Cybercrime Lawmaking and Human Rights in Ethiopia

Kinfe Micheal Yilma ♣

Abstract

Ethiopia has embarked upon an ambitious project of revising a number of laws with a view to entrench human rights and democratic governance. Part of this legal reform program has been the revision of Computer Crime Proclamation No 958/2016. This article examines key aspects of the Draft Computer Crime Proclamation prepared by the Media Law Working Group from a human rights perspective. As it shall be shown in this article, making the cybercrime legal regime human rights friendly has been the overarching objective of the revision project. Most human rights concerns associated with the current cybercrime legislation are, as a result, rectified in the cybercrime Bill. However, the Bill goes overboard in embracing themes that go well beyond the scope of cybercrime legislation. With respect to the overall revision process, the article submits that the process has not been sufficiently inclusive.

Key terms:

Cybercrime · Computer crime · Human rights · Digital rights · Lawmaking · Legitimacy

DOI http://dx.doi.org/10.4314/mlr.v15i1.3

Received: 25 March 2021 **Accepted**: 28 July 2021

Suggested citation:

Kinfe Micheal Yilma (2021), 'Cybercrime Lawmaking and Human Rights in Ethiopia', 15 *Mizan Law Review* 1: 73-106

♣ Kinfe Micheal Yilma (PhD), Assistant professor of law at Addis Ababa University School of Law. Email: kinfeyilma@gmail.com
ORCID: https://orcid.org/0000-0003-2514-0491

The author gratefully thanks Halefom Hailu Abraha and the two anonymous reviewers for feedback on the earlier versions of this article. An earlier version of this article was presented at a consultative workshop convened by Lawyers for Human Rights –Ethiopia, at Sapphire Addis Hotel on 29 December 2020.

1. Introduction

While Ethiopia remains to be one of the least-connected countries in the world,[1] it has taken progressive policy measures over the past two decades to regulate the Internet. Ethiopia adopted its first Information and Communication Technology (ICT) Policy in 2002, which has since been revised in 2009 and 2016. The Digital Transformation Strategy of 2020 is the more recent iteration in Ethiopia's ICT policymaking. These policy iterations have gradually been translated into a range of laws. So far, a handful of Internet laws have been adopted including laws dealing with cybercrime, telecom fraud, e-transactions, disinformation and hate speech online, and many others are in the pipeline such as data protection law. But such efforts of making the Ethiopian legal regime fit for purpose in the digital era often sought to marshal ICTs towards achieving the nation's socio-economic development objectives.

Yet, the impact of enacting new Internet laws in the enjoyment of human rights often receive little attention. Stated differently, concern for human rights often took the backseat in Ethiopia's attempts at making its legal framework fit for purpose in the digital age. In part, this has to do with the lack of room for civil society groups working in the human rights field during the preparation of draft pieces of legislation as well as the tendency to rush bills for legislative imprimatur without sufficient stakeholder consultation.[2]

Frequently used acronyms:

CARD	Center for the Advancement of Rights and Democracy in Ethiopia
CoE	Council of Europe
INSA	Information Network Security Agency
NDRE	Network for Digital Rights in Ethiopia
NISS	National Intelligence and Security Service
TFO	Telecom Fraud Offence

[1] According to data from Internet World Stats, the level of Internet penetration as of December 2020 has been around 18%. *See* details at <https://www.internetworldstats.com/africa.htm#et>. At the time of writing, Ethio-telecom reports that it has close to 55 million mobile service subscribers and over 25 million data and Internet users but these statistics do not reflect the level of Internet penetration in Ethiopia. *See* <https://www.ethiotelecom.et/> (Last accessed 31 July 2021).

[2] For more on trends in Internet lawmaking in Ethiopia, *see* Kinfe Micheal Yilma (2020), Between Regulatory Reticence & Legislative Rush: Internet Lawmaking in Ethiopia KM Yilma (ed) *The Internet and Policy Responses in Ethiopia: New Beginnings and Uncertainties* (International Law Series, Vol. IV) 1-10.

This era of little concern for human rights in lawmaking appears to be changing. Ethiopia has embarked on an ambitious project of reforming the nation's various laws since the mid-2018. Under the auspices of the Justice and Legal Affairs Advisory Council,[3] the reform concerned primarily revising a number of existing laws and drafting a few new pieces of legislation. But unlike past reform initiatives, human rights seem to have taken center-stage in the ongoing legal reform program. Much of the reform work seeks to bring laws, including the Anti-Terrorism and Computer Crime Proclamations, in line with international and human rights standards. But this is not entirely surprising in light of the fact the post-2018 legal reform program came against the backdrop of serious allegations of human rights violation by the government, including through the instrumentality of the law.

Against this background, this article examines the revision of Computer Crime Proclamation No 958/2016 from a human rights perspective. Based on a closer investigation of the Draft Computer Crime Proclamation (2020, alternatively referred to as 'cybercrime Bill' in this article), it considers new changes introduced in the cybercrime Bill and the overall process of the revision project. The remainder of the article develops in four sections. Section 2 discusses the place accorded to 'digital rights' in the post-2018 legal reform program.

In Section 3, a brief history of cybercrime lawmaking in Ethiopia from 2004 to 2016 is outlined to provide a background to the current reform effort. Section 4 considers the way in which the current cybercrime legislation infringes a set of human rights. Section 5 examines the initiative to revise Proclamation No 958/2016, including key changes introduced in the Draft Computer Crime Proclamation and the overall revision process. Section 6 closes with some observations and suggestions. For the sake of convenience, the terms cybercrime and computer crime are alternatively used throughout this article.

2. Post-2018 Reforms and 'Digital Rights' in Ethiopia

Ethiopia's human rights record has been dismal for decades. Despite having a Constitution – a third of which constituting a bill of rights, the government has constantly been accused of rights violations, stifling dissent and failing to hold free, fair and democratic elections. Its poor human rights record was especially manifested in its persistent (ab)use or overuse of laws to prosecute

[3] Federal Attorney General, Legal and Justice Affairs Advisory Council Establishment Directive No 24/2010.

journalists and rights advocates. Some of the high-profile prosecutions of rights activists even concerned alleged training on and use of digital security tools.[4] Such aggressive measures may have played a significant role in the underdevelopment of a vibrant digital rights space in Ethiopia. But the unpleasant 'authoritarian' label has long overshadowed the economic achievements of the government.

With the reshuffle in government after persistent public protests in mid-2018, a glamour of hope that a new era of rights protection and building of democratic institutions flickered. From a digital rights perspective, a number of measures taken in the wake of the change in administration projected a new era of human rights, including in the digital context. One such measure has been the unblocking of hundreds of websites and promises of ending arbitrary gateway measures such as website blocking, Internet filtering and throttling as well as network shutdowns. A 2017 joint report of Amnesty International and Open Observatory of Network Interference documents that Ethiopia notoriously blocked dozens of websites which, according to the government, disseminate content deemed objectionable for social, political and security reasons.[5]

In the aftermath of the much-touted reform, most of these websites were unblocked.[6] Such measures have had an impact in nudging civil society groups towards the digital rights space. In the past, non-governmental entities working in this field have also been few and far between. It is only recently that civil society groups with some interest in digital rights are emerging. A good case in point is the recently launched Network for Digital Rights in Ethiopia (NDRE), which operates within the auspices of the Center for the Advancement of Rights and Democracy in Ethiopia (CARD).[7] With the current government's ambition of bringing about digital transformation, concern for human rights online is likely to grow. Part of the series of pro-

[4] *See* Ethiopia: Free Zone 9 Bloggers, Journalists (Human Rights Watch, 13 April 2015) <https://bit.ly/2HIteTJ> (Last accessed on 20 January 2021).

[5] Ethiopia Offline: Evidence of Social Media Blocking and Internet Censorship in Ethiopia (Amnesty International and Open Observatory of Network Interference, 2017) <https://bit.ly/3iW20rj> (Last accessed on 20 January 2021).

[6] Ethiopia Allows Access to over 260 Websites (Committee to Protect Journalists, 22 June 2018) <https://bit.ly/2Fh4bG9> (Last accessed on 20 January 2021).

[7] *See* details about the Network here: <https://ndrethiopia.org> (Last accessed on 20 January 2021).

human rights measures were the release of journalists, including those prosecuted for expressing opinions through the use of online platforms.[8]

A key aspect of the post-2018 reform has been large-scale revision of laws often thought to have been instruments of repression and human rights violation. As part of this law and justice reform program, a number of new draft laws meant to uphold human rights and broaden the democratic space have been drafted. And some of these laws are already enacted such as the Ant-terrorism, Media and Civil Society Organizations Proclamations. Other pro-human rights bills in the offing include draft laws on access to information, freedom of assembly and cybercrime.[9]

As shall be highlighted in the next section, the current cybercrime legislation contains provisions that unreasonably interfere with and restrict fundamental human rights such as the right to privacy, freedom of expression and due process guarantees. As part of the legal reform program, a new Bill that seeks to remedy the current cybercrime law has been introduced. The Draft Computer Crime Proclamation embodies new substantive criminal provisions. But as shall be considered in Section 5, it particularly goes a long way in addressing human rights concerns surrounding the extant law.

Along with other upcoming Bills, the revision of the cybercrime legislation holds a promise of enhancing the protection of digital rights in Ethiopia. But more importantly, the active consideration of this Bill by stakeholders as well as the government would help to push back against the apparent backtracking in the government commitment to and pledge for democratic reforms and human rights protection. In stark and quick regression, the government has returned to its habit of arbitrary and unlawful network disruptions in the past few months. For over eight months, Internet and telecom services as well as electricity remain disrupted in most parts of the Tigray regional state where there has been an ongoing conflict since early November 2020.[10] In parts of Oromia region –where there is also a lingering conflict, network disruptions

[8] Ethiopia Frees Politician Jailed over 2015 Facebook Posts (Africa News, 5 March 2018) <https://bit.ly/38ZZhtg> (Last accessed on 20 January 2021). [Note that the release was immediately before the reshuffle in government but part of the pledge by the then governing party to open up the democratic space].

[9] *See* details on the website of the Advisory Council at: <http://www.ljaac.gov.et/About/WorkingGroups#firstContent> (Last accessed on 20 January 2021).

[10] *See* #KeepItOn in Tigray: Ethiopia Must Lift the Blackout from Conflict Zone (Access Now, 29 July 2021) < https://bit.ly/3rIHMWh> (Last accessed on 31 July 2021).

were reportedly in place for over a year.[11] And this is on top of recurrent Internet shutdowns taken to curb disinformation in the wake of political assassinations, among other trigger factors.[12]

Problematic about this regressive practice is that no clear legal basis exists for network disruptions.[13] Often, the government presents unpersuasive defences for its opaque shutdown practices. One recalls here the claim that since the Internet is neither water nor air, and therefore, it may be shut when the government deems there is a threat to national security.[14] But more recently, the Office of the Federal Attorney General incidentally offered a legal justification of sorts for Internet shutdowns in its formal comments on a report of the UN Special Rapporteur on Freedom of Opinion and Expression that criticized government shutdown practices.[15] The Attorney General notes that the 2013 law which re-established the Information Network Security Agency (INSA) empowers the Agency to 'keep the country safe from any threats against national security and it can take measures when the necessity arises'.[16]

According to the Attorney General, this law provides a legal basis for Internet shutdowns. But a closer look at this law does not support this claim. Nowhere in this law the Agency's power of cutting Internet access for national security purposes is either explicitly stated or remotely implied. Regressive and worrisome is not just the frequent resort to network disruptions but also the tendency to invoke vague and impertinent laws to justify the measures. Perhaps, one frontier to push back against the regression in reforms as well as to push forward with advancing digital rights causes in Ethiopia is the revision of the cybercrime law. As alluded to above, its central goal of humanizing –

---

[11] *See* Ethiopia: Communications Shutdown Takes Heavy Toll: Restore Internet, Phone Services in Oromia (Human Rights Watch, 9 March 2020) <https://bit.ly/3aNihM3> (Last accessed on 31 July 2021).

[12] *See*, for example, Ethiopia's Government Shut down the Entire Country's Internet (Business Insider, 7 February 2020) <https://bit.ly/2PsfpwW> (Last accessed on 31 July 2021).

[13] For more on the proliferation of network disruptions in Ethiopia and its legality, *see* generally Kinfe Micheal Yilma, *Network Disruptions and the Law in Ethiopia: A Legal Guide* (Internews Network, July 2021).

[14] Twitter Backlash after Ethiopia PM's Internet 'Not Water or Air' Threat (Africa News, 3 August 2019) <https://bit.ly/3bF0ia2> (Last accessed on 20 January 2021).

[15] Report of the UN Special Rapporteur on the Promotion and Protection of Freedom of Opinion and Expression, David Kaye (29 April 2020) Paras 51-52.

[16] Comments by the State on the Report of the UN Special Rapporteur on the Promotion and Protection of the Freedom of Opinion and Expression on His Visit to Ethiopia (15 April 2020), Para 20.

perhaps over-humanizing– cybercrime investigation and prosecution lends weight to the budding fight for digital rights in Ethiopia.

3. Development of Cybercrime Law in Ethiopia (2004-2016)

This section provides a brief historical account of cybercrime lawmaking in Ethiopia. From the first set of cybercrime rules of the Criminal Code to the currently in force Proclamation No 958/2016 and several drafts introduced in the interim, it highlights key developments in cybercrime lawmaking in Ethiopia between 2004 and 2016. As shall become clear, Ethiopia introduced a relatively modern and comprehensive cybercrime legislation with the adoption of Proclamation No 958/2016. But with this modern set of cybercrime rules come some provisions that give rise to human rights concerns, particularly on the right to privacy and freedom of expression. This point will be considered further in Section 4.

3.1 The Criminal Code

Ethiopia introduced the first set of cybercrime rules in 2004 with the adoption of the Criminal Code. The Code contained only three items of cybercrime; viz. 'illegal access of a computer, computer system or computer network'; 'causing damage to data' and 'disrupting use of computer services'.[17] Indeed, it also criminalized acts committed with the view to 'facilitate the commission of computer crime'.[18] There are two basic common threads among these rules. One is that all of the listed crimes, except the fourth one – i.e. adding and abetting commission of computer crime – are punishable when committed both intentionally and negligently.

Second, they are punishable when the perpetrator acted in the absence of any authorization to do so, or 'without authorization' as the law calls it. Notably, this feature does not apply to the fourth type of computer crime under the Code. That the law restricted its scope only when the act was committed 'without authorization' means that potentially punishable acts, but made just by 'exceeding authorization' already given, are not punishable under the Code. Also notable about the cybercrime rules under the Code is that they are all punishable, not only when perpetrated against a standalone computer, but also against a computer system and computer network. Nevertheless, the Code

[17] *See* Criminal Code Proclamation No 414/2004, *Federal Negarit Gazeta*, Arts 706, 707 and 708 respectively.
[18] *Id*. Art 709.

failed to provide definitions of technical terms such as 'computer system' and 'computer network'.

Rules of procedure and evidence applicable to other types of crimes – i.e. the existing Criminal Procedure Code[19] – did apply to cybercrimes because the Criminal Code does not envisage tailored evidentiary and procedural rules for cybercrimes. The Criminal Procedure Code was adopted half a century ago and offered no modern rules of procedure and evidence tailored to cybercrimes. But the Code is now slated to be replaced by a new legislation which seeks to provide a comprehensive set of rules of procedure and evidence for all types of crimes, including cybercrimes.[20] This would mean that the Draft Code of Criminal Procedure and Evidence would replace the special evidentiary and procedural rules of Computer Crime Proclamation No 958/2016. It is to be noted that the Draft Code would also repeal provisions dealing with jurisdiction and international cooperation.

With regard to crimes other than computer crimes discussed above, but provided under other provisions of the Code, the rules of computer crimes would not apply, but rather the relevant provisions of the Criminal Code shall be applicable.[21] For example, the commission of defamation through a computer or computer network or computer system is punishable under Title III, Chapter I and II, Arts 607-619 of the Criminal Code rather than the computer crime rules. This, in a way, defined the scope of the Code vis-à-vis computer crimes in that only when computers are 'targets' of the crime would the computer crime rules apply. And therefore, the two categories of cybercrime – 'tool cybercrimes' (where computers are used as a mere tool of commission of the crime) and 'computer-incidental cybercrimes' (where the use of computers in the commission of the crime is merely incidental) – were outside the scope of the computer crime rules of the Code.

Ethiopian criminal law also provided rules of concurrency that apply where a crime is committed by means of a computer but which also leads to a commission of another crime punishable under other provisions of the Criminal Code. Under these circumstances, Ethiopian law stipulated that both the computer crime rules and the other relevant provisions of the Code shall concurrently apply.[22] This provision may apply in the following scenario: a

[19] *See* Criminal Procedure Code Proclamation No 185/1961, *Negarit Gazeta*.

[20] Draft Criminal Procedure and Evidence Code (January 2021) Art 2(2(f)). And the proposed repeal would also apply to the Telecom Fraud Offence Proclamation which, as will be highlighted below, also criminalizes certain cybercrimes.

[21] Criminal Code, *supra* note 17, Art 710.

[22] *Id*. Art 711.

hacktivist or a whistle-blower hacks into a computer system of the Ethiopian armed forces and takes military secrets and later discloses or permits others to disclose them to the media. While the hacking provision of the Code would have applied in respect of unauthorized access, the disclosure of secret military documents is punishable under Title III, Chapter II, Art 336 of the Criminal Code. All that the rules of concurrence say, therefore, is that the criminal shall be punishable under both provisions of the Code, concurrently.

The Criminal Code was drafted by the former Ministry of Justice and the Justice and Legal System Research Institute.[23] With regard to computer crimes, the preparation of the Code was funded under ITU/EU co-funded project 'Support for Harmonization of the ICT Policies in Sub-Saharan Africa' (HIPSSA).[24] In its preface, the Code identifies – as one discernible gap in the 1957 Penal Code – the failure to properly address crimes born alongside advances in technology.[25] More particularly, the previous Code did not incorporate crimes such as computer crime, although this now attracts attention both in legislation, not only within national frontiers but also at the regional and international levels.[26] The 1957 Penal Code did not adequately address such crimes with the degree of seriousness they deserve.[27]

Background documents of the current Criminal Code state that a range of foreign laws have been taken as benchmarks, while parts of the Code governing cybercrime were crafted. The State of Massachusetts' 'Act to Prevent Computer Crime', the State of Texas' 'Computer Crime Law' and United Kingdom's (UK) 'Computer Misuse Act' have, for instance, all been used as input while drafting the computer crime part of the Ethiopian Criminal Code.[28] Certainly, these instruments were neither benchmark nor modern given the time that the Ethiopian Code was adopted. By 2004, some relatively modern cybercrime instruments had already been adopted at the global level. One such instrument is the Council of Europe (CoE) Cybercrime Convention which was adopted in 2001. Indeed, one sees clear marks of the UK's Computer Misuse Act in our Criminal Code. The Act was initially issued in 1990 – during the time when widely known cybercrimes were confined to

[23] *Id*. Preface, II.
[24] *See* Ethiopia: Cyber Security Profile (International Telecommunications Union) <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles/Ethiopia.pdf> (Last accessed on 20 January 2021).
[25] Criminal Code, *supra* note 17, Preface, II.
[26] *Ibid*.
[27] *Ibid*.
[28] *See* Explanatory Note to Criminal Code of Ethiopia (Ministry of Justice, 2004) 321.

nothing more than hacking, dissemination of malware and DoS attacks. Yet, dozens of computer crimes were already plaguing cyberspace in 2004 which the Code apparently failed to regulate.

It is to be noted that dozens of cybercrimes have been committed in Ethiopia since the enactment of the 2004 Criminal Code, but there currently are only few reported court cases where cybercrime rules of the Code were applied.[29] The single publicly reported cybercrime case involved two former business partners Yonas Kassahun and Akiko Seyoum.[30] This is the only reported case adjudged under the cybercrime rules of the Criminal Code before they were repealed by Proclamation No 958/2016. The accused, Yonas Kassahun, was initially convicted and sentenced for the crime of cracking which concerns illegally hacking into a computer system of another person (in this case email account of Akiko) with a further criminal intent of stealing information or damaging one.[31] But upon appeal –and under a shadow of allegations of judicial corruption– a higher court changed the charge to mere hacking, i.e. illegal access with no further criminal intent, and the accused had been released on suspension.[32]

3.2 The Telecom Fraud Offence Proclamation

The Telecom Fraud Offence (TFO) Proclamation is another piece of legislation that criminalizes certain acts that may be categorized as cybercrimes. This law criminalizes acts that target or make use of telecom networks, telecom services or systems. But the advent of technological convergence between telecom and the Internet technologies means that such acts are essentially cybercrimes. It is also vital to note that the definition of 'telecom services' in the TFO law incudes 'Internet services' and 'data

---

[29] For a survey of cybercrime incidents in Ethiopia till mid-2014, *see* KM Yilma, Developments in Cybercrime Law and Practice in Ethiopia (2014) 30/6 *Computer Law and Security Review,* pp. 720, 726-729.

[30] **የፌዴራል መጀመሪያ ደረጃ ፍርድ ቤት**: ***ዐቃቤ ሕግ ና ዮናስ ካሳሁን***. **መቁ**: 108335: 12 **ጥቅምት** 2007; **የፌዴራል ከፍተኛ ፍ/ቤት**: ***ዮናስ ካሳሁን ና ዐቃቤ ሕግ***. **የኮ/መቁ** 158203 28 **ታህሳስ** 2007 [Reported in *Wonber*, 16th Half Year, September 2015, pp. 52-86].

[31] *See*, for example, Yonas Kassahun Receives Two-Year Jail Sentence for Cyber Crimes Against Akiko Seyoum (Fortune, 2 November 2014) <http://bit.ly/1bEUb5C>; Akiko *Sees* a Cyber-Crime Guilty Ruling against Accuser for 42m Br (Fortune, 26 October 2014) <http://bit.ly/1GuZAcf> (Last accessed on 20 January 2021).

[32] *See*, e.g., Diaspora Investor Set Free in a Higher Court Reversal of A Two-Year Sentence (Fortune, 11 January 2015) <http://bit.ly/1Fmkedi>. (Last accessed on 20 January 2021); Yonas Scores a Win in the Battle of the Exes (Fortune, 1 November 2016) <https://bit.ly/3oufNqf> (Last accessed on 20 January 2021).

communication services'.[33] In that sense, the TFO legislation criminalizes three cybercrimes. First, it criminalizes unlawful interception, obstruction of access and interference with telecom services, systems and data.[34] An act would be considered unlawful if/when it is being carried out without the authorization of a lawful user, competent authorities or the service provider. With the enactment of Computer Crime Proclamation No 958/2016 –which introduces provisions criminalizing illegal access, interception of and interference with computer systems– this provision has been repealed.[35]

Second, the TFO law criminalizes the use of telecom services, networks and systems for the commission of other crimes, especially disseminating terrorist and obscene materials.[36] This provision makes reference to the Anti-terrorism Proclamation and the Criminal Code respectively for what constitutes terrorist and obscene materials. Moreover, this provision also criminalizes the use of telecom services for other 'illegal purposes' such as criminal defamation through the use of telecom services.[37]

Third, the TFO law criminalizes what may generally be grouped as telecom-related frauds and forgery such as manipulating or duplicating and selling or otherwise distributing SIM cards, credit cards, subscriber identification numbers, obtaining services through the use of forged documents or by fraudulently using the identity code of another person.[38] Although this provision is not explicitly repealed by Proclamation No 958/2016, the crimes of computer-related fraud, forgery and electronic identity theft that are embodied in the Proclamation essentially make it redundant.[39]

3.3 Interim Draft Laws

Prior to and after the adoption of the TFO legislation, Ethiopia has introduced draft pieces of legislation on cybercrime. The first Bill, Draft Computer Misuse Act, was introduced in 2009 along with other draft cyber laws, otherwise termed 'Draft ICT Security Legislation', covering e-transactions

[33] Telecom Fraud Offence Proclamation No 761/2012, *Federal Negarit Gazeta*, Art 2(1).
[34] *Id*. Art 5.
[35] Computer Crime Proclamation No 958/2016, *Federal Negarit Gazeta*, Art 45(1) cum Arts 3-5.
[36] Proclamation No 761/2012, *supra* note 33, Art 6.
[37] *Id*. Art 6(2).
[38] *Id*. Art 10.
[39] Proclamation No 958/2016, *supra* note 35, Arts 9-11.

and data protection.[40] Commissioned by the former Information and Communication Technology Development Agency, the drafting of this little-known Bill was undertaken by Telecommunications Consultants India Ltd. In terms of substance, two points are worth highlighting about this Bill. First, the Draft Computer Misuse Act was benchmarked after relatively older cybercrime laws of Singapore (1998) and the UK (1990).[41] Second, the scope of this Bill –like the Criminal Code– was circumscribed in two respects. First, it criminalized only a small set of cybercrimes, and as such, it does not stipulate content-related crimes such as child pornography and computer-related forgery and fraud.[42] Second, it did not envisage tailored evidentiary and procedural rules. Overall, this Bill was poorly drafted –and in light of the time when it was drafted, it is now substantively outdated.

A new draft cybercrime legislation emerged in 2013 which departed significantly from the 2009 obscure Bill.[43] Drafted by lawyers at the INSA, this Bill was modern in its orientation and comprehensive in its scope. Its modern and holistic orientation flows from the apparent influence of the CoE's Cybercrime Convention. The 2013 Bill departed from the 2009 Bill as well as the Criminal Code, in two respects. First, it criminalized most types of cybercrimes including content and fraud-related crimes.[44] Second, it envisaged tailored evidentiary and procedural rules.[45] After three years of hiatus – and new drafting (or redrafting) by the Ministry of Justice (currently Office of the Federal Attorney General) – the second version of the Bill was adopted by the Council of Ministers in March 2016.

The Bill was subsequently submitted to the Ethiopian Parliament where it was discussed for an unusually long duration.[46] The second version of the Bill was, by and large, similar in scope –in terms of both substantive and procedural provisions – with the initial version save some new provisions and minor structural as well as 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 has been published in the official law gazette as Proclamation No 958/2016.

[40] Draft ICT Security Legislation (June 2009) [On file with Author].
[41] Draft Computer Misuse Act (June 2009) Art 1.
[42] *Id*. Art 4.
[43] Draft Computer Crime Proclamation (Version 1.0, March 2013).
[44] *Id*. Arts 3-14.
[45] *Id*. Arts 18-22.
[46] Draft Computer Crime Proclamation (Version 2.0, March 2016).

3.4 The Computer Crime Proclamation No 958/2016

As alluded to above, Proclamation No 958/2016 is the final outcome of the 2013 Bill. This means that it is by and large modern and comprehensive, but it also emerged with some changes to the initial versions of the law. It has made, for instance, provisions of the law notably detailed, unlike the truncated nature of the initial draft, which generally works against requirements of precision in legislative drafting. Precision is a desirable virtue of legal provisions as it mitigates problems in judicial interpretation of the rules. In this sense, the present cybercrime law seems to have 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.

Perhaps following the change of hands in the drafting exercise from INSA to the Federal Attorney General, the law now puts the latter as the principal implementing body.[47] Unlike a leading enforcement role assumed by INSA and the Federal Police under the initial draft, the Federal Attorney General (that has drafted the second version of the law) has now come to be the principal enforcer of the law. And, INSA's role has largely been relegated to provision of technical support in the course of cybercrime investigation and prosecution by the Federal Attorney General.[48] The only scenario where INSA would have some investigatory power is with regard to sudden searches and digital forensic investigations for preventive purposes.[49]

In terms of substantive criminal rules, the law maintains almost all items of cybercrimes incorporated both in the initial and second versions.[50] When it comes to procedural and evidentiary matters, the law has incorporated provisions dealing with the preservation and production of computer data by service providers, rules by which computer data or systems could be searched, accessed and seized by investigators, rules on the admissibility of electronic evidence, and related authentication procedures.[51] The law also pays due attention to the importance of cooperation with law enforcement bodies of other countries and organizations, and requires the Federal Attorney General to facilitate such international cooperation.[52]

---

[47] Proclamation No 958/2016, *supra* note 35, Arts 22-25, 30-31, 38.
[48] *Id*. Arts 23 and 39.
[49] For more, *see* next section.
[50] Proclamation No 958/2016, *supra* note 35, Part II.
[51] *Id*. Parts III and IV.
[52] *Id*. Part VI.

Overall, the law is relatively modern and comprehensive. But the law has missed the opportunity to criminalize, among others, racist and xenophobic content, intellectual property-related crimes, revenge pornography and large-scale cyber-attacks through botnets. The Computer Crime Proclamation would have been the pertinent legal instrument to criminalize these emerging cybercrimes that are regulated in many international instruments such as the African Union (AU) Convention on Cybersecurity and Personal Data Protection, the European Union (EU) Directive on Attacks against Information Systems and the CoE Cybercrime Convention and its additional protocol. But as shall be discussed in what follows, the Computer Crime Proclamation also raises serious human rights concerns.

4. Centering Human Rights in Cybercrime Lawmaking

Human rights concern about the cybercrime legislation began to surface shortly after the second version of the law was released. Numerous news reports, commentaries and editorials have been written about the law, most of which highlighting its impact on human rights such as privacy and freedom of expression.[53] Global civil society organizations have also released reports regarding the law before and after its enactment stressing its impact on human rights.[54] This section discusses provisions of the Computer Crime Proclamation that present potential threats to the right to privacy, freedom of expression and age-old principles of procedural justice. Section 5 considers the most recent revision project in light of these aspects of the Proclamation.

4.1 The right to (data) privacy

The current cybercrime law embodies some problematic provisions that trample the right to privacy. But most of these provisions are retained despite concerns expressed during the drafting stage. The second version of the draft, for instance, had authorized INSA to conduct digital forensic investigations against computers suspected to be sources or targets of cyber-attacks without

[53] *See*, for example, Controversial Cybercrime Draft Proclamation Tabled for Approval (The Reporter, 16 April 2016); New Computer Crime Law Hinders Vibrant Online Discourse (Fortune, 24 April 2016); Troubling Aspects of Ethiopia's Cybercrime Bill (The Reporter, 16 April 2016); The Computer Crime Law: Another Inroad on Human Rights? (The Reporter, 30 April 2016); Ethiopia's New Cybercrime Legislation: Government Heard but Only Partially (The Reporter, 11 June 2016).

[54] *See*, for example, Ethiopia: Computer Crime Proclamation – A Legal Analysis' (Article 19, July 2016) <https://bit.ly/3ae0jSa>; Ethiopia's New Cybercrime Law Allows for More Efficient and Systematic Prosecution of Online Speech (Electronic Frontier Foundation, 9 June 2016) <https://bit.ly/3ccvuje> (Last accessed on 20 January 2021).

judicial warrant where there are reasonable grounds to believe that computer crimes are likely to be committed.[55] Moreover, it had empowered INSA investigators to conduct (without judicial warrant) 'sudden searches' against suspected computers for preventive purposes.[56] Following criticisms against these rules, the final version of the law has mandated prior judicial warrant before such far-reaching measures are taken by INSA.[57]

INSA, however, still wields the power to conduct warrantless virtual – not physical!– digital forensic investigation under its reestablishment proclamation of 2013.[58] It is to be noted, though, that a recent subordinate legislation has included the requirement of judicial warrant for purposes of conducting forensic investigation by INSA.[59] According to the Regulation, "the Agency shall carry out digital forensic digital investigation in cooperation with relevant investigating bodies pursuant with Article 6(8) of the (INSA Reestablishment) Proclamation and by the order of a court."

Although there is contradiction between the two laws, regulations are subsidiary pieces of legislation in the hierarchy of laws in Ethiopia. This means that the Proclamation prevails at all times in cases of contradiction but the sheer desire to rectify a limitation of the Proclamation by a subordinate legislation leaves one wondering why. In any case, there is a need to attach the requirement of judicial oversight to the Proclamation's provision. What makes such power of sudden searches and virtual forensic investigation chilling to privacy rights is the absence of any oversight mechanism by courts.

The power of sudden search under the law is far more intrusive even when compared with other Ethiopian laws that envisage sudden search. The Anti-terrorism Proclamation, for instance, allows the Federal Police to conduct 'physical' surprise searches but only upon obtaining the approval of the Commissioner of the Federal Police or his delegate.[60] This form of oversight, although not as independent as judicial oversight, is preferable to random sudden searches without any form of oversight.

[55] Draft Computer Crime Proclamation, *supra* note 43, Art 2.
[56] *Ibid*.
[57] Proclamation No 958/2016, *supra* note 35, Art 26.
[58] Information Network Security Agency Re-establishment Proclamation No 808/2013, *Federal Negarit Gazeta*, Art 6(8).
[59] Execution of Information Network Security Agency Reestablishment Proclamation Council of Ministers Regulation No 320/2014, *Federal Negarit Gazeta*, Art 10(1).
[60] Anti-terrorism Proclamation No 1176/2020, *Federal Negarit Gazeta*, Art 31.

Another problematic provision of the Computer Crime Proclamation relates to the newly inserted 'duty to report' obligation on communication service providers, and government organs.[61] Service providers are required to report to INSA and the Police when they come to know of the commission of cybercrimes or circulation of illegal content (such as child pornography) on their computer systems. It further requires INSA to determine in a Directive the form and procedure by which the reporting will be carried out. The concern with such obligation is that it has the potential to prompt service providers to preemptively monitor communications on their networks under the pain of facing penalties for failing to report. Under such technically onerous statutory obligation –and under the pain of possible penalties– service providers could be prompted to employ algorithmic bots to automatically detect illegality which, as we know, could impact not just the right to privacy but also free expression online.[62]

Countries with robust privacy regimes do not impose a general obligation to monitor communications by service providers.[63] It, however, remains unclear what penalties would follow when service providers disregard their 'duty to report'. One might envisage the possibility of applying penalties prescribed under the Criminal Code since the cybercrime legislation does not address the issue. But how government agencies would be held responsible for failure to report under the above rule lacks clarity. Perhaps, INSA might shed light on these points once it enacts the Directive that will regulate the manner and procedures of reporting.

What further compounds one's concern is that the law also permits the use of a single judicial warrant issued with respect to a specific computer system to be used in conducting investigation into another computer system.[64] Art 32(2) of the Proclamation envisages a scenario of accessing computer data stored in computer systems that could be accessed through a computer system for which a warrant has been obtained. This provision is borrowed from the CoE and AU Cybercrime Conventions but invites legitimate concerns, one being that such a vague and general warrant erodes individual rights of people whose computer systems would be accessed even without their awareness. Allowing extension of virtual or physical search warrant (initially granted to

[61] Proclamation No 958/2016, *supra* note 35, Art 27.
[62] *See* Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion Expression, Frank La Rue (16 May 2017) Para 40.
[63] *See*, for example, EU E-commerce Directive 2000/31/EC 2000 (2000) Art 15.
[64] Proclamation No 958/2016, *supra* note 35, Art 32(2).

a specific computer system to another system) appears, therefore, to be a legislative overreach.

Privacy concerns also arise regarding the rule governing interception and surveillance of communication.[65] In particular, the requirements for surveillance are unclear. The law provides that the investigatory organ may 'request' a court warrant to intercept in real-time or conduct surveillance on communications made by means of telephone, telecommunications and electronic devices in order to prevent and/or prosecute computer crimes. The requirement for interception/surveillance is written solely as a *request* for a court warrant. Moreover, it states the court's role when receiving the request as follows: 'the court shall decide and determine a relevant organ that could execute interception or surveillance as necessary'.[66]

This suggests that investigators will certainly obtain the warrant/permit upon 'request', and as such, the role of courts is simply symbolic. Symbolic in the sense that the court's decision would particularly concern as to 'who' would do the surveillance, not explicitly whether surveillance could be undertaken in the first place.[67] So, the provision implies that courts cannot deny requests submitted by investigators. This is problematic when one considers the possibility of intrusions and abuse in the face of symbolic oversight. Judicial warrants should only be issued if shown to be necessary and proportionate, no other practical means of obtaining vital evidence are available, are targeted, and are based on reliable information.

Art 25(2) of the law recognizes this necessity and proportionality proviso but not in the context of court warrants. Rather, it applies in deciding whether surveillance should be undertaken by the Attorney General. Moreover, the provision authorizes the Attorney General to grant permission in urgent cases for investigators to conduct interception or surveillance without court warrant if there is a reasonable ground to believe that a cybercrime is committed, or to be committed against critical infrastructure.[68] But the Attorney General must seek a warrant from the President of the Federal High Court within 48 hours. *Post facto* judicial oversight is helpful to reverse/minimize the adverse effect on the right to privacy of the emergency warrant. However, it is unclear

[65] *Id*. Art 25.

[66] *Id*. Art 25(1).

[67] The Amharic version –which prevails when inconsistency arises– states the role of the court more explicitly, and in manner that is less symbolic. It provides: "ፍርድቤቱም ተገቢውን በመወሰን እንዳስፈላጊነቱ ጠለፋው ወይ ምክትትል የሚደረግበት ሁኔታ እና ትዕዛዙን የሚያስፈፅመውን አካል ይወስናል::"

[68] Proclamation No 958/2016, *supra* note 35, Art 25(3).

why a warrant must be sought from the President of the Federal High Court rather than the court itself, and if the President of the Federal High Court would exercise a pure judicial function in such cases or would be a mere imprimatur.

Finally, the provision of the Proclamation dealing with retention of communication data raises privacy concerns.[69] The English version of the Proclamation obliges service providers to retain computer traffic data for one year, and it seems that the one-year period is the maximum duration of retention. But, the Amharic version of this provision, which prevails over the English version in case of discrepancies, requires service providers to retain traffic data for a minimum of one year ("ቢያንስ ለአንድ ዓመት ይዞ ማቆየት ይኖርበታል"). In effect, what is prohibited in the Amharic version of the provision is retaining traffic data for less than a year. This also implies that service providers are allowed to store communication data for an indefinite period of time.

This provision should be reconsidered in at least two respects in light of international best practices, including the invalidation of the EU Data Retention Directive by the Court of Justice of the EU.[70] The invalidation of the EU Directive was partly due to the longer duration of retention (a minimum of 6 months and a maximum of 2 years) and its breadth –as it applied to all crimes– as opposed to serious crimes. Therefore, Article 24 should be amended to be more focused, require a relationship between the data and a threat to public safety, and include sufficient limitations and safeguards. These safeguards should include substantive and procedural conditions on the access and use of the data, data security requirements, and objective criteria to limit the number of persons authorized to access or use the data.

4.2 Freedom of Expression

Proclamation No 958/2016 contains provisions that tend to impose overbroad restrictions on the right to freedom of expression and of the press. First, the way in which 'Crimes against Public Security' is framed may have a chilling effect on freedom of expression and information.[71] In particular, it does not clearly prescribe what constitutes 'inciting violence'. The lack of clarity may prompt self-censorship contrary to international human rights standards.

[69] *Id*. Art 24.
[70] *Digital Rights Ireland and Seitlinger and Others* [Joined Cases C-293/12 and C-594/12] (8 April 2014).
[71] Proclamation No 958/2016, *supra* note 35, Art 14.

Second, the cybercrime law criminalizes defamation over the Internet.[72] Defamation is, of course, already a crime in the Criminal Code.[73] What the cybercrime law does is extend it to defamation published through the use of computer systems. But the trend worldwide has been to decriminalize defamation to avoid its adverse effects on the enjoyment of free speech, including on the Internet. And an additional reason why defamation should be decriminalized in Ethiopia is because it already is a civil offence in Ethiopian law of torts, offering victims some recourse.[74]

Third, the Computer Crime Proclamation attaches harsh penalties for commission of most crimes. Such an approach would impel self-censorship and hence unduly chill free expression. For instance, the punishment for offences under Section I (Articles 3–5) appears to be excessive and could potentially affect freedom of expression. Similarly, the appropriateness of the punishment of 25 years prison sentence for aggravated cases under Article 8 calls for reconsideration. But the overall propensity of imposing harsh penalties concerns other laws that touch on aspects of cybercrime. For instance, the TFO law imposes harsh penalties for what seem to be minor infractions. As highlighted in Section 2, only one provision of the TFO law is repealed by Proclamation No 958/2016 (and the cybercrime Bill). This means that other provisions of the law criminalizing certain cybercrime-like acts would continue to apply.

4.3 Due process rights

The Computer Crime Proclamation entails rules that negate crucial principles of procedural justice such as due process of law. The law, for instance, allows courts to rule *ex parte* upon request by investigators for a production order against a person thought to be in possession of computer data needed for investigation.[75] Granting a production order even without the presence of the person concerned that could have legitimate reasons to protest an otherwise unreasonable request erodes due process rights. Disclosure of personal computer data in the course of enforcing such an order also implicates data privacy rights.

Another important principle of procedural justice apparently abrogated by the law relates to the burden of proof in cybercrime proceedings. The law states that where the Prosecutor has proved 'basic facts', the court may on its

[72] *Id*. Art 13.
[73] Criminal Code, *supra* note 17, Art 613.
[74] Civil Code Proclamation No 165/1960, *Negarit Gazeta*, Arts 2044-2049.
[75] Proclamation No 958/2016, *supra* note 35, Art 31(2).

own motion shift the burden of proof to the accused.[76] This provision violates a long-established principle of criminal justice which imposes on the government the burden to prove guilt beyond any reasonable doubt. It also denies the right of the accused to be presumed innocent until proven guilty as the mere decision by the court to shift the burden sends the wrong message that a *prima facie* case has been established by the prosecutor.

What also lurks behind this provision is that given the little cybercrime investigation and prosecution experience in Ethiopia, prosecutors might often resort to such provision in the face of thin evidence against suspected individuals. A prosecutor might plead the court to shift the burden of proof by simply adducing rather inconclusive evidence such as the appearance of a person's face in an illegal content or other criminal venture with which the suspect has nothing or little to do. This is more likely to occur when computers of innocent individuals are compromised and turned into 'zombies' by hackers remotely, and later used to commit cybercrimes like DDoS (Distributed Denial of Service) attacks. In such technically complex cases, ordinary individuals suspected of committing a cybercrime will, therefore, find it too cumbersome to refute the presumption once the burden is shifted.

5. Cybercrime Law Reform in Ethiopia (2018 onward)

This section examines cybercrime law reform efforts that began in the wake of the reforms in mid-2018. It considers two themes. First, it briefly discusses the process of revising the current cybercrime legislation. As shall be submitted, the revision process has not, thus far, been entirely inclusive of stakeholders and hence there is the risk of lower procedural legitimacy once it is adopted. Second, it considers major changes introduced in the revised cybercrime Bill. While the Bill introduces a few new criminal provisions, a central objective of the law appears to be making the nation's cybercrime legal regime human rights friendly.

5.1 The Revision Process

As highlighted above, the ongoing effort of revising the nation's cybercrime legislation was part and parcel of the post- 2018 multi-pronged legal reform program. The task of revising Computer Crime Proclamation No 958/2016 has been undertaken by a Media Law Working Group established under the Legal and Justice Affairs Advisory Council. The Working Group is said to be composed of journalists, lawyers, government representatives and scholars

[76] *Id*. Art 37(2).

who act on a voluntary basis.[77] Its prime responsibility has been to conduct a rigorous assessment of laws, institutions, and practices affecting the media in Ethiopia. In particular, the Working Group has been tasked with the analysis of the shortcomings associated with laws governing the media with special emphasis on laws affecting the media, freedom of information, broadcasting, computer crimes, and other laws and practices connected with media and expression rights.[78] In addition to providing research-based recommendations, the Working Group has had the mandate to draft laws and regulations in order to ensure the growth of an independent, diverse and vibrant media sector.

As its name clearly suggests, the Working Group has had a slightly broader mandate of revising laws relevant to the media. The revision work ultimately led to the drafting of three pieces of draft legislation on media, access to information and cybercrime. The Draft Computer Crime Proclamation has, therefore, been revised by the Working Group. But the rationale for the mandate in crafting cybercrime legislation to a Working Group whose task specifically is to revise laws that affect the media is not clear. While cybercrime law would relate to free expression –and as highlighted in Section 3, the current cybercrime law chills free speech to an extent– it is barely related to media law.

The concern with such an approach is that clouded by the focus on the 'media', the level of attention that the cybercrime bill receives during the legislative process might be lower. It would have made more sense if the revision work was entrusted to Working Groups tasked with revising the nation's criminal and procedural laws. As alluded to in the preceding section, the Draft Criminal Procedure and Evidence Code has some interplay with the cybercrime Bill. Of the three Bills prepared by the Media Law Working Group, the Media Law Proclamation has been enacted by the Parliament.[79] But the fate of both the Computer Crime and Access to Information Proclamations remains uncertain.

Public and stakeholder consultations are key to the procedural legitimacy and normative quality of laws. Nevertheless, the extent to which the revision of the cybercrime Bill has been preceded by and enriched with input from key stakeholders is in question. The Working Group has taken some steps to draw

[77] Conservation with Mr Solomon Goshu, Chairman of the Working Group, September 2019.
[78] *Ibid.*
[79] Media Proclamation No 1238/2021, *Federal Negarit Gazeta*.

on expert inputs on all the three Bills, one example being the August 2019 Workshop.[80] But stakeholder consultations, in the true sense of the terms, held thus far were driven mainly by international and local civil society groups. In this regard, two such consultations are worth a mention. One is the panel discussion organized by the NDRE, CARD and the Africa Bureau of the Internet Society at the Forum on Internet Freedom in Africa held in Addis Ababa in September 2019. This event drew many participants from different sectors, including civil society, academia, relevant government departments and regional organizations. The second platform to draw input from stakeholders was organized by Lawyers for Human Rights, a local civil society organization in Ethiopia. While this event attracted limited participation –partly because of the restrictive conditions of the pandemic– it was another useful opportunity to provide inputs to the revision of the Draft Computer Crime Proclamation.

Consultations are crucial in enhancing procedural legitimacy. Not only the substance of a bill but also the process through which it is crafted must earn legitimacy to achieve its underlying objective, be it guaranteeing rights, limiting power or setting governance norms. 'Procedural legitimacy' relates to sources and the nature of the process that validates the outcome.[81] As such, it concerns as to 'who' and 'how' could rightly produce a substantively legitimate bill. But it is to be noted that procedural legitimacy is sometimes seen as a pre-condition to the substantive legitimacy –which concerns primarily the legitimacy or pertinence of the content or the 'purposive direction' of the bill.[82]

When the output, like the case of the 'fruits of a poisonous tree' metaphor, is a product of an illegitimate process, it would, *mutatis mutandis*, be illegitimate. Thus, procedural legitimacy concerns the inclusiveness and the integrity of the process. Whether a bill achieves procedural legitimacy hinges on several factors. The degree to which it embraces the inputs, and addresses the concerns of relevant stakeholders is a primary consideration. Beyond the question of who has participated in the process, the transparency in the course of drawing the bill is another consideration. Moreover, the manner in which the integrity and security of the process is maintained to prevent possible

[80] *See* Brief Explanatory Notes on the Revised Computer Crime Proclamation (December 2020) 2 [Noting that Public consultation was held with 'relevant' stakeholders and 'relevant' comments were incorporated].

[81] Frederick Barnard (2001), *Democratic Legitimacy: Plural Values and Political Power* (McGill-Queen's University Press) 27-28.

[82] Samantha Besson (2005), *The Morality of Conflict: Reasonable Disagreement and the Law* (Hart Publishing) 220.

dilution also counts towards the procedural legitimacy of a bill. In light of this point, it cannot be overemphasised that the Working Group should work towards enhancing the procedural legitimacy of the Draft Computer Crime Proclamation.

Public consultations, as mentioned above, are important in strengthening the normative quality of laws as well. Drawing input from various relevant actors working in cross-cutting themes would enhance the quality of its content. This is particularly useful for a field like cyber law which combines technical and criminological as well as legal notions. Beyond lawyers, meaningful consultation with stakeholders from various disciplines including computer science, software engineering and criminology would significantly improve the substantive quality of the law. As shall be outlined in the next section, the Draft Computer Crime Proclamation is yet to attain the desirable quality. It, for instance, embodies provisions that are outside the scope of cybercrime law and it envisages a less thought-out surveillance oversight regime.

5.2 New changes in the cybercrime Bill and human rights

Changes introduced in the cybercrime Bill can generally be grouped into three categories. First, the Bill introduces a number of provisions that underline – if not overemphasize – the need for the protection of human rights in the course of cybercrime investigation and prosecution. Second, the Bill introduces several new cybercrimes, including acts already criminalized in the Criminal Code. Third, it brings forward miscellaneous themes, including those barely related to cybercrime. This section discusses these three key components of the Draft Computer Crime Proclamation.

5.2.1 (Over)humanizing cybercrime legislation

Making the cybercrime legal framework human rights friendly appears to be the overarching objective of the revision project.[83] Cybercrime investigative techniques, including procedures of evidence collection and preservation, generally involve measures that would interfere with human rights. In an attempt to address such concerns, the Bill tends to humanize the existing law in two respects.

First, it remedies most human rights unfriendly provisions of the current legislation. As discussed in Section 4, the current cybercrime law of Ethiopia carries some provisions that would undermine the enjoyment of human rights.

[83] *See* Brief Explanatory Notes, *supra* note 80, at 1.

Such concerns are now mostly addressed by the Bill.[84] Second, the Bill introduces new human rights clauses that stress the imperatives of upholding human rights in the course of cybercrime investigation and prosecution. But this is not an innovation of the Bill, because the current cybercrime law already embodies a human rights 'principle' that seeks to ensure that investigative techniques do not infringe the rights of individuals. Art 27 of Proclamation No 958/2016 provides as follows:

> The prevention, investigation and evidence procedures provided in this Part and Part Four of this Proclamation shall be implemented and applied in a manner that ensure protection for human and democratic rights guaranteed under the Constitution of the Federal Democratic Republic of Ethiopia and all international agreements ratified by the country.

But the Draft Computer Crime Proclamation envisages additional clauses that reinforce, if not repeat, this 'principle'. In Art 19 – captioned 'Protection of Political Speech and Public interest'– the Bill provides:

> In the application of the provisions of Articles 15 to 18, (sic) courts and other quasi-judicial organs shall be guided by the principle that expressions made in public interest, in particular political speech made in the context of public discourse should be protected to the widest extent possible and that limitations should be applied only in circumstances where it is necessary to ensure national security, public order, health and the protection of public morals in a democratic society.

Perhaps what makes this clause different from the human rights 'principle' highlighted above is the particular focus on free speech, specifically 'political speech'. No doubt free expression is a fundamental human right guarantee crucial for the development of democracy. But it is unclear why it should be singled out, and over-emphasized in the Bill. The Bill does not stop there, it embodies a further human rights clause. Under the Miscellaneous Provisions Part of the Bill, Art 48 –captioned 'Human Rights Safeguard Clause'– stipulates as follows:

> In adopting legal measures in the area of computer crime and establishing the framework for implementation thereof, law

[84] *See*, for example, Draft Computer Crime Proclamation (December 2020) Arts 43 [Reverses the rule that shifts burden of proof from the Prosecutor to the accused]. But note that not all human rights concerns flagged in Section 4 are addressed in the cybercrime Bill such as the 'duty to report' provision, ambiguities concerning the symbolic role of courts in surveillance oversight and data retention period.

> enforcement officials, the Office of Attorney General, the Agency and other organs of the state shall ensure that the measures so adopted will not infringe on the human rights of individuals guaranteed under the constitution and other domestic laws. In particular, measures should not unduly infringe on such fundamental rights including freedom of expression, the right to privacy, the right to a fair hearing and other due process guarantees of individuals.

In this proviso, the Bill reiterates the human rights 'principle' but goes on to state an illustrative list of human rights and fundamental freedoms that should not be infringed in the course of implementing the law. Indeed, the Bill has also introduced a new paragraph in the Preamble that highlights the need to protect human rights while investigating cybercrimes. It reads:

> WHEREAS it has become important to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the Constitution and international human rights conventions ratified by Ethiopia.

Upholding human rights in the course of cybercrime investigation and prosecution is a worthy goal. In this regard, the Draft Computer Crime Proclamation is commendable in addressing most of the human rights concerns associated with the existing law. And the addition of a new preambular paragraph – added to the already existing human rights 'principle' clause– that seeks to uphold human rights in potentially intrusive investigative measures is a welcome development. But the extent to which such a goal should be legislative in the sense that it forms part of a cybercrime legislation is uncertain. With the insertion of additional human rights clauses, the rather progressive Bill has veered off course. Added to the inclusion of other themes unrelated to cybercrimes discussed further below, this tendency of incorporating less related themes renders the Bill formless.

5.2.2 (Over)expanding scope of cybercrime legislation

To a degree, the Draft Computer Crime Proclamation expands the scope of the current legislation. It does so by incorporating two types of cybercrimes. Emergent cybercrimes that are now being criminalized worldwide such as revenge pornography are one category of cybercrimes. Revenge pornography relates to the use of computer systems to publish the intimate images of an ex-partner without consent aimed at causing emotional distress. In line with the

global trend –and the growing incidents of such acts in Ethiopia,[85] the cybercrime Bill criminalizes revenge pornography.[86] Related to this is that the Bill also added 'virtual' child pornography to the already existing crime of child pornography.[87] While the current legislation would potentially cover online child pornography in all its forms,[88] the specificity in the Bill is a welcome addition.

In the second category of newly added crimes, one finds three crimes: incitement of genocide, crimes against humanity and cyberterrorism.[89] These three acts are already criminalized in the Criminal Code and the Anti-terrorism Proclamation regardless of how the messages inciting the prohibited conduct are disseminated or published.[90] What the cybercrime Bill simply does is that it specifies the use of computer systems like the Internet to incite genocide, crimes against humanity and terrorism. In an age where the commission of grave international crimes like genocide are increasingly incited through social media, criminalizing such conduct is imperative. But this approach of re-defining every crime so that its commission through the use of the Internet is captured can be problematic. For one, why re-define them while the Criminal Code already criminalizes such acts in technology neutral terms. But importantly, the question of where this end remains –which crimes are going to be re-defined?

Other additions in the cybercrime Bill include new definition of terms such as 'child pornography', 'interference' and 'subscriber information'.[91] But the provision that criminalizes hacking, for instance, already unpacks the meaning of 'interference' while the term 'subscriber information' is used nowhere in

[85] *See* Kristen Cheney *et al* (2017), Feeling 'Blue': Pornography and Sex Education in Eastern Africa, 48 *IDS Bulletin* 81, 83 [Highlighting this trend in Ethiopia].

[86] Draft Computer Crime Proclamation, *supra* note 84, Art 14 ('Unlawful Dissemination or Publication of an Intimate Image').

[87] *Id*. Art 13(1(b)).

[88] Computer Crime Proclamation No 958/2016, *supra* note 35, Art 12.

[89] Draft Computer Crime Proclamation, *supra* note 84, Arts 16-17.

[90] Criminal Code, *supra* note 17, Arts 269-270 cum Art 36 ['Incitement']; Anti-terrorism Proclamation, *supra* note 60, Art 10. Art 36 of the Criminal Code provides that the punishment to be imposed [for incitement] shall be the punishment provided by law for the intended crime. Note that the Criminal Code does not use the terms 'crimes against humanity', but 'war crimes against the civilian population' (Art 270). The latter, however, captures the essence of crimes against humanity, at least those committed during wartime. Oddly though, Art 44(1) of the Code refers to criminal acts under Art 270, *inter alia*, as 'crimes against humanity' not 'war crimes against the civilian population'.

[91] Draft Computer Crime Proclamation, *supra* note 84, Arts 2(19), Arts 2(6), 2(14).

the law except in the definition of computer data where it is listed as one type of such data.[92] This makes one wonder whether such additions are necessary at all. The Bill also adds definition of other notions such as Internet shutdown which, as shall be considered in the following section, are beyond the scope of cybercrime legislation.[93]

The other notable change in the Bill concerns the reduction in penalties for some cybercrimes. As alluded to in Section 4, the harshness of penalties tends to induce self-censorship, and hence chills expression rights. With this notion in mind, the Bill reduces penalties significantly. For the crime of hacking for instance, the current law imposes a simple imprisonment not exceeding three years.[94] The Bill reduces the prison sentence to a maximum of two years, though it –oddly– increases the corresponding financial penalty to 60,000 from 50,000.[95]

5.2.3 Miscellaneous Changes

The third group of changes in the cybercrime Bill concerns two themes. First, it outlines a legal framework for Internet shutdowns, blocking and filtering. Second, it institutes a surveillance oversight body fashioned in the form of a Committee. This section discusses these two themes.

Rules for Gateway Measures

An innovation of the cybercrime Bill is that it introduces a legal framework for what are collectively called 'gateway' measures such as Internet shutdowns, blocking & filtering.[96] Tucked in Part III of the Bill that covers content-related crimes, it stipulates that such measures should be: (a) undertaken in a transparent manner, (b) subject to legal challenge by affected persons, (c) based on prior court order and (d) taken to achieve specific legitimate aims such as national security and public health. The Bill further requires service providers to notify users and the general public of an impending gateway measure. However, this provision raises a number of questions.

At the most basic level, it is unclear how gateway measures are related to cybercrime law. The legislative objective of any cybercrime legislation is to lay out rules for the criminalization, investigation and prosecution of crimes

[92] *Id*. Arts 5(1), Art 2(4).
[93] *Id*. Arts 2(15-17).
[94] Proclamation No 958/2016, *supra* note 35, Art 3(1).
[95] Draft Computer Crime Proclamation, *supra* note 84, Art 3(1).
[96] *Id*. Art 22.

committed through the use of or against computer systems. As highlighted in Section 2, there is no clear legal basis for gateway measures in Ethiopia despite the indefensible justifications offered recently by the Office of the Federal Attorney General. The initiative to ground gateway measures on a firm legal basis, and with some human rights safeguards is commendable.

What makes such an initiative more desirable is the impending liberalisation and partial privatization of the telecom sector. As new telecom operators enter the telecom market, the incidence of factors that usually trigger gateway measures in Ethiopia might increase as well as requests for gateway measures from the government. But it goes well beyond the scope of cybercrime legislation to institute a legal framework for gateway measures. Perhaps, the best way forward is to relocate this provision –with appropriate changes– elsewhere, probably in the Draft Criminal Procedure and Evidence Code or as an amendment to INSA's establishment legislation, or a new freestanding piece of legislation.

Beyond a question of formal pertinence, the rule governing gateway measures is beset by further conceptual ambiguities. First, it states that gateway measures would be taken when orders are given by a 'competent body' to service providers.[97] But it is not clear which department of government is given this far-reaching power – is it INSA, the Office of the Attorney General, the National Intelligence and Security Service (NISS) or the Federal Police? Art 22(3) of the Bill suggests that the envisioned competent body is not a single government department but several bodies: 'service providers, the agency [INSA] or any other government body'.

While leaving this discretion to a number of bodies is problematic in and of itself, it is also odd how 'service providers' are seen as decision-makers with regard to gateway measures. What is clear, however, is that the envisioned 'competent body' is not the judiciary. This is a major misstep for a revision project whose prime goal is entrenching human rights protection in the cybercrime prevention, investigation and prosecution. Orders to take gateway measures should always be given by an independent and impartial tribunal. Otherwise, the incidence of such orders would continue unabated, and *post facto* options of judicial recourse to challenge the measures would do little to remedy damages already sustained. Perhaps, the requirement of court order might be waived in exceptional circumstances that dictate immediate measures but judicial review should be mandated at a later stage – e.g. within 48 hours.

[97] *Id*. Art 22(4).

Second, the provision stipulates that 'any affected party' may challenge before courts 'decisions of service providers, the Agency or any other government body'.[98] At least two questions arise here. For one, does this right to institute a legal challenge apply before the measures are taken or after the fact? The term 'decision' suggests that the legal challenge may be launched before the decision to, for instance, shutdown the Internet is implemented by service providers. And this reading of the provision also finds support from the duty of notification, discussed further below, on service providers regarding impending measures.

But it is still vital to clarify this point. What constitutes being 'affected', and who would be considered an 'affected party' in the context of gateway measures are not straightforward. Would ordinary Internet users whose access to the Internet is cut due to Internet shutdowns be considered an 'affected party' that may lodge a legal challenge? Would businesses such as banks whose services rely on the availability of network be able to legally challenge network disruptions? How about civil society groups –would they have a standing for judicial recourse? Such questions remain unanswered. But in light of the recurrence of network disruptions in Ethiopia, it is vital that civil society groups are bestowed a legal standing on the behalf of ordinary users.

Third, the provision envisages a notification regime by which service providers 'should notify their users accordingly and should provide sufficient information to the public about the order and action taken.'[99] The ambiguity in this provision relates to whether the notice should be provided before or after the gateway measure. The terms 'order and action taken' suggest that it is *post facto* notification, after the service provider cut the Internet, blocked websites or began filtering content. If the notice were to be provided before the fact, it would allow 'affected parties' to launch a legal challenge to prevent the impending gateway measure.

But the notice regime would offer little if the notification comes after the fact, especially when the measures would cause irreparable losses, be it material or otherwise. *Ex post* notices would be useful only if the loss sustained due to the network disruption can be recuperated, for example through damages/compensation. To make the notice rules more effective, the best way forward is to envisage a two-pronged notification regime. *Ex ante* notices should be provided to users before measures are taken and *ex post* notices only for urgent cases. In the latter case, the relevant government body

[98] *Id*. Art 22(3).
[99] *Id*. Art 22(4).

may seek court order and have gateway measures taken in exceptional cases but notices should be provided after the fact.

Oversight for Digital Surveillance

The cybercrime Bill institutes two types of safeguards against arbitrary practices of surveillance.[100] First, it obliges the Office of the Federal Attorney General to issue transparency reports annually detailing the number of real-time surveillance measures undertaken for purposes of investigating cybercrimes. The Bill further instructs the Office of the Attorney General to issue a Directive as to the 'form and procedures of reporting'.[101] Second, it creates an oversight 'Committee' consisting of representatives from INSA, the Ethiopian Human Rights Commission, the Judiciary and civil society. The main functions of this 'independent' Committee would be to monitor government surveillance practices and adjudge complaints of arbitrary/ unlawful digital surveillance, search and seizure. No doubt this provision is added to the Bill as a human rights safeguard against arbitrary search, seizure and surveillance. But its formulation is far from clear which, in turn, undermines its objective of preventing or remedying arbitrary digital surveillance.

Ambiguities of three sorts are apparent. First, the Bill envisions a Committee, as opposed to other more pertinent bodies as an oversight body such as a court or tribunal. The Committee is referred to as an 'independent' body, but its apparent casual and tentative nature does not seem to ensure its independence. That the Committee is to be formed by the Attorney General also casts doubt on its independence. For instance, who would get to be a member of the Committee from civil society groups is to be determined – or co-opted – by the Attorney General.

But more importantly, the Bill gives to the Attorney General complete discretion not only in deciding who joins the Committee but also how it would be formed and then operate, including term limits and selection criteria as well as termination. Even the Directive that the Attorney General is empowered in the Bill to issue would concern only the 'form and procedure' of its annual report on government surveillance measures.[102] This gives unwarranted discretion to the Attorney General, thereby undercutting the operational independence of the envisioned surveillance oversight body.

[100] *Id*. Art 33.
[101] *Id*. Art 33(5).
[102] *Id*. Art 33(5).

With a view to ensure the independence of the surveillance oversight body and ensure democratic governance, at least the following changes in the relevant provision are needed. One is to rename the body to make it look more like a permanent body with clearly defined term limits, procedures of selection, termination and codes of conduct. Surveillance legislation in other countries often creates a Commission that operates as an independent, full-time surveillance oversight body.

In the UK for instance, the Investigatory Powers Act creates a 'Commission', led by a Commissioner who is often a retired judge, to oversee surveillance activities of law enforcement, the intelligence agencies, prisons, local authorities and other government agencies[103] As will be noted below, relevant Standing Committees of the Ethiopian Parliament are already tasked by law to provide 'legislative oversight' for surveillance in Ethiopia. Creating a separate Committee in a specific legislation would be superfluous unless it is constituted as an independent, full-time surveillance oversight body.

Secondly, key details about the Committee should also be detailed in the cybercrime legislation, rather than leaving it to the discretion of the Attorney General. Otherwise, it would be usurping a key legislative as well as democratic function of elected members of the legislature. Furthermore, to ensure its operational and institutional independence, the surveillance oversight body should be created under the aegis of the judiciary. Or, at least the decisions of the Committee should be appealable to court.

But even then, that the judiciary is one of the members of the Committee complicates the process. It should also broaden membership to include the technical community. As a technical matter, proper monitoring of and adjudicating complaints against arbitrary digital surveillance would require the insight and input of the technical community. And of course, with civil society groups present in the Committee, the addition of the technical community would bring the Committee closer to a multi-stakeholder body.

Third, the question of how this surveillance oversight regime relates to or is different from other parallel regimes remains. NISS is tasked to undertake surveillance, by employing various mechanisms, on any matters of national security and to investigate serious crimes such as terrorism.[104] And its

[103] *See*, for example, Investigatory Powers Act (2016) Sections 227 *et seq*. See also details about the Investigatory Powers Commissioner's Office at <https://www.ipco.org.uk/> (Last accessed on 20 January 2021).

[104] National Intelligence and Security Service Re-establishment Proclamation No 804/2013, *Federal Negarit Gazeta*, Art 8.

establishment law puts in place three levels of oversight to prevent arbitrariness: legislative, executive and judicial.[105] Its measures, including surveillance, are thus subject to review by a Standing Committee of the Parliament, the Prime Minister and the Judiciary.

Would surveillance undertaken by NISS when investigating cyber-terrorism or crimes against public security –both criminalized in the cybercrime Bill– be subject to oversight regime in the Bill or NISS's establishment law or both? Of course, NISS assumes no investigative roles either in the current cybercrime law or the Bill. But in light of its broader mandate to investigate national security-related crimes as well as terrorism, its involvement is inevitable. To prevent institutional rivalry and ensure efficiency, it is important that drafters of the Bill work out clearly the relationship between the two parallel regimes of surveillance oversight.

A final but related point worth highlighting is whether the role the surveillance oversight body would be restricted to cybercrimes or it would cover all forms of digital surveillance beyond cybercrimes. As a body to be established by a cybercrime legislation, it would readily suggest that its powers relate only to surveillance in the context of cybercrime investigation and prosecution. But it is vital that the scope of the envisioned oversight body's functions is clearly defined in light of the statutory surveillance powers of other government agencies. Further to be considered is the interplay between the relevant provisions of the cybercrime Bill and the Draft Criminal Procedure and Evidence Code which repeals procedural and evidentiary provisions of the current cybercrime legislation.

6. Concluding Observations

This article mapped the development of cybercrime law in Ethiopia with a particular focus on the more recent effort of revising Computer Crime Proclamation No 958/2016. Launched in the wake of the post-2018 ambitious reform program, a Draft Computer Crime Proclamation has been prepared by the Media Law Working Group created within the Federal Attorney General's Legal and Justice Affairs Advisory Council. As shown in this article, the cybercrime Bill introduces some changes to the current cybercrime legislation. But a key aspect of the revision has been to rectify provisions of the current law that tend to undermine the enjoyment of human rights. While a few new cybercrimes are included, the revision work goes a long way in humanizing the cybercrime legal and regulatory framework.

[105] *Id*. Arts 22-24.

The article has also highlighted a number of shortcomings of the current version of the cybercrime Bill, including in going off track by embracing unrelated themes such as gateway measures as well as the failure to reconcile the Bill with other upcoming Bills such as the Draft Criminal Procedure and Evidence Code. Moreover, the Bill embodies a number of normative ambiguities concerning the notification rules for gateway measures and the new surveillance oversight body.

On top of these shortcomings, Ethiopian authorities will have to tackle two further challenges as they now move to enact and then implement the law. First, owing to the technical nature of cybercrime prevention, investigation and adjudication, capacity building must be taken as a matter of priority. Cybercrime units in the police forces, investigators and judges must be properly acquainted with the nature, scope and purposes of the law. Courses that introduce students to the new realities presented by the Internet including cybercrimes are not offered in any of Ethiopia's law schools. In the absence of such formal education, the most feasible approach both in the long and short-term is to launch continuous capacity building programs in concert with international partners such as the United Nations Office on Drugs and Crime and the Council of Europe that run such programs for developing countries.

Secondly, the enactment of the law would mean little unless the government takes international cooperation seriously. This is because most cybercrime threats posed to Ethiopia are from abroad, at least at this point in time. A good illustrative example is the potentially criminal behavior that can be transmitted through social media platforms which underlines the need for a robust international cooperation framework. The cybercrime Bill rightly mandates the Federal Attorney General to facilitate international cooperation to successfully prevent and prosecute cybercrimes.[106] Efforts of building cooperation could easily start with regional bodies such as the various economic communities in Africa that are increasingly building alliances in dealing with cyber criminality.

The Federal Attorney General could also draw useful lessons from the European Commission which has recently joined hands with big tech firms such as Facebook to jointly deal with extremist and hate speech in online platforms through a sort of co-regulatory mechanism. But as alluded to above, the Draft Criminal Procedure and Evidence Code repeal parts of the Computer Crime proclamation, including its provisions governing international

[106] Draft Computer Crime Proclamation, *supra* note 84, Art 49.

cooperation.[107] Thus the point above about international cooperation should be seen in light of this impending change.

Finally, in light of limited changes introduced in the cybercrime Bill, it is useful to consider whether pursuing an amendment legislation –instead of an all-out repeal,[108] as it is now being pursued– is preferable. A modest amendment Bill might, in comparison to a lengthy new Bill, have a better chance of being adopted quickly. An amendment legislation seems sensible in the context of the cybercrime Bill for other reasons as well. As this article demonstrated, some of the changes in the cybercrime Bill are beyond the scope of cybercrime legislation while the others are too limited to warrant an all-out repeal. This makes the case for pursuing an amendment cybercrime Bill as opposed to a freestanding new Bill stronger. ■

[107] Draft Criminal Procedure and Evidence Code, *supra* note 20, Art 2(2(f)).

[108] Draft Computer Crime Proclamation (*supra* note 84) Art 52 [Repealing Computer Crime Proclamation No 958/2016 and Art 5 of the TFO Proclamation. But it is also vital to note that the cybercrime Bill, like almost all Ethiopian laws, repeals all laws that are inconsistent with it. See *Id*. Art 52(3)].