COMPUTER LAW & SECURITY REVIEW ■■ (2016) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Comment

# Ethiopia's new cybercrime legislation: Some reflections

*Kinfe Micheal Yilma* *

*Center for Media and Communications Law, Melbourne Law School, The University of Melbourne, Carlton, VIC, Australia*

*Keywords:*
Cybercrime
Computer crime
The right to privacy
Illegal content
Procedural justice
Ethiopia
Africa

ABSTRACT

Ethiopia has been enacting various pieces of legislation to regulate some aspects of the digital environment. The cybercrime proclamation of 2016 is the most recent addition to the statute book that criminalizes a range of cybercrimes. It has also introduced a number of novel evidentiary and procedural rules that will assist in the investigation and prosecution of cybercrimes. The law has, however, attracted criticisms from various corners mainly owing to some of its human rights unfriendly provisions. This comment provides brief analysis of the cybercrime legislation and highlights some of the challenges that lie ahead in the course of putting the law into practice.



## 1. Background

Ethiopia introduced the first set of cybercrime rules with the enactment of the Criminal Code in 2004. The Code had criminalized a set of three cybercrimes namely 'hacking', 'dissemination of malware' and 'denial of service attacks (DoS)'.[1] Several cybercrimes have been perpetrated against the Ethiopian cyberspace since the enactment of the computer crimes rules but there currently are only a few reported court cases.[2] In 2013, Ethiopia's cyber command – Information Network Security Agency (INSA) – released draft comprehensive cybercrime legislation that not only extended the range of outlawed cybercrimes but also introduced crucial evidentiary and procedural rules for the investigation and prosecution of cybercrimes.[3]

After three years of hiatus – and new drafting (or redrafting) role assumed by the Office of the Federal Attorney General (the Attorney General) – formerly called Ministry of Justice, the second version of the Bill has been adopted by the Council of Ministers in March 2016. The Bill was subsequently transmitted to the Ethiopian Parliament where it was discussed for an

* Center for Media and Communications Law, Melbourne Law School, The University of Melbourne, 185 Pelham St., Carlton, VIC 3053, Australia; School of Law, Addis Ababa University, Ethiopia.
*E-mail addresses:* kdesta@student.unimelb.edu.au, kinfeyilma@gmail.com.

http://dx.doi.org/10.1016/j.clsr.2016.11.016



[1] See Criminal Code of the Federal Democratic Republic of Ethiopia, *Federal Negarit Gazeta*, Proclamation No. 414/2004, Arts 706–711.

[2] For a discussion on major cybercrime incidents in Ethiopia until mid-2014, see Kinfe Micheal Yilma, 'Developments in Cybercrime Law and Practice in Ethiopia', (2014) 30 CLSR 720, 725–729. On a recent cybercrime case adjudged by Ethiopian courts, see Kinfe Micheal Yilma and Halefom Hailu Abraha, 'The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce and the New Media', (2015) 9 MLR 108, 110–111.

[3] See *A Proclamation to Legislate, Prevent and Control Computer Crime* (Draft), Version 1.0, 2013 (On file with author).

Please cite this article in press as: Kinfe Micheal Yilma, Ethiopia's new cybercrime legislation: Some reflections, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.11.016

unusually long time.[4] The second version of the Bill was, by and large, similar in content, in terms of its substantive and procedural provisions to the initial version save some new provisions, minor structural and linguistic changes.

The Legal and Governance Affairs Standing Committee of the Parliament held a public consultation with stakeholders, including relevant government agencies, academic institutions and members of the general public. The Ethiopian Parliament finally adopted the law in early June 2016 and it has since been published in the official law gazette.[5] Despite reform suggestions put forward during the initial draft stage, some provisions have caused concern, particularly those that encroach on constitutionally guaranteed rights. It has, as a result, attracted widespread attention from various commentators after the second version was unveiled. Numerous news reports, commentaries and editorials have been written about the law, most of which have highlighted its impact on human rights such as privacy and freedom of expression.[6] Global civil society organizations have also released reports regarding the law, before and after its enactment, emphasizing these issues.[7]

## 2. An overview of the new cybercrime law

The cybercrime law recently endorsed by the Ethiopian Parliament has emerged with some changes to the initial versions of the law. The new law is presented in more detail, unlike the truncated nature of the initial draft, which generally worked against requirements of precision in legislative drafting. Precision is a desirable virtue of legal provisions as it mitigates problems when it comes to judicial interpretation of the rules. In this sense, it is submitted that the present cybercrime law has sacrificed precision for the sake of ensuring clarity, by framing provisions in an excessively detailed manner.

A major shift in the new law concerns the reshuffling of the institutional arrangement in the investigation and prosecution of cybercrimes. Following a shift in responsibility for the drafting exercise from INSA to the Federal Attorney General, the law now identifies the latter as the principal implementing body.[8] Unlike the leading enforcement role assumed by INSA and the Federal Police under the initial draft, the Attorney General, who drafted the second version of the law, has now become the principal enforcer. INSA's role has largely been relegated to the provision of technical support in the course of cybercrime investigations and prosecution by the Attorney General.[9] The only scenario where INSA would have some investigatory power, as shall be seen below, is with regard to sudden searches and digital forensic investigations for preventive purposes.

In terms of substantive criminal rules, the law maintains almost all provisions on cybercrime incorporated both in the initial and second versions. This appears to have produced some replication of crimes within the law. An example, in this regard, is the crime of 'causing damage to computer data' – or commonly referred to as 'spreading malware'.[10] A crime of almost an identical sort is provided in Art 7(1) of the law which is captioned as 'criminal acts related to usage of computer devices and data'. All the remaining sub-articles of Art 7 deal with what are normally called 'acts committed to facilitate the commission of cybercrimes.'[11] The same problem of unnecessary replication is discernible with respect to the 'crime against liberty and reputation of persons' where the first two sub-articles are essentially redundant.[12]

Redundancies are also present when one looks across other pieces of legislation. A case in point is 'cyber-terrorism' which Ethiopia's controversial Anti-terrorism law already outlaws. This again is essentially replicated under the heading of 'crime against public security' within the cybercrime law.[13]

The provision partially reads:

> whosoever intentionally disseminates through a computer system any written, video, audio or any other picture that incites violence, chaos or conflict among people shall be punishable with rigorous imprisonment not exceeding three years.

The only imaginable difference between this proviso and that of anti-terror legislation is that terrorist acts must be guided by a certain political, religious or ideological cause. However, the crime against publicity is still couched in neutral terms such that it might well embrace cyber-terrorist acts: i.e. all acts that incite violence, chaos or conflict with or without some political, religious or ideological cause are potentially punishable under the cybercrime legislation.

The law also creates a new cybercrime scenario of 'aggravated cases' when cybercrimes are committed against 'top secret' military or foreign policy computer data, systems or networks at a time when the nation is in a state of emergency

[4] See *A Proclamation to Provide for Computer Crime* (Draft), Version 2.0, 2016 (On file with author).

[5] See Computer Crime Proclamation, *Federal Negarit Gazeta*, Proclamation No. 958/2016.

[6] See, for instance, Yonas Abiye, 'Controversial cybercrime draft proclamation tabled for approval', *The Reporter* (Addis Ababa, 16 April 2016); New computer crime law hinders vibrant online discourse, *Addis Fortune* (Addis Ababa, 24 April 2016); Kinfe Micheal Yilma, 'Troubling aspects of Ethiopia's cybercrime Bill' *The Reporter* (Addis Ababa, 16 April 2016); Alemayehu Gebremariam, 'State terrorism and computer crime in Ethiopia', *Ethiopian Review* (California, 30 May 2016); Solomon Goshu, 'The computer crime law: another inroad on human rights?', *The Reporter* (30 April 2016); Kinfe Micheal Yilma, 'Ethiopia's new cybercrime legislation: Government heard but only partially', (*The Reporter*, 11 June 2016).

[7] See, for instance, 'Ethiopia: Computer Crime Proclamation – A Legal Analysis' (*Article 19*, July 2016) available at <https://goo.gl/azy3BP>; Kimberly Larcson, 'Ethiopia's new cybercrime law allows for more efficient and systematic prosecution of online speech' (*Electronic Frontier Foundation*, 9 June 2016), available at <https://goo.gl/RJaAfq> (Last accessed on 15 October 2016).

[8] See *Computer Crime Proclamation*, supra n 5, Arts 22–25, 30–31, 38.

[9] *Ibid*, Arts 23 and 39.

[10] *Ibid*, Art 6.

[11] *Ibid*, Art 7(2–4).

[12] *Ibid*, Art 13.

[13] *Ibid*, Art 14; *Cf*, Anti-terrorism Proclamation, *Federal Negarit Gazeta*, Proclamation No. 652/2009, Art 3(6) cum Art 2(7).

Please cite this article in press as: Kinfe Micheal Yilma, Ethiopia's new cybercrime legislation: Some reflections, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.11.016