Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

# Developments in cybercrime law and practice in Ethiopia

*Kinfe Micheal Yilma*[*]

*Hawassa University, School of Law, Ethiopia*

*Keywords:*
Computer crime
Cybercrime
Criminal code
Draft computer crime law
Cybersecurity
Ethiopia

ABSTRACT

With increasing access to information and communication technologies such as the Internet, Ethiopia has recently taken responsive legislative measures. One such legislative measure is enactment of cybercrime rules as part of the Criminal Code of 2004. These rules penalize three items of computer crimes namely hacking, dissemination of malware and denial of service attacks. The cybercrime rules are however slightly outdated due to changes that have occurred in the field of cybercrime since the enactment of the Code. The surge of new varieties of cybercrimes previously uncovered under the Code and the need to legislate tailored evidentiary and procedural rules for investigation and prosecution of cybercrimes have recently prompted the Ethiopian government to draft modern and comprehensive cybercrime legislation, but the draft law still needs further work on cybercrimes in light of other major legislative developments at regional and national levels. This article closely examines major developments in cybercrime law and practice in Ethiopia since the enactment of the first set of cybercrime rules and proffers recommendations towards a unified cybercrime regime.



## 1. Introduction

Ethiopia is amongst countries with the lowest level of Internet penetration and use. A 2012 World Internet Stats data, for instance, claims that Ethiopia has had only 1.1% Internet penetration.[1] Similarly, the World Economic Forum also rates the number of Internet users in Ethiopia at 1.1%, ranking 142 out of 144 countries.[2] Recent data released by the Ethiopian government claims that the level of Internet penetration has reached 5.5% as of December 31, 2013.[3] This delay in the proliferation of the Internet has partly played a role in delaying legislative measures in the field, cybercrime included. It was only in 2004 that Ethiopia enacted the first set of cybercrime rules with the adoption of the Criminal Code. The Code penalizes a short list of computer crimes most notably computer hacking, spreading malware and denial of service (DoS) attacks. Dozens of cybercrimes have been committed in Ethiopia since the enactment of the Code, but there currently are no reported court cases where cybercrime rules of the Code are applied.

* Lecturer-in-Law, Hawassa University, School of Law, P.O. Box 2204, Hawassa, Ethiopia.
E-mail addresses: kinfeyilma@gmail.com, kinfey@hu.edu.et.

[1] See World Internet Stats (2012) *World Internet Usage and Population Statistics*. Available from: http://www.internetworldstats.com/africa.htm#et. [Accessed on 1 July 2014].

[2] See Schwab, K. (ed.) (2012) *The Global Competitiveness Report 2012–2013*, Full Data Edition, The World Economic Forum, 491.

[3] See Ethiopian Ministry of Communication and Information Technology (2014) *Communication and Information Technology Statistical Bulletin*, 1(1), 7.

http://dx.doi.org/10.1016/j.clsr.2014.09.010
0267-3649/

Convinced that existing computer crime rules are inadequate and to address ever evolving cybercrime behaviour, the Ethiopian government has recently drafted new legislation. The limitations of the Code are mainly threefold. Primarily, the Code criminalizes only three items of cybercrimes and hence does not address new crime committed against or through computers. In addition to common forms of cybercrime such as hacking, spreading malware and DoS attacks, a range of new cybercrimes have already emerged in the wake of the enactment of the Code. This is said to have rendered these rules inadequate in the wake of economic, social and political risks posed by cyber-attacks.[4] Related to this, recent digitization efforts and expansion of information and communications technology (ICT) infrastructure meant higher vulnerability to cyber threats which could not adequately be addressed by the narrowly defined rules of the Criminal Code.[5] Secondly, the computer crime rules of the Code do not provide tailored procedural and evidentiary provisions that would be necessary in the investigation and prosecution of such offences.[6] As the Code currently stands, the basic rules of criminal procedure, enacted as far back as 1961, continue to apply to computer crime regulation. Worse still, Ethiopia has never introduced evidence law proper other than a set of rules scattered across various pieces of legislation. It goes without saying that such procedural and evidentiary rules are too outdated to be applied to the cybercrime given the peculiarity and novelty of these online crimes. Thirdly, the cybercrime rules of the Code were not crafted to take full account of the cross-border nature of this form of criminal behaviour and the need for international cooperation in the prevention, investigation and prosecution of cybercrime.[7] Indeed, post enactment of the Code saw formation of international as well as regional treaties on cybercrime. This in turn required Ethiopia to adopt the requisite legal framework as part of the regional and global efforts against cybercrime.[8]

Owing to these limitations of the computer crime rules of the Code, the Ethiopian government has recently crafted a relatively comprehensive and modern cybercrime law. Whilst the draft law embodies quite commendable provisions that are meant to deal with the ever dynamic field of cybercrime, it is yet to be reworked and enriched with the rich experiences of other jurisdictions and benchmark international instruments. Of all global cybercrime instruments, one clearly sees marks of the Council of Europe (CoE) Cybercrime Convention in most parts of the draft legislation. The draft legislation nevertheless has a lot lessons to take before it is officially passed by the Ethiopian legislature. It must particularly be revisited in light of other legislative developments in the Ethiopian legal regime such as telecom fraud offence law, advertisement law and copyright law as well as regional legislative initiatives such as the African Union (AU) Convention on Confidence and Security in Cyberspace which, among others, covers cybercrime.

This article examines the salient features of the Ethiopian legal regime governing cybercrimes. With a view to provide some background to readers, it discusses the extant policy, legal and institutional framework of cybersecurity in general and cybercrime in particular. It then closely examines the computer crime rules of the Ethiopian Criminal Code of 2004 along with major cybercrime incidents that have occurred since their adoption. The article further considers major reforms that the draft law of 2013 envisages and offers recommendations towards a unified cybercrime regime for Ethiopia.

### 1.1. *Cybercrime law and policy making in Ethiopia*

Policy and law making powers in Ethiopia follow the federal arrangement that were reintroduced in 1991. The federal Constitution of the 1995 devolves legislative powers between the federal government and the nine regional states. The Constitution bestows upon the federal legislature the primary legislative power to enact a penal code while allowing states to enact penal laws on 'matters' that are not specifically covered by the federal penal legislation.[9] While the federal government retains the primary law making power in criminal matters, states' power is rather residual. In other words, states may issue penal legislation only on matters that are not covered by the Federal Penal Code. In line with this constitutional proviso, the federal legislature enacted a comprehensive Criminal Code in 2004 that incorporates 'computer crime' rules.[10]

What flows from the constitutional division of penal law making powers is that states apparently have no constitutional mandate to issue cybercrime law. This is precisely because the subject matter – i.e. computer crime – is specifically covered under the federal Criminal Code, no matter how narrow the Code is in its list of cybercrimes. States, according to this reading of the Constitution, cannot introduce new varieties of cybercrime taking their objective conditions into account. Should there be a need to broaden the scope of the cybercrime regime, it is the federal legislator that has the power to do so as it retains jurisdiction over computer crime because it has already dealt with the 'subject matter' under existing law.

Further reading of the Ethiopian Constitution suggests that state cybercrime law making power is framed in such a

[4] See Explanatory Note to the Draft Computer Crime Proclamation, July 2013, 2 (Amharic: Translation Mine) [On file with the author]. See also Preamble of the Proclamation to Legislate, Prevent and Control Computer Crime, Draft, 2013, para 3. [On file with the author].

[5] *Ibid*, 4.

[6] *Ibid*, 3. See also the preamble of the draft computer crime law, para 4.

[7] *Ibid*.

[8] *Ibid*.

[9] See Constitution of the Federal Democratic Republic of Ethiopia, *Federal Negarit Gazeta*, Proclamation No. 1/1995, Art 55(5).

[10] See Criminal Code of the Federal Democratic Republic of Ethiopia, *Federal Negarit Gazeta*, Proclamation No. 414/2004. Ethiopia had its first penal code in 1930 – the Penal Code of the Empire of Ethiopia. This penal code was later replaced by the Penal Code of the Empire of Ethiopia – Proclamation No. 158/1957 – which in turn was partly supplemented by Revised Special Penal Code of the Provisional Administration Council – Proclamation No. 214/1982. None of the previous penal codes regulated cybercrimes. The Telecom Fraud Offense law is another most recent legislation, which partly touches upon aspects of cybercrime, issued by the federal parliament. See Telecom Fraud Offense Proclamation, *Federal Negarit Gazeta*, Proclamation No. 761/2012.