COMMENT

Some Remarks on Ethiopia's New Cybercrime Legislation

DOI http://dx.doi.org/10.4314/mlr.v10i2.7

Kinfe Micheal Yilma ♣

Abstract

Ethiopia has been enacting various pieces of legislation, since recently, to regulate some aspects of the digital environment. The Cybercrime Proclamation of 2016 (Computer Crime Proclamation No.958/2016) is the most recent addition to the legal regime that criminalizes a range of cybercrimes. It has also introduced a number of novel evidentiary and procedural rules that will assist in the investigation and prosecution of cybercrimes. The law has, however, attracted criticisms from various corners mainly owing to some of its human rights unfriendly provisions. This piece provides brief comments on the cybercrime legislation and highlights some of the challenges that lie ahead in the course of implementing the law.

Key terms

Cybercrime, computer crime, the right to privacy, illegal online content, procedural justice, Ethiopia

Introduction: Ethiopia's new cybercrime legislation

Ethiopia introduced the first set of cybercrime rules with the enactment of the Criminal Code in 2004. The Code criminalizes a set of three cybercrimes namely 'hacking', 'dissemination of malware' and 'denial of service attacks (DoS)'.[1] Several cybercrimes have been perpetrated against the Ethiopian cyberspace since the enactment of the computer crimes rules, but there currently are only a few reported court cases.[2] In 2013, Ethiopia's cyber command –

♣ Kinfe Micheal Yilma, Doctoral Candidate and teaching fellow, Melbourne Law School, The University of Melbourne, Australia; LLB (Addis Ababa University), LLM (University of Oslo), LLM (Brunel University London). Lecturer-in-Law, Addis Ababa University School of Law, Ethiopia (On study leave).

Thanks are due to Selamm BR Abraham and Halefom Hailu for comments and for availing valuable information. E-mail: kinfeyilma@gmail.com

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

[2] For a discussion on major cybercrime incidents in Ethiopia until mid-2014, *see* Kinfe Micheal Yilma (2014), 'Developments in Cybercrime Law and Practice in Ethiopia', 30

Information Network Security Agency (INSA)– released a draft comprehensive cybercrime legislation that not only extended the range of outlawed cybercrimes but also introduced crucial evidentiary and procedural rules for the investigation and prosecution of cybercrimes.[3]

After three years of hiatus –and new drafting (or redrafting) by the Ministry of Justice (currently Office of the Federal Attorney General), the second version of the bill has been adopted by the Council of Ministers in March 2016. The bill was subsequently submitted to the Ethiopian Parliament where it was discussed for unusually long duration.[4] The second version of the bill was, by and large, similar in content –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 since been published in the official law gazette.[5] Despite reform suggestions put forward on the initial drafts, some provisions identified to be worrisome particularly those that encroach on constitutionally guaranteed rights are regrettably maintained.

It has, as a result, attracted widespread attention from various corners after the second version was unveiled. Numerous news reports, commentaries and editorials have been written about the law, most of which highlight its impact on human rights such as privacy and freedom of expression.[6] Global civil society

Computer Law and Security Review 720, 725-729. On a recent cybercrime case adjudged by Ethiopian courts, see Kinfe Micheal Yima and Halefom Hailu Abraha (2015), 'The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce and the New Media', 9 *Mizan Law Review* 108, 110-111.

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

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

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

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

organizations have also released reports regarding the law before and after its enactment highlighting its impact on human rights.[7] This comment is an overview on the new cybercrime legislation and highlights its major limitations as well as practical challenges that lie ahead in the course of putting the law into action.

1. Salient Features of the New Cybercrime Law

The cybercrime law recently enacted by the Ethiopian parliament has 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 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.[8] 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 sheer provision of technical support in the course of cybercrime investigation and prosecution by the Federal Attorney General.[9] The only scenario where INSA would have some investigatory power, as shall be seen below, is with regard to sudden searches and digital forensic investigations for preventive purposes.

In terms of substantive criminal rules, the law maintains almost all items of cybercrimes incorporated both in the initial and second versions. One, however, notes some replication of crimes within the law. An example, in this regard, is the crime of 'causing damage to computer data' –or commonly referred to as 'spreading malware'.[10] A crime of almost identical sort is provided in Art 7(1) of the law which is captioned as 'criminal acts related to usage of computer

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

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

[9] Id., Arts 23 and 39.

[10] Id., Art 6.

devices and data'. All the remaining sub-articles of Art 7 deal with what are normally called 'acts committed to facilitate the commission of cybercrimes'.[11] The same problem of unnecessary replication is discernible with respect to the 'crime against liberty and reputation of persons' where the first two sub-articles are essentially redundant.[12]

Redundancies are also present if one looks across other pieces of legislation. A case in point is 'cyber-terrorism' which Ethiopia's controversial Anti-terrorism law already outlaws, but again Article 14 of the Computer Crime Proclamation[13] essentially replicates it under the caption of 'crime against public security'. The provision reads:

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

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

The law also creates a new cybercrime scenario of 'aggravated cases' when cybercrimes are committed against 'top secret' military or foreign policy computer data, system or network at a time when the nation is in a state of emergency or threat.[14] In such cases, the punishment could go up to 25 years of rigorous imprisonment. Concerns are likely to arise here regarding the excessive length of the punishment. The provision states:

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

When it comes to procedural and evidentiary matters, the law has incorporated provisions dealing with the preservation and production of computer data by

[11] Id., Art 7(2-4).
[12] Id., Art 13.
[13] Id., Art 14; *Cf*, Anti-terrorism Proclamation, *Federal Negarit Gazeta*, Proclamation No. 652/2009, Art 3(6) cum Art 2(7).
[14] Id., Art 8.

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.[15] 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.[16]

2. Problematic Provisions in the Proclamation

The Computer Crime Proclamation incorporates provisions that present potential threat to the right to privacy and age-old principles of procedural justice. The right to privacy is guaranteed under Article 26 of the Ethiopian Constitution and international treaties such as Art 17 of the International Covenant on Civil and Political Rights to which Ethiopia is a state party.[17] The initial versions of the law had some problematic provisions that potentially trample these constitutionally guaranteed rights. 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 judicial warrant where there are reasonable grounds to believe that computer crimes are likely to be committed.[18]

Moreover, it had empowered INSA investigators to conduct warrantless 'sudden searches' against suspected computers for preventive purposes.[19] 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.[20] INSA, however, still wields the power to conduct warrantless virtual – not physical– digital forensic investigation under its reestablishment proclamation of 2013.[21]

It is to be noted that a recent subordinate legislation that furthers the 2013 reestablishment proclamation has included the requirement of judicial warrant for purposes of conducting forensic investigation by INSA.[22] According to the

[15] Id., Part IV, Arts 29-35.
[16] Id., Art 42.
[17] On sources of Ethiopian privacy law, *see* Kinfe Micheal Yilma (2015), 'Data Privacy Law and Privacy in Ethiopia', 5 *International Data Privacy Law* 177, 179-180.
[18] *See* Art 25, *The Draft Computer Crime Law*, Version 2.0, *supra* note 4.
[19] Ibid.
[20] *See* Computer Crime Proclamation, *supra* note 5, Art. 26.
[21] *See* Information Network Security Agency Re-establishment Proclamation, *Federal Negarit Gazeta*, Proclamation No. 808/2013, Art 6(8).
[22] *See* Council of Ministers Regulation to Provide for Execution of Information Network Security Agency Reestablishment Proclamation, *Federal Negarit Gazeta*, Regulation No. 320/2014, Art. 10(1).

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." The contradiction between the two laws is rather confusing in view of the fact that regulations are subsidiary pieces of legislation in Ethiopia's hierarchy of laws. 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 the 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 would have been far more intrusive even when compared with other Ethiopian laws that envisage sudden search. The infamous Anti-terrorism proclamation, for instance, allows the Federal Police to conduct 'physical' sudden searches but only upon obtaining the approval of the Commissioner of the Federal Police or his delegate.[23] This form of oversight, although not as independent as judicial oversight, is preferable to random sudden searches without any form of oversight.

Another problematic provision of the Computer Crime Proclamation relates to the newly inserted 'duty to report' obligation on communication service providers, and government organs.[24] It further requires INSA to determine in a Directive the form and procedure by which the reporting will be carried out. 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. The concern with such an 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 non-cooperation.

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.[25] Countries with robust privacy regimes do not impose a general obligation to monitor communications by service providers.[26] It, however, remains unclear what penalties would follow when service providers disregard their 'duty to report'. One might envisage the

[23] *See* Anti-terrorism Proclamation, *supra* note 13, Art. 16.
[24] *See* Computer Crime Proclamation, *supra* note 5, Art. 27.
[25] *See* Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion Expression, Frank La Rue, UN Doc. A/HRC/17/27, 16 May 2017, para. 40.
[26] *See*, for instance, EU E-commerce Directive, *Directive 2000/31/EC*, 2000, Art 15.

possibility of applying penalties prescribed under the Criminal Code since the cybercrime legislation does not forbid this. But how government agencies would be held responsible for failure to report under the above rule is more puzzling. Perhaps, INSA might shed light on these points once it enacts the Directive that will regulate the manner and procedure of reporting.

What further compounds our 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.[27] 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 warrant has been obtained. This provision is borrowed from the Council of Europe (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 a specific computer system to another system) appears, therefore, to be a legislative overreach.

The cybercrime law also 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.[28] 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 order also implicates data privacy rights.

Another important principle of procedural justice apparently abrogated by the law relates to burden of proof in cybercrime proceedings. The law states that where the Prosecutor has proved 'basic facts', the court may on its own motion shift the burden of proof to the accused.[29] This provision violates a long established principle of criminal justice which imposes on the government the burden to prove 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

[27] *See* Computer Crime Proclamation, *supra* note 5, Art 32(2).
[28] Id., Art 31(2).
[29] Id., Art 37(2).

individuals. A prosecutor might plead the court to shift the burden of proof by simply adducing rather inconclusive evidence like 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 of evidence once the burden is shifted.

3. The Challenges Ahead

The Computer Crime Proclamation is by and large modern and comprehensive. Compared to the initial draft versions, the law is relatively better particularly in eliminating some human rights-unfriendly rules –and adding some that uphold these rights. An example is that the new law carves a provision –captioned 'principle'– that requires provisions of the law to be implemented without contravening human and democratic rights enshrined in the Ethiopian Constitution and international human rights instruments ratified by Ethiopia.[30] Such a guiding principle, if properly complied with by our cybercrime investigators, would serve as an important safeguard to the rights of individuals suspected of being involved in computer crimes. But some areas of concern on the initial versions of the law, as alluded to above, are regrettably maintained.

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 criminalizing these emerging cybercrimes that are regulated in many international instruments such as the African Union Convention on Cyber Security and Personal Data Protection, European Union (EU) Directive on Attacks against Information Systems and the Council of Europe (CoE) Cybercrime Convention and its additional protocol. Overall, the law as it currently stands has a lot to be rectified. One cannot but hope that the government considers ways to amend the law in due time. The Ethiopian Ministry of Communication and Information Technology has completed a study on the protection of intellectual property rights in the context of ICTs.[31] An upcoming law informed by this study might perhaps address IP related cybercrimes.

[30] Id., Art 21.

[31] *See* Ministry of Communication and Information Technology, *Development of Information and Communication Technology Intellectual Property Right Legal*

Ethiopian authorities will have to tackle two major challenges as they now move to 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.[32] 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 partners.

International organizations such as the United Nations Office on Drug and Crime (UNODC) could be crucial partners in this regard particularly given UNODC's previous technical assistance to a number of developing countries. Such capacity building programs could also be useful in restructuring bodies involved in the field such as the cybercrime unit at the Federal Police, INSA and the Office of the Federal Attorney General. The government must also allocate sufficient resources towards raising public awareness about the law. This is not only to allow victims of cybercrimes to be vindicated by the law but also to avoid commission of cybercrimes due to lack of awareness. In a country, like Ethiopia, where the Internet is a recent phenomenon, unwary users are likely to engage in acts that might amount to crime under the cybercrime legislation. Recent awareness campaigners by INSA through radio broadcasts could very well be strengthened to introduce the law to the public.[33]

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 behaviour that can be transmitted through social media platforms. Potentially racist and extremist content in the social media can indeed provoke protesters to destroy property, incite ethnic-based violence and displace of a large number of people.[34] Before the United General Assembly, Ethiopia's Prime Minister Hailemariam Dessalegn noted

Framework for Ethiopia: A Situational Analysis Report, November 2015 (On file with author).

[32] For more on this, *see* Kinfe Micheal Yilma and Halefom Hailu Abraha (2015), 'The Internet and Ethiopia's IP law, Internet governance and legal education: An overview', 9 *Mizan Law Review* 154, 169-173.

[33] INSA runs a weekly radio show called 'cybergna' (literal rendition of the Amharic term would mean 'in the language of cyber') to educate the public about various aspects of ICTs. See details at <https://goo.gl/3CaAdS> (Last accessed on 15 October 2016).

[34] *See*, for instance, Samrawit Tassew, 'Destruction, Looting Mare Popular Oromia Protests', (*Addis Fortune,* 11 October 2016), available at <https://goo.gl/vrouUI> (Last accessed on 15 October).

that "social media has certainly empowered populists and other extremists to exploit people's genuine concerns and spread their message of hate and bigotry without any inhibition." [35]

Short of other means to tackle the problem, the Ethiopian government has increasingly been blocking access to social media platforms and had completely shut down mobile data services. Such drastic measures, it goes without saying, result in considerable economic losses. A recent report by the Brookings Institution, for instance, has indicated that Ethiopia has lost about 9 million US dollars due to frequent Internet shut downs.[36] This is also playing out in international relations fora where the UN is slowly moving to regard internet shutdowns as violation of international human rights law, a good case in point being the recent Human Rights Council Resolution.[37] Ethiopia had abstained from this Resolution.[38]

Concluding Remarks

Ethiopia does not have a full-fledged law that governs the regulation of problematic content on the Internet. Content regulation rules are scattered in various pieces of legislation including the cybercrime legislation, and these are hardly fit for purpose. There is, for instance, no known procedural law that governs the manner by which illegal, offensive and harmful content could be blocked, filtered or taken down. Where the government believes that certain content is problematic, it normally instructs the state-owned sole telecom provider –Ethio-telecom– to block access to content or block the website altogether.

The absence of clear legislative guidelines and oversight mechanism might, in some cases mean blocking of an otherwise innocuous website or content. And, there is no mechanism by which producers of the content or website administrators could challenge the measures. Recently, the Ethiopian Ministry of Communication and Information Technology has commissioned a comprehensive study on the development of online content regulatory framework. The Consultant, to which this author has been a lead investigator,

[35] 'Ethiopian leader at UN Assembly decries use of social media to spread messages of hate and bigotry', (*UN News Center*, 21 September 2016), available at < https://goo.gl/408Acs > (Last accessed on 15 October 2016).

[36] *See* Internet shut downs cost $2,4 billion last year, *The Brookings Institution*, 6 October 2016, p. 8 available at < https://goo.gl/dYq89i > (Last accessed on 15 October).

[37] 'The promotion, protection and enjoyment of human rights on the Internet', *Human Rights Council Resolution*, UN Doc. A/HRC/32/L.20, 27 June 2016, Para 10.

[38] *See* Yohannes Anberbir, 'Ethiopia abstains UN online freedom resolution', (*The Reporter*, 23 July 2016), available at < https://goo.gl/eqlIo0> (Last accessed on 15 October).

has presented a comprehensive report to the Ministry for further action.[39] A future law on the regulation of problematic content is expected to provide the manners through which problematic content will be classified and taken down.

But this would still require a robust international cooperation framework. The law, as noted above, rightly mandates the Federal Attorney General to facilitate international cooperation to successfully prevent and prosecute cybercrimes. Efforts of building cooperation could easily start with regional bodies such as the various economic communities in Africa that are increasingly building alliance 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.[40]

Some form of working relationships with social media platforms especially those with huge consumer base in Ethiopia such as Facebook could be very crucial in tacking dissemination of potentially criminal content in the Ethiopian cyberspace. Another promising channel of cooperation is acceding to the CoE Cybercrime Convention, which is open for accession by any country. Given that the Convention envisages a robust cooperation regime, Ethiopia could benefit by acceding to the treaty.[41] Ratifying the AU Convention is also worth considering.

While many questioned the desirability of the Prime Minister's recent speech about problematic online content before the UN General Assembly, it might perhaps signal his government's determination to deal with the matter head on in the near future. We hope to see soon the establishment of the requisite institutional bodies envisaged in the law including investigators within INSA, prosecutors in the Office of the Federal Attorney General and a special bench within the Federal High Court. Also important is to set out the channel through which the efforts of these organs of the government could be coordinated and directed towards the same goal. ■

[39] Ministry of Information and Communication Technology, *Development of Online Content Regulatory Legal Framework for Ethiopia: Situational Analysis Report*, June 2016 (On file with author).

[40] *See* European Commission and IT Companies announce Code of Conduct on illegal online hate speech, Press Release, 31 May 2016, available at <https://goo.gl/FV9ARf> (Last accessed on 15 October).

[41] Council of Europe Cybercrime Convention, 23.XI, 2001, Arts 23-35 cum Art 37.