Version 11 May 2015

The state of cybercrime legislation in Africa – an overview

Council of Europe/Project Cybercrime@Octopus[1]

1. Introduction: Why should countries of Africa adopt legislation on cybercrime and electronic evidence?

Cybercrime is not only a question of attacks against the confidentiality, integrity and availability of computer data and systems but against the core values and the human development potential of societies increasingly relying on information technology.

In the light of this, governments cannot remain passive; they have the obligation to protect society and individuals against crime.

In practice, however, governments face serious challenges:

- while millions of attacks against computers and data are recorded each day worldwide, only a small fraction of cybercrime[2] – that is, offences against and by means of computers – is actually prosecuted and adjudicated;

- moreover, evidence in relation to any crime is increasingly available in electronic form on computer systems or storage devices and needs to be secured for criminal proceedings.[3] Criminal investigations not relying on electronic evidence seem to become the exception.

An effective criminal justice response is needed. This involves the investigation, prosecution and adjudication of offences against and by means of computer systems and data as well as the securing of electronic evidence in relation to any crime. It also requires efficient international cooperation given the transnational nature of cybercrime and in particular of volatile electronic evidence.

2. A legal framework on cybercrime and electronic evidence: what is required?

Governments are not only obliged to take effective measures for the prevention and control of cybercrime and other offences involving electronic evidence, but they must also respect human rights and rule of law requirements when doing so. Criminal law is a means to achieve this.

Comprehensive legislation covering both substantive law (conduct to be defined as a criminal offence) and procedural law (investigative powers for law enforcement) is the foundation of a criminal justice response.

Legislation on cybercrime and electronic evidence needs to meet a number of requirements:

---

[1] The views expressed in this technical report do not necessarily reflect the official position of the Council of Europe or of the Parties to the Budapest Convention on Cybercrime. Contact: alexander.seger@coe.int

[2] Defined here as offences against and by means of computer data and systems in the sense of Articles 2 to 11 of the Budapest Convention on Cybercrime. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[3] For example, the recent disputes over the encryption of iPhones were not related to cybercrime but to cases of terrorism and drug trafficking. http://recode.net/2016/04/08/apple-fbi-encryption-battle-shifts-to-new-york/

- It must be sufficiently (technology) neutral to cater for the constant evolution of technology and crime as it otherwise risks becoming obsolete already by the time it enters into force.

- Law enforcement powers must be subject to safeguards to ensure that rule of law and human rights requirements are met.

- It must be sufficiently harmonised or at least compatible with the laws of other countries to permit international cooperation, for example, to meet the dual criminality condition.

African States preparing legislation on cybercrime may draw on a number of documents to seek guidance. These include in particular the African Union Convention on Cyber Security and Personal Data Protection adopted in Malabo in June 2014.[4] That treaty reflects a strong commitment by Member States of the African Union to establish a secure and trusted foundation for the information society. It covers a broad range of measures ranging from electronic transactions, to the protection of personal data, cyber security and also cybercrime.

Given that this treaty is rather new and is yet to be tested in practice, and given its broad scope, the present report uses the Budapest Convention on Cybercrime[5] as reference. This Convention is more specifically focusing on cybercrime and electronic evidence, including international cooperation, and is increasingly being used in Africa.

The Convention on Cybercrime was opened for signature in Budapest, Hungary, in 2001. Elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA it is open for accession by any State prepared to implement it and to engage in international cooperation. By April 2016 it had 49 Parties and a further 17 States that had been invited to accede or have signed it.

The Budapest Convention is backed up by the Cybercrime Convention Committee representing the Parties to this treaty and capacity building programmes.[6]

It would seem that the African Union Convention on Cyber Security and Personal Data Protection and the Budapest Convention on Cybercrime complement each other.

Concepts and definitions

In terms of concepts and definitions, States should define "computer system" in a broad sense to encompass also devices such as smart phones, tablets or others while remaining technology neutral. Article 1.a of the Budapest Convention offers an example.[7] Similarly, for criminal law purposes, "service providers" should comprise all types of service providers as proposed in Article 1.c Budapest Convention. While a general definition of "computer data" will be required (see Article 1.b), a specific definition of "traffic data" should be foreseen (see Article 1.d).

In criminal investigations, the data most often needed is "subscriber information". This type of information is less privacy-sensitive than traffic or content data. It will, therefore, be useful to define "subscriber information" separately so that a lighter regime for access to and sharing of

[4] https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf
[5] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG
[6] In 2014, a dedicated Cybercrime Programme Office of the Council of Europe became operational in Bucharest, Romania, and is responsible for capacity building programmes on cybercrime and electronic evidence worldwide.
[7] See also the Guidance Note on the notion of "computer system"
http://www.coe.int/en/web/cybercrime/guidance-notes

subscriber information can be established while traffic and in particular content data require stricter safeguards. Article 18.3 Budapest Convention offers a definition of "subscriber information".

Substantive criminal law: conduct to be defined as a criminal offence

In terms of substantive law States should criminalise illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, child pornography and offences related to infringements of copyright and related rights.

Substantive criminal law under the Budapest Convention on Cybercrime

Article 2	Illegal access to a computer system
Article 3	Illegal interception of non-public transmissions to, from or within a computer system
Article 4	Data interference
Article 5	System interference
Article 6	Misuse of devices
Article 7	Computer-related forgery
Article 8	Computer-related fraud
Article 9	Offences related to child pornography
Article 10	Offences related to infringement of copyright and related rights
Article 11	Attempt, aiding or abetting
Article 12	Corporate liability

It is noteworthy that these provisions alone or in combination still cover most of what constitutes cybercrime even now, fifteen years after adoption of the Convention, because they have been formulated in a technology-neutral manner. Guidance Notes adopted by the Cybercrime Convention Committee show how different provisions can be applied to address botnets, distributed denial of service attacks and other phenomena.[8]

Of course, an international agreement always represents a minimum common denominator, and a State is free to decide to go beyond. However, many States, including in Africa, often face opposition when attempting to criminalise additional types of conduct. This is particularly true for often vaguely defined provisions that criminalise contents, speech or anything "contrary to morality".

Procedural law: Law enforcement powers to secure electronic evidence

The Budapest Convention comprises a range of specific procedural law powers such as orders for the search, seizure and production of data or the interception of communications as well as the power to order the expedited preservation of data.

The procedural powers are:

Procedural powers in the Budapest Convention on Cybercrime

Article 16	Expedited preservation of any type of data
Article 17	Expedited preservation and partial disclosure of traffic data
Article 18	Production orders
Article 19	Search and seizure of stored computer data

[8] http://www.coe.int/en/web/cybercrime/guidance-notes

Article 20	Real-time collection of traffic data
Article 21	Interception of content data

Importantly, these apply to:

- specific criminal investigations where specified data is needed. They don't apply to national security measures or the bulk collection of data;

- electronic evidence in relation to any type of crime and not only in relation to offences against and by means of computers.

Rule of law safeguards

Law enforcement powers – such as the search of computer systems, the interception of communications and others – interfere with the right to private life and other fundamental rights of individuals. Such an interference is only allowed if certain rule of law conditions are met. In particular, these powers must be prescribed by law, pursue legitimate aims, be necessary and proportionate, allow for effective remedies and be subject to guarantees against abuse.

In the Budapest Convention, these safeguards are reflected in Article 15:

> **Article 15 – Conditions and safeguards**
>
> 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
>
> 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
>
> 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

International cooperation

Finally, this treaty is to ensure effective international cooperation on cybercrime and electronic evidence by combining "traditional" mutual legal assistance with expedited means to preserve data in another country, the later with the support of a network of 24/7 points of contact. Again, cooperation is not limited to cybercrime but is extended to cooperation on electronic evidence found on a computer system in relation to any crime.

In 2014, the Cybercrime Convention Committee established a Cloud Evidence Working Group to propose solutions allowing for effective access data stored on servers "somewhere in the cloud", that is, in foreign, multiple, unknown or changing jurisdictions. Options under consideration include an additional Protocol to the Budapest Convention.

The Budapest Convention as a guideline

The Budapest Convention may thus serve as a checklist for the development of domestic substantive and procedural law on cybercrime and electronic evidence. It seems that more than 130 States around the world have used it as a guideline in one way or the other. However, the Convention as a whole is a mature, balanced and coherent document and is best considered as a whole.[9]

For States becoming Parties, the treaty serves as a legal framework for international cooperation. The Budapest is open for accession to any State prepared to implement its provisions.[10] And indeed, an increasing number of States in Africa are deciding to follow this path.

3. The situation in Africa

The current state of cybercrime legislation

A cursory overview of the 54 countries of Africa in terms of specific criminal law provisions on cybercrime and electronic evidence suggests that by April 2016:

- 11 States seemed to have basic substantive and procedural law provisions in place (Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia) although implementing regulations may still be missing in one or the other country.[11]

- A further 12 States seemed to have substantive and procedural law provisions partially in place (Algeria, Benin, Gambia, Kenya, Madagascar, Morocco, Mozambique, Rwanda, South Africa, Sudan, Tunisia and Zimbabwe).

- The majority of African States (30) did not have specific legal provisions on cybercrime and electronic evidence in force.

- Draft laws or amendments to existing legislation reportedly had been prepared in at least 15 States (Burkina Faso, Djibouti, Ethiopia, Guinea, Kenya, Lesotho, Mali, Morocco, Namibia, Niger, South Africa, Swaziland, Togo, Tunisia, and Zimbabwe).[12] In some instances, bills had been presented to national parliaments, in others the fate of draft laws is uncertain.

Country	**Indicative status of specific criminal law provisions on cybercrime and electronic evidence (as at April 2016)[13]**	
Algeria	Partial	▪ Partial legislation in force ▪ Criminal Code of 2004 for substantive law

[9] The Budapest Convention is supplemented by an Additional Protocol on Xenophobia and Racism committed via computer systems (ETS 189). http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 Furthermore, the Cybercrime Convention Committee – representing the Committee of the Parties – is adopting Guidance Notes to facilitate the use of the Budapest Convention for addressing new phenomena. http://www.coe.int/en/web/cybercrime/guidance-notes

[10] States that participated in the negotiation of the Convention (member States of the Council of Europe, Canada, Japan, South Africa and the USA) may sign and ratify it. Any other State may become a Party through accession. The result is the same.

[11] In addition, Chad reportedly adopted a law on cybercrime in July 2014 but the text was not accessible when the present report was finalised.

[12] Reform efforts may also be underway in additional States but may have been ignored for lack of accessible information.

[13] Based on information available.

		▪ Law n° 09- 04 on specific rules on the prevention and the fight against offences related to information and communication technologies of 2010.
Angola	No	▪ No specific legislation in force ▪ Amendments to criminal code including substantive criminal law provisions under discussion for several years
Benin	Partial	▪ Substantive criminal provisions on cybercrime in Law 2011-20 on corruption and related offences (12 October 2011) ▪ No specific procedural law provisions
Botswana	Yes	▪ Cybercrime and Computer-related Crimes Act 2007 ▪ Electronic (Evidence) Records Act 2014 for admissibility of electronic evidence
Burkina Faso	No	▪ No specific legislation in force ▪ Draft law on cybercrime (substantive law)
Burundi	No	▪ Partial substantive law provisions in Penal Code 2009
Cabo Verde	No	▪ No specific legislation in force ▪ Draft law on cybercrime following Budapest Convention (2016)
Cameroon	Yes	▪ Law 2010/012 (21 December 2010) relating to Cybersecurity and Cybercriminality
Central African Republic	No	▪ No specific legislation in force
Chad	TBC[14]	▪ Loi relatifs à la cyber sécurité et la lutte contre la cybercriminalité (July 2014)
Comoros	No	▪ No specific legislation in force
Congo, Democratic Republic of the	No	▪ No specific legislation in force
Congo, Republic of the	No	▪ No specific legislation in force
Côte d'Ivoire	Yes	▪ Law 2013-451 (19 June 2013)
Djibouti	No	▪ No specific legislation in force ▪ Draft law on cybercrime
Egypt	No	▪ No specific legislation in force
Equatorial Guinea	No	▪ No specific legislation in force
Eritrea	No	▪ No specific legislation in force
Ethiopia	No	▪ No specific legislation in force ▪ Draft law submitted to Parliament in April 2016
Gabon	No	▪ No specific legislation in force
Gambia	Partial	▪ Information and Communications Act 2009 with substantive criminal law provisions
Ghana	Yes	▪ Electronic Transactions Act, 2008 (ETA) for substantive and procedural law ▪ Mutual Legal Assistance Act, 2010 (MLAA) with specific provisions on international cooperation on cybercrime and electronic evidence ▪ Accession to Budapest Convention underway
Guinea	No	▪ No specific legislation in force ▪ Draft law (projet de loi relative à la cybercriminalité) adopted by the Government in April 2016
Guinea-Bissau	No	▪ No specific legislation in force
Kenya	Partial	▪ Legislation partially in force (Kenya Information and Communication Act 2009)

[14] Text of the law not available.

		▪ Draft law on cybercrime in preparation (April 2016)
Lesotho	No	▪ No specific legislation in force ▪ Bill on computer crime and cybercrime 2013
Liberia	No	▪ No specific legislation in force
Libya	No	▪ No specific legislation in force
Madagascar	Partial	▪ Loi 2014-006 sur la lutte contre la cybercriminalité (19 juin 2014)
Malawi	No	▪ No specific legislation in force
Mali	No	▪ No specific legislation in force ▪ Draft law on cybercrime available
Mauritania	Yes	▪ Loi 2016-007 relative à la cybercriminalité (20 January 2016) ▪ Note: Implementing regulations pending
Mauritius	Yes	▪ Computer Misuse and Cybercrimes Act 2003
Morocco	Partial	▪ Partial legislation in force ▪ Amendments to criminal and criminal procedure codes underway with specific provisions on cybercrime and electronic evidence
Mozambique	Partial	▪ Partial substantive law provisions in amended Penal Code of 2015
Namibia	No	▪ No specific legislation in force ▪ Draft law with substantive provisions (Electronic Transactions and Cybercrime Bill 2013)
Niger	No	▪ No specific legislation in force ▪ Draft law following Budapest Convention
Nigeria	Yes	▪ Cybercrimes (Prohibition, Prevention, etc.) Act 2015 ▪ Evidence Act as amended in 2011 for admissibility of electronic evidence
Rwanda	Partial	▪ Partial substantive law provisions in Penal Code (section 5)
Sao Tome and Principe	No	▪ No specific legislation in force (amendments to the Penal Code (Law 6/2012) cover illegal interception, computer-related fraud and child pornography)
Senegal	Yes	▪ Law 2008-11 (25 January 2008) following Budapest Convention ▪ Accession to Budapest Convention underway
Seychelles	No	▪ No specific legislation in force
Sierra Leone	No	▪ No specific legislation in force
Somalia	No	▪ No specific legislation in force
South Africa	Partial	▪ Partial legislation in force ▪ Draft law (Cybercrimes and Cybersecurity Bill) in National Assembly following public consultations in December 2015. Following Budapest Convention
South Sudan	No	▪ No specific legislation in force
Sudan	Partial	▪ Cybercrime Act 2007
Swaziland	No	▪ No specific legislation in force ▪ Draft Computer Crime and Cybercrime Bill
Tanzania	Yes	▪ Cybercrimes Act 2015 (20 February 2015)
Togo	No	▪ No specific legislation in force ▪ Draft law on cybercrime
Tunisia	Partial	▪ Few provisions in Penal Code. ▪ Draft law on cybercrime and accession to Budapest Convention under consideration
Uganda	Yes	▪ Computer Misuse Act 2011 (14 February 2011)

Zambia	Yes	▪ Computer Misuse and Crimes Act 2004 ▪ Electronic Communication and Transactions Act (ECT Act) no 21 (31 August 2009)
Zimbabwe	Partial	▪ Chapter VIII Criminal Law (Codification and Reform) Act 2004 with substantive law provisions ▪ Computer Crime and Cyber Crime Bill in preparation

Observations

- As only about 20% of States have the basic legal framework in place, the situation in Africa regarding legislation on cybercrime and electronic evidence is not satisfactory. On the positive side, it is encouraging that reforms are under underway in many States, even though in some cases, draft laws have been under discussion for several years with little progress.

- A number of (draft) laws contain provisions that create risks to the freedom of expression and other fundamental rights, in particular where offences are vaguely defined and conditions and safeguards are weak or missing. Examples are the criminalisation of the "creation of sites with a view to disseminating ideas and programmes contrary to public order or morality", "broadcasting information to mislead security forces", "publication of false information" and similar. This not only affects the rights of individuals and restricts media freedoms but also undermines trust and hinders international and public/private cooperation.[15]

- Procedural law powers are not always precisely defined and safeguards may be lacking. For example, a law allows for orders to compel the production of content data without court order, or a police officer can carry out searches or seizures of computers without court order. This may be contrary to rule of law requirements, namely, that investigative powers that interfere with the rights of individuals must be prescribed precisely, be subject to guarantees against abuse, be necessary and proportionate and must allow for effective remedies.

- On the other hand, data protection regulations are increasingly being adopted in African States, often in conjunction with laws on cybercrime. This creates additional safeguards to the rights of individuals. Mauritius, Morocco and Senegal are not only Parties or have been invited to accede to the Budapest Convention on Cybercrime, but have also requested accession to the Data Protection Convention 108 of the Council of Europe.[16] The African Union Convention on Cyber Security and Personal Data Protection of 2014 also contains an important chapter on the protection of personal data.

- Joining an international treaty such as the Budapest Convention on Cybercrime not only provides a legal framework for international cooperation but instills confidence and trust that such cooperation has a solid foundation in domestic law. This also applies to cooperation between criminal justice authorities and private sector service providers. Mauritius was one of the first countries of Africa to adopt comprehensive legislation on cybercrime in 2003, and in 2014 was the first African State to become a Party to the Budapest Convention on Cybercrime. South Africa signed this treaty in 2001 and the additional Protocol on Xenophobia and Racism in 2008 but has not yet ratified these

[15] For analysis of the state of the protection of freedom of expression on the Internet in European countries see page 47 ff of http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680646af8

[16] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

instruments. Morocco and Senegal have been invited to accede and it is expected that both will become Parties in the course of 2016. These countries participate in the Cybercrime Convention Committee[17] and are priority countries for capacity building. Several other African countries have expressed their political commitment to join and implement this Convention.

- Limited capacities of law enforcement, prosecutors and the judiciary is the main impediment to an effective criminal justice response to cybercrime and other offences involving electronic evidence not only in Africa but in most countries around the world.[18] The adoption of legislation by African States needs to be accompanied by capacity building programmes. The Council of Europe – often jointly with the European Union – is providing support to those African countries that have requested accession to the Budapest Convention, including in the training of criminal justice authorities.[19]

4. Conclusions

The current state of legislation on cybercrime and electronic evidence in Africa is not satisfactory. By April 2016, only 20% of countries seemed to have the minimum legislation in place.

On the positive side, some African countries represent examples of good practice, the African Union Convention on Cyber Security and Personal Data Protection of 2014 should help create a political momentum for stronger legislation and the Budapest Convention on Cybercrime may serve as a guideline for comprehensive legislation that reconciles the need for an effective criminal justice response with the need to meet human rights and rule of law requirements. Accession to this treaty will facilitate cooperation between African countries and criminal justice authorities of countries in other regions of the world.

Efforts currently underway in a number of African countries to reform domestic legislation should be supported and carried through. Over-criminalisation – in particular with regard to content and speech – should be avoided, and conditions and safeguards limiting law enforcement powers should be established. The enactment of data protection legislation should be encouraged.

The adoption of legislation should go hand in hand with the improvement of criminal justice capacities, ranging from the establishment of specialised units for cybercrime investigations and computer forensics, to the strengthening law enforcement and judicial training, interagency cooperation, financial investigations, child protection, public/private cooperation and international cooperation.

The challenge may seem immense, but as indicated at the outset: governments cannot remain passive; they have the obligation to protect society and the right of individuals and to create the conditions for realising the human development potential of information technology.

---

[17] http://www.coe.int/en/web/cybercrime/tcy
[18] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e6
[19] See the GLACY and GLACY+ projects on Global Action on Cybercrime.
http://www.coe.int/en/web/cybercrime/capacity-building-programmes