct;
shall be punishable with rigorous imprisonment from three years to 10 years.
2/ Whosoever entices or solicits a minor for sexual explicit conduct by transmitting or sending erotic speeches, pictures, text messages or videos through computer system shall be punishable with rigorous imprisonment from five to 10 years.

13. Crimes against Liberty and Reputation of Persons
Whosoever intentionally:
1/ intimidates or threatens another person or his families with serious danger or injury by disseminating any writing, video, audio or any other image through a computer systems shall be punishable, with simple imprisonment not exceeding three years or in a serious cases with rigorous imprisonment not exceeding five years.
2/ causes fear, threat or psychological strain on another person by sending or by repeatedly transmitting information about the victim or his families through computer system or by keeping the victim's computer communication under surveillance shall be punishable with simple imprisonment not exceeding five years or in serious case with rigorous imprisonment not exceeding 10 years.

3/ disseminates any writing, video, audio or any other image through a computer system that is defamatory to the honor or reputation of another person shall be punishable, upon complaint, with simple imprisonment not exceeding three years or fine or both.

14. Crimes against Public Security
Without prejudice to the provisions Article 257 of the Criminal Code of the Federal Democratic Republic of Ethiopia, Whosoever intentionally disseminates through a computer system any written, video, audio or any other picture that incites fear, violence, chaos or conflict among people shall be punishable with rigorous imprisonment not exceeding three years.

15. Dissemination of Spam
1/ Whosoever, with intent to advertise or sell any product or service, disseminates messages to multiple e-mail addresses at a time shall be punishable with simple imprisonment not exceeding three years and fine or, in serious case, with rigorous imprisonment not exceeding five years and fine not exceeding Birr 50,000.
2/ Notwithstanding the provision of sub-article (1) of this Article, dissemination of commercial advertisement through email account shall not be punishable provided that:
a) there is prior consent from the recipient;
b) the primary purpose of the advertisement is to introduce customers with new products or services and the customers have willing; or
c) the advertisement contains valid identity and address of the sender, and valid and simple way for the recipient to reject or unsubscribe receipt of further advertisement from the same source.

16. Criminal Liability of Service Providers
A service provider shall be criminally liable in accordance with Articles 12 to 14, of this Proclamation for any illegal computer content data disseminated through its computer systems by third parties, if it has:
1/ directly involved in the dissemination or edition of the content data;
2/ upon obtaining actual knowledge that the content data is illegal, failed to take any measure to remove or to disable access to the content data; or
3/ failed to take appropriate measure to remove or to disable access to the content data upon obtaining notice from competent administrative authorities.

SECTION FOUR – OTHER OFFENCES

17. Failure to Cooperate and Hindrance of Investigation
Whosoever:
1/ fails to comply with the obligations provided for under sub-article (2) of Article 23, sub-article (6) of Article 24, sub-article (2) of Article 29, sub-article (2) of Article 30 or sub-article (4) of Article 31 of this Proclamation, shall be punishable with simple imprisonment not exceeding one year or fine;
2/ intentionally hinders the investigation process of computer crimes conducted pursuant to this Proclamation shall be punishable with rigorous imprisonment not exceeding five years and fine not exceeding Birr 50,000.

18. Criminal Act Stipulated in Other Laws
Where any crime other than those provided for under this Part is committed by means of a computer, the relevant law shall apply.
19. Concurrent Crimes
Where any of the criminal acts provided for under this Part has resulted in the commission of another crime punishable under any special law or criminal code, the relevant provision shall apply concurrently.

20. Penalty Imposed on Juridical Person
Notwithstanding sub-article (1), (3) and (4) of Article 90 of the Criminal Code of the Federal Democratic Republic of Ethiopia, where any offence stipulated under this Part is committed by juridical person,
1/ the penalty shall be fine from Birr 50,000 to 500,000 for a crime punishable with fine;
2/ when the penalty provided for is imprisonment, the penalty shall be:
a) a fine not exceeding 50,000 Birr for a crime punishable with simple imprisonment not exceeding three years,
b) a fine not exceeding 100,000 Birr for a crime punishable with simple imprisonment not exceeding five years,
c) a fine not exceeding 150,000 Birr for a crime punishable with rigorous imprisonment not exceeding five years,
d) a fine not exceeding 200,000 Birr for a crime punishable with rigorous imprisonment not exceeding 10 years,
e) a fine of up to the general maximum laid down in sub-article (1) of this Article for a crime punishable with rigorous imprisonment exceeding 10 years.
3/ Where fine is expressly provided as punishment for a crime, it shall be five fold.

PART THREE – PREVENTIVE AND INVESTIGATIVE MEASURES

21. General
1/ Computer crime prevention and investigation shall be conducted in accordance with the provisions of this Part.
2/ Without prejudice the provisions of this Part, for issues not clearly covered in this law, the provisions of the Criminal Code and other relevant laws shall be applicable to computer crimes.

22. Investigative Power
1/ The public prosecutor and police shall have joint power to investigate criminal acts provided for in this Proclamation. And the public prosecutor shall lead the investigation process.
2/ Where requested to support the investigation process, the Agency shall provide technical support, conduct analysis on collected information, and provide evidences if necessary.

23. Retention of Computer Data
1/ Without prejudice to any provision stipulated in other laws, any service provider shall retain the computer data disseminated through its computer systems or data relating to data processing or communication service for at least one year.
2/ The data shall be kept in secret unless a court or public prosecutor orders for disclosure.

24. Real-time Collection of Computer Data
Without prejudice special provisions stipulated under other laws,
1/ to prevent computer crimes and collect evidence related information, the investigatory organ may, request court warrant to intercept in real-time or conduct surveillance, on computer data, data processing service, or internet and other related communications of suspects, and the court shall decide and determine a relevant organ that could execute interception or surveillance as necessary.
2/ Sub-article (1) of this Article shall only be applicable when there is no other means readily available for collecting such data and this is approved and decided by the Minister.
3/ Notwithstanding the provisions of sub-article (1) and (2) of this Article, the Minister may give permission to the investigatory organ to conduct interception or surveillance without court warrant where there are reasonable grounds and urgent cases to believe that a computer crime that can damage critical infrastructure is or to be committed.

4/ The Minister shall present the reasons for interception or surveillance without court warrant under sub-article (3) of this Article to the President of the Federal High Court within 48 hours, and the president shall give appropriate order immediately.
5/ Unless believed that it is necessary to conduct other criminal investigation, any irrelevant information collected pursuant to sub-articles (1) to (4) of this Article shall be destroyed immediately upon the decision of the Minister.
6/ Any service provider shall cooperate when requested to carry on activities specified under sub-articles (1) and (3) of this Article.
7/ Without prejudice sub-article (5) of this Article, any information collected in accordance with this Article shall be kept confidential.

25. Protection of Computer, Computer System or Infrastructure from Danger
1/ Where there are reasonable grounds to believe that a computer crime is to be committed and it is necessary to prevent and control the crime, provide early warning to citizens, to minimize the risks or for effectiveness of the investigation, the Agency in collaboration with the investigatory organ, may conduct sudden searches, conduct digital forensic investigation, provide appropriate security equipment or take other similar measures on computers, computer systems or infrastructures that are suspected to be attacked or deemed to be the sources of attack.
2/ For the implementation of the provision of sub-article (1) of this Article, as may be necessary and upon request, concerned organs shall have duty to cooperate.

26. Duty to Report
1/ Any service provider who has knowledge of the commission of the crimes stipulated in this Proclamation or dissemination of any illegal content data by third parties through the computer system it administers shall immediately notify the Agency, accordingly report to the police about the crime and take appropriate measures.
2/ The Agency may issue a directive as to the form and procedures of reporting.

27. Arrest and Detention
Without prejudice the provisions stipulated in special laws,
1/ where there are reasonable grounds to believe that a computer crime is committed or under commission, police may arrest suspects in accordance with the provisions of the Criminal Procedure Code.
2/ Where the investigation on the person arrested pursuant to sub-article (1) of this Article is not completed, remand may be granted in accordance with the provisions of the Criminal Procedure Code; provided, however, the overall remand period may not exceed four months.

PART FOUR – EVIDENTIARY AND PROCEDURAL PROVISIONS

28. General
1/ Computer crime proceedings and collection of evidence shall be conducted in accordance with the provisions of this Part.
2/ Without prejudice to the provisions of this Part, the General Part provisions of the Criminal Code and the Criminal Procedure Code shall be applicable to computer Crimes.

29. Order for Preservation of Computer Data

1/ Where there are reasonable grounds to believe that a computer data required for computer crime investigation is vulnerable to loss or modification, the investigatory organ may order, in writing, a person to preserve the specified data under his control or possession.
2/ The person ordered under sub-article (1) of this Article shall immediately take necessary measures to secure the specified computer data and preserve it for three months and keep such order confidential.

3/ The investigatory organ may order only a one-time extension for another three months up on the expiry of the period stipulated under sub-article (2) of this Article.

30. Order for Obtaining of Computer Data

1/ Where a computer data under any person's possession or control is reasonably required for purposes of a computer crime investigation, the investigatory organ may apply to the court to obtain or gain access to that computer data.
2/ If the court is satisfied, it may, without requiring the appearance of the person concerned, order the person who is in possession or control of the specified computer data, to produce it to the investigatory organ or give access to same.

31. Access, Search and Seizure

1/ Where it is necessary for computer crime investigation, the investigatory organ may, upon getting court warrant, search or access physically or virtually any computer system, network or computer data.
2/ Where the investigatory organ reasonably believes that the computer data sought is stored in another computer system and can be obtained by same computer system, the search or access may be extended to that other computer system without requesting separate search warrant.
3/ In the execution of search under sub-article (1) or (2) of this Article, the investigatory organ may:
a) seize any computer system or computer data;
b) make and retain a copy or photograph data obtained through search;
c) maintain the integrity of the relevant stored data by using any technology;
d) render inaccessible the stored data from the computer system on which search is conducted; or
e) recover deleted data.
4/ In the execution of search, the investigatory organ may order any person who has knowledge in the course of his duty about the functioning of the computer system or network or measures applied to protect the data therein to provide the necessary information or computer data that can facilitate the search or access.
5/ Where the investigatory organ finds the functioning of a computer system or computer data is in violation of the provisions this Proclamation or other relevant laws, it may request the court to order for such computer data or computer system to be rendered inaccessible or restricted or blocked. The court shall give the appropriate order within 48 hours after the request is presented.
6/ Where the search process on juridical person requires the presence of the manager or his agent, the investigatory organ shall take appropriate measure to do so.

32. Admissibility of Evidences

1/ Any document or a certified copy of the document or a certified printout of any electronic record relating to computer data seized in accordance with this Proclamation may be produced as evidence during court proceedings and shall be admissible.
2/ Without prejudice to the admissibility of evidences to be produced in accordance with the Criminal Procedure Code and other relevant laws, any digital or electronic evidence:
a) produced in accordance with this Proclamation; or
b) obtained from foreign law enforcement bodies shall be admissible in court of law in relation to computer crimes.

33. Authentication

Without prejudice to the authentication of written documents stipulated in other laws, any person who produces evidences provided under Article 32 of this Proclamation in a court proceeding has the burden to prove its authenticity.

34. Original Electronic Document
1/ Any electronic record which is obtained upon proof of the authenticity of the electronic records system or by which the data was recorded or stored shall be presumed original electronic document
2/ Without prejudice to sub-article (1) of this Article, the electronic printout which is obtained using a secured system under regular operation shall be considered original electronic evidence.
3/ Where the authenticity of an electronic record is not proved, any evidence that shows the following fact shall be admissible.
a) the computer system was operating properly or the fact of it's not operating properly did not affect the integrity of the electronic record; or
b) it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the other litigant party seeking to introduce it; or
c) it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

35. Presumption of Courts
When assessing the admissibility of evidence in accordance with this Proclamation, the court may have regard to the procedure, standard or manner in which a similar computer system is functioning.

36. Burden of proof
1/ Public prosecutor has the burden of proofing material facts regarding the cases brought to the court in accordance with the standards stipulated in law.
2/ Notwithstanding the provisions of sub-article (1) of this Article, upon proof of basic facts of the case by the public prosecutor if the court believes necessary to shift the burden of proofing to the accused, the court may do so.

PART FIVE – INSTITUTIONS THAT FOLLOW UP CASES OF COMPUTER CRIME

37. Public Prosecutor and Police Following up Cases of Computer Crime
1/ A public prosecutor or investigative officer empowered to follows up computer crime cases in accordance with the powers conferred by law shall have the responsibility to enforce and cause to enforce the provisions of this Proclamation.
2/ Public prosecution office and Police empowered in this Proclamation may organize separate specialized task units when necessary to follow-up computer crimes.

38. Duty of the Agency
The Agency shall have duty to establish online computer crimes investigation system and provide other necessary investigation technologies.

39. Jurisdiction
1/ The Federal High Court shall have first instance jurisdiction over computer crime stipulated under this Proclamation.
2/ The judicial jurisdictions stipulated under Article 13 and paragraph (b) of sub-article (1) of Article 17 of the Federal Democratic Republic of Ethiopia 2004 Criminal Code shall include computer crimes.

40. Establishment of Executing Task Force
1/ Without prejudice the power of the Agency to lead national cyber security operation as stipulated in other relevant laws, a National Executing Task Force comprising the heads of the

Ministry of Justice, the Federal Police Commission and other relevant bodies shall be established in order to prevent and control computer crimes.
2/ The Minister of Ministry of Justice shall lead the Executing Task Force, identify other relevant organizations to be incorporated in the Task Force and ensure their representation.
3/ The Task Force shall, for the prevention and control computer crimes, develop national discussion forum, discuss on occasional dangers materialized and provide recommendation thereof, design short and long-term plans to be performed by the respective institutions as well as put in place synchronized system by coordinating various relevant organs.

PART SIX – MISCELLANEOUS PROVISIONS

41. International Cooperation

1/ The Ministry of Justice shall cooperate and may sign agreements with the competent authority of another country in matters concerning computer crime, including the exchange of information, joint investigations, extradition and other assistances in accordance with this Proclamation and agreements to which Ethiopia is a party and within the limits of the country's legal system.
2/ For the implementation of this Proclamation, the investigatory organ, when necessary, may exchange information, perform joint cooperation in other forms or sign agreement with institutions of another country having similar mission.
3/ Any information or evidence obtained pursuant to this Article shall apply for the purpose of prevention or investigation of computer crimes.

42. Suspension, Confiscation or Blockage of Computer System or Asset

1/ The court, in sentencing an offender under this Proclamation, may give additional order for the suspension, confiscation or removal of any computer system, data or device or blockage of data processing service used in the perpetration of the offence.
2/ The property or proceedings of the accused that he directly or indirectly acquired through the computer crime for which he has been convicted shall be confiscate if the accused is convicted through a final decision;
3/ Unless they are contradictory to the provisions of this Proclamation, the relevant provisions of the Revised Anti-Corruption Special Procedure and Rules of Evidence Proclamation No. 434/2005 (as amended) shall be applicable with respect to restraining or forfeiture order of computer system, data, equipment or other assets.

43. Repeal and Inapplicable Laws

1/ Articles 706 to 711 of the Criminal Code of the Federal Democratic Republic of Ethiopia and article 5 of Telecom Fraud Offence proclamation no. 761/2012 are hereby repealed.
2/ No proclamation, regulations, directives or practices shall, in so far as they are inconsistent with this Proclamation, be applicable with respect to matters provided for by this Proclamation.

44. Effective Date

This Proclamation shall enter into force on the date of its publication in the Federal Negarit Gazeta