20th August

Comments on The Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (version -1/01.2011)

By Michael M. Murungi
August 2012

At most, The Draft African Union Convention on the Establishment of a Credible LegalFramework for Cyber Security in Africa (version -1/01.2011) [http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf] could benefit from some further conceptual reflections on why it is necessary and at least, more legislative drafting input.

It has taken me the better part of two days to read each Article of the 60-page document and to give my comments in context. But I need not have gone into all of that because my preliminary opinion is that African states have done a poor job of answering the question "Is there an existing treaty or body of international law that prescribes a model for domestic legislation on cybersecurity to which we can accede or should we instead promulgate our own treaty for Africa?" I think that the conceptual background to the very idea of an African convention on cybercrime needs to be re-examined.

The Budapest Convention [http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG] (or The Council of Europe Convention on Cybercrime as it is more formally known) was the first international instrument on cybercrime and so far, one of the best international attempts at harmonizing domestic laws and improving forensic approaches and co-operation between states in preventing, detecting, pursuing and prosecuting for cybercrimes. It was opened for signature in Budapest, Hungary in November 2001 and entered into force in July 2004. Such has been its appeal that even non-European states have signed or acceded to it - USA, Canada, Japan and the Republic of South Africa.

The Draft African Union Convention attempts to state in over 18,000 words what the Budapest Convention has stated in just over 10,000 words.

My analysis of the Draft African Union Convention is organized into two parts: Part I makes some general observations on some conceptual issues about the Convention. In Part II, I have included verbatim the Articles of the Convention that I would recommend for review, followed by a statement justifying my recommendation.

Part I: Some General Observations on the Convention
Reading through the Draft African Union Convention, I came under the impression that the following conceptual questions need to be (re)considered:

- *Should the African Union promulgate and prescribe its own Convention on Cybercrime or encourage its Member States to sign and accede to the Budapest Convention?*

The answer to this question should not be wound up with the issue of the African Union's self-determination and its sovereignty in promulgating international legal instruments for its Member States. The proper approach would be for the Union to aspire to the best international legislative standards and to look to other international instruments where they lend themselves to the legislative aspirations of the African Union and by extension those of its Member States.

- *What are African aspirations with respect to the information society? Does Internet freedom, e-commerce, cybersecurity, personal data protection etc mean different things to Africans on the one hand and Europeans, Americans and Japanese on the other?*

The Internet is the domain or 'territory' in which the broad range of actions and interactions that comprise e-commerce, e-government, cybercrime, etc take place. It is less of a physical place and more of the "organization of our experience when we are using a linked interface" (Maureen McHugh – blogger & writer). No state can claim dominion over it – and this is not to be confused with the power to restrict access to it. The features of life that traditional governance models seek to regulate - ubiquity, anonymity, freedom and openness – are hardwired into the architecture of cyberspace. It is a melting pot of cultures, knowledge systems, social and business conventions and governance and regulatory models.

Because of the distributed nature of the Internet, Africa cannot abstract a particular 'corner' of the cyberspace domain for itself and enforce its laws within that domain any more than it can compel a citizen of a European country to observe an African convention on cybercrime – the most it can do is to prescribe a standard of behavior

for Africans who enter the domain of cyberspace. But such a prescription will be ineffective and will stand in isolation if it does not bring itself up (or down) to a standard that shakes hands with the prescriptions governing the citizens of the many other nations or regions who populate cyberspace. A law for cyberspace is therefore not the law of the state that has the strongest opinion about what such a law should be but the negotiated compromise representing the sum total of the basic aspirations of most of the nations of the world regarding how individuals should behave in cyberspace.

When I go online, I am not an African on the Internet. I am a Netizen – a citizen of the Internet. My frame of reference should not be so much the laws of my country because a.)they will not be binding on the citizen of another country with whom I am interacting on cyberspace and b). what my country's laws forbid may not be necessarily forbidden in the other country. Therefore, if every Netizen insisted on bringing their own law into cyberspace, there would be as much conflict and stagnation as there are inconsistencies in the various domestic laws. The proper approach instead would be for the countries of the world to find the principles of morality and law on which they are broadly in agreement, and to abstract from them rules of a general nature which they will undertake to require their citizens to observe when they enter cyberspace.

While it is ok for us to espouse our 'African aspirations' on the law of cyberspace, we have to know and accept that those aspirations are not necessarily universal, and our aspirations will have to meet with European, American, Asian…aspirations before we can settle upon a general body of principles and laws that should govern Internet behaviour.

- *Achieving the broadest possible forms of international co-operation among states in the detection and prevention of cybercrime and in the pursuit, arrest and prosecution of cybercriminals should be a major goal of any international convention on cybersecurity.*

The biggest dilemma in policing, pursuing and prosecuting for cybercrimes lies in the difficulty of resolving the questions of jurisdiction, sovereignty, the applicable law and the forum of trial. Therefore, an important measure of the quality and efficacy of any international instrument on cyberlaw is the extent to which it encourages and achieves the co-operation of as many states as possible in making mutually reciprocal undertakings for the enforcement of the convention (as domesticated) within their geographical borders. It is no surprise therefore that one-third of the Budapest convention is devoted to International Co-operation, Extradition and Mutual Legal Assistance.

The African Union Draft Convention disposes of this important aspect of international cyberlaw in one paragraph:

"*Article III – 1 – 7: International cooperation*
Each Member State shall adopt such measures as it deems necessary to foster exchange of information and the sharing of quick, expeditious and reciprocal data by Member States' organizations and similar organizations of other Member States with responsibility to cause the law to be applied in the territory on bilateral or multilateral basis".

- *An African convention on cybersecurity should be an abstraction of broad principles rather than a prescription of definitive propositions of law.*

The rationale for this is self-evident as it is fairly well established in international legislative drafting. First, and most importantly, the convention is supposed to be a representation of the aspirations of (and is supposed to appeal to) all the countries that are members of the African Union. These countries have varying legal, political and of course value systems. The danger with making definite prescriptions is that the convention will quickly contradict one or other aspect of the domestic legislation in a number of countries.

Secondly, African Union member states need to see that some room has been left for them to domesticate the convention by incorporating into their own laws legal provisions that are nuanced to their country's unique circumstances while preserving the broad principles expressed in the convention. This legislative leeway is constrained when the text of an international convention begins to read like an Act of Parliament (see my comment no. 5 on the Draft Convention in part II of this article).

While the preamble to the Draft African Union Convention is very articulate in identifying the values and general principles that should inspire domestic legislation on cybersecurity, what happens after the preamble is carnage. The language acquires a certain patchiness, clarity and beauty expression is lost and the soul of the convention is progressively diluted with a rambling set of definitions that excludes many other terms of art used in the text and statements that are sometimes unintelligible and grammatically uninspiring.

To be fair though, the Convention does attempt to get it right when in Article III it states:
Article III – 1 – 19: Harmonization: Each Member State shall ensure that the legislative measures adopted in respect of material and procedural provisions on cyber security reflect international best practices and integrate the

minimum standards contained in extant legislations in the region at large so as to enhance the possibility of regional harmonization of the said legal measures.

However, the 'international best practices' and 'minimum standards' of legislation that this article is referring to are exactly what the text of the Convention should be about. If African union member states are to look elsewhere for international best practices in cyberlaw legislation, then what would be the need for an African Union Convention on Cyberlaw?

- *The foremost purpose of an international legal framework on cybersecurity is a free, secure, empowered and advancing information society – not to foster e-commerce.*

This proposition goes to the very soul of cyberspace and to the existential inquiry separating those who describe the sum total of the human interactions taking place there as an information economy and those who describe and see it as an information society. Looking at its early beginnings as ARPANET, to the character of what accounts for most of the present-day human interactions in cyberspace (social networking) and to what is seen as the character of those interactions in the cyberspace of the future, it is a bit of a vulgarity to view and describe cyberspace as the fulfillment of our wildest commercial desires. The *zeitgeist* of cyberspace is not embodied in the electronic shopping cart but in the cultural, intellectual, ethical, spiritual and political open space that it has created for humanity. Therefore, the reference point for all inquiry about making cyberspace a secure space should not be the tired old conference refrain: 'to foster e-commerce'. Rather, it should be to preserve and even expand the freedom, openness and neutrality of cyberspace as a space for individual and group self-expression, innovation and interaction.

While the Preamble to the Draft African Union Convention rightly observes the great need to "build an information society that respects values, protects rights and freedoms, and guarantees the security of the property of persons, organizations and nations", the text of the Convention does violence to this approach when it boldly and abruptly begins with …..drum roll….. "Organization of Electronic Commerce". The information economy is only the market place corner of cyberspace. In the hierarchy of treatment of the different subject matter of cyberlaw, it should be subordinated to the elements that define the soul of the information society – the online protection of the human freedoms of self-determination, expression and privacy, the protection of net neutrality and openness, bridging the digital divide, etc.

End of part I

Part II: Specific Comments on the Text of Pertinent Articles of the Convention

In this part, I have included a verbatim statement of the Articles of the Convention that in my opinion need to be re-considered, followed by a statement of my reason why I hold that opinion.

"Article I – 2: Electronic commerce is an economic activity by which a person offers or provides goods and services by electronic means".
Comment1: Any complete definition of e-commerce – or any form of commerce for that matter – would include both the seller and the buyer/consumer's sides of the transaction. This definition only includes the seller side - 'economic activity by which a person offers or provides goods and services by electronic means'. Perhaps a better attempt at the definition would have used the terms: '…offers and receives..'.

"Article I – 3: The activities defined in Article 1 – 2 of this Convention shall be exercised freely in the African Union space except:
1) Gambling, even in the form of legally authorized betting and lotteries;
2) Legal representation and assistance activities; and
3) Activities exercised by notaries in application of extant texts".
Comment2:
- My understanding of this Article is that its purpose is not to criminalize gambling or the other two activities listed under it – vaguely worded as they are – but to provide that those activities are not to be regarded as e-commerce in any context in which that term is used in the Convention and/or, presumably, in any domestic law of the state parties.

- Having said that, this Article presumes the universality (or is it 'Africanality'?) of the term 'Notary'. Though the concept may be well known in African countries, it may be known by different terms in different terms. The term notary might be more widespread in Commonwealth countries than in other countries. It is therefore a term with fairly limited use. Perhaps it should not be used at all – plain language should be used to define the

concept – or if it is used, a definition of it should be provided in the definition section of the Convention.

- Finally, why does the exclusion from the definition of e-commerce only restricted to legal services – legal representation and the notarization of 'extant texts' – and what by Jove is an 'extant text'?

"Article I – 4: Without prejudice to other information obligations defined by extant legislative and regulatory texts in African Union Member States, any person exercising the activities set forth in Article I – 2 of this Convention shall provide to those for whom the goods and services are meant, easy, direct and uninterrupted access using an open standard in regard to the following information….whether the person is subject to value added tax"

Comment3:

- What is 'open standards?". This is a term of art which would be included in the definition section. I presume that it is meant to refer to the use of non-proprietary standards.

- Technological neutrality – The Convention appears to absolutely decree the use of 'open standards' in e-commerce. Technological neutrality for the purposes of this Convention should mean refraining from prescribing any form of technology, including open technology. Freedom of choice is an inalienable right for both the consumer and the seller. It should be left to the market to decide what technology is preferable. The right is an absolute right to choose technology. To define it as the right to choose from open technology is to patronize the players in e-commerce and to restrict a very basic human and economic freedom.

Comment4: value added tax is another term of art. Though the idea of a tax levied on goods and services and collected at the point of sale may be universal, the term 'value added tax' is not necessarily used by all African countries to describe it. Perhaps a more generic description would have been used or alternatively, a definition of the term provided in the definition section.

"Article I – 7: The activity defined in Article I – 2 of this Convention shall be subject to the laws of the African Union Member State on the territory of which the person exercising such activity is established, subject to the intention expressed in common by the said person and the recipient of the goods or services."

Comment5: Domestic legislation

Fair enough, e-commerce shall be regulated by the laws of the member states. However, there are two important points here: first, there are many provisions of this Convention that either contradict existing laws of member countries or at the very least, constrain the freedom of member countries to fashion their own e-commerce laws. Secondly, considering the different processes through which international treaties and conventions are domesticated into law in member states (In pure monist states the principles of international law become part of the domestic law immediately the treaty is ratified and in a dualist state, the principles only become domestic law after they have been formally adopted through a domestic legal instrument/legislative exercise. Many monist states would not be coaxed into ratifying a Convention that directly conflicts with domestic legislation and both dualist and monist states would shy away from a Convention whose prescriptions leaves little room for domestic legislative leeway.

"Section III: Publicity by electronic means. Article I – 8: Any publicity action, irrespective of its form, accessible through on-line communication service, shall be clearly identified as such. It shall clearly identify the individual or corporate body on behalf of whom it is undertaken."

Comment6: Net Anonymity

Anonymity is not only hard-wired into the architecture of cyberspace, it is also the best technological expression of the individual right to self-determination and privacy. Attempting to legislate against net anonymity is therefore not only futile but against the declaration of freedom of cyberspace. No person should be compelled to reveal his or her identity online. Moreover, no cyber-citizen should have their freedom of choice limited to only those services for which the providers have provided their identity.

"Article I – 9: Publicity actions, especially promotional offers such as price discounts, bonuses or free gift, as well as promotional competitions or games disseminated by electronic mail, shall upon receipt be clearly and unequivocally identified in the title of the message by their addressees or, where this is technically impossible, on the body of the message".

Comment7: Legislative overkill

This provision is so specific in its wording as to leave little to the imagination of domestic lawmakers. It should scarcely be in the place of an international convention to make provisions regulating promotional offers, price discounts, bonuses…..

"Article I – 12: The provisions of Article I – above notwithstanding, direct prospection by electronic mail shall be permissible where: 1) Where the particulars of the addressee have been obtained directly from him/her; and 2) The direct prospection concerns similar products or services provided by the same individual or corporate body."

Comment8: Can't prior consent be legally solicited?

So this provision seeks to outlaw the sending of solicitous spam mail – fair enough, but how does one obtain the 'prior consent' of the individual without being caught by the provision – i.e. without 'prospecting' for the consent? Would it not be more practicable (and perhaps even advantageous to the consumer) instead to presume that prior consent has been given until the consumer opts out or waives the consent? When I am walking on the street, I don't hold a sign up saying 'I don't consent to the solicitations of street-side vendors. Instead, I decline or ignore their solicitations or avoid that part of town altogether. All I care for the government to do is to ensure that the vendor respects my 'no' answer (anti-harassment and privacy laws) and that the laws regulate street-side vending. As I surf down cyberspace central, its enough for me to know that I have access to technologies that enable me to opt out of unsolicited communications –and to opt in as I might in exercise of my freedom of choice – and that I have laws that protect me from trespass into my corner of online cyberspace.

"Article I – 17: The information requested for the purpose of concluding a contract or information available during contract execution may be transmitted by electronic means where the addressee of such information has agreed to the use of the said means."

Comment9: Presumption in favour of electronic communications.

This is the age of information technology. It would be fair to make a presumption in favour of the acceptability of electronic communications, rather than to require that the person preferring to receive a communication by electronic means should expressly give prior notice of that preference to the sender. It should be presumed that the use of electronic communications is proper unless the recipient has previously expressly stated a preference for an alternative means of communication.

"Article 1 – 18: Information meant for a professional may be addressed to him/her by electronic mail provided he/she has communicated his/her electronic professional address.

Comment10: What is the purpose of this provision and who is a 'professional'?..

"Article I – 19: A service provider or supplier, who offers goods and services in professional capacity by electronic means, shall make available the applicable contractual conditions in a way that facilitates the conservation and reproduction of such conditions. The offer shall comprise:

1) The various stages to be followed to conclude the contract by electronic means;
2) Such technical facilities as would enable the user to identify the errors committed in data input and to correct such errors prior to conclusion of the contract;
3) The languages to be used for concluding the contract;
4) Where the contract is to be lodged, the modalities for this action by the author of offer and the conditions for accessing the contract so lodged;
5) The means of electronic consultation of the professional and commercial rules by which the author of the offer intends to be guided, if need be".

Comment11: Freedom of contract.

Contracts are by definition agreements of a commercial nature between two or more persons. While provisions can and should be made for the protection of consumers, this has to be balanced with the doctrine of freedom of contract, the operation of which would mean that no law should prescribe the format of or the provisions that should be contained in a contract. The exceptions to this would be controlled contracts for which domestic law makes special provisions either for regulating a profession and protecting consumers. For instance, in may commonwealth countries, contracts for the sale of land cannot be made exclusively verbally – there has to be a memorandum or some other thing in writing to evidence the contract. In deference to the doctrine of freedom of contract, these exceptions would be identified in domestic law. As such, the Convention would not prescribe a template by which all e-commerce contracts

have to be prepared.

"Article I – 22: Agreements concluded between professionals may be exempted from the provisions of Articles I – 20 and 21 of this Convention."
Comment12: So who is a 'professional'?

"Article I – 23: In the absence of legal provisions to the contrary, no person shall be compelled to take a legal action by electronic means."
Comment13: The right to choose not to use technology
Even though it may not be clear what 'a legal action' is supposed to mean for the purpose of this provision, I would agree with the general principle that the individual's freedom of choice includes the right to choose not to use technology. That freedom would extend not only to legal action but any other actions that can conceivably be reasonably done without electronic means.

Article I – 25: The following acts shall be exempted from the provisions of Article I - 24 of this Convention:
1) Acts under the signature of a private individual, relating to family law and law of succession; and
2) Acts of civil or commercial nature under the signature of a private individual, relating to personal or real security, except where such acts have been established by a person for the purposes of his/her profession."
Comment14: Real property?
What is the term 'personal or real security' meant to refer to? Did the Convention mean to refer to 'personal or real property' in solidarity with many domestic laws ?

"Article I – 26: The written matter emanates from a sequence of letters, characters, figures or all other signs and symbols with intelligible meaning, regardless of their base and transmission modalities."
Comment15: Written matter in electronic form does not have to be intelligible
It should not be the business of any law to prescribe the form of communication that individuals may engage in. There is no law generally forbidding the transmission of unintelligible matter in any form. (If there was then whoever emailed me this Convention would have committed a serious violation that law!). There equally should be no law forbidding the transmission of such matter between two people by electronic means. Two consenting individuals should have the liberty to communicate in gibberish if they so please as they should be to use representations of information that may not be conventionally intelligible.

"Article I – 30: The requirement to transmit several copies of a written matter shall be deemed to have been met, where the said written matter can be printed by the addressee."

Comment16:Meaning, purpose and technological neutrality: What is the meaning or purpose of this provision?
What is 'written matter'? Does it include matter that is written in electronic format? If it does, then does it mean that if a document is print-disabled, sending copies of it to various people by email does not amount to 'transmitting several copies'?
In deference to technological neutrality, instead of 'printed', perhaps the term 'reproducing or rendering in material form' might be more appropriate. Alternatively, a definition of the term printing may be provided in the interpretation section.

"Article I – 31: A written matter in electronic form shall be admissible for the purpose of invoicing, on equal terms as paper based written matter, provided the authenticity of the origin of the data therein and the integrity of the content are guaranteed."
Comment16B: Legality of electronic records
Without the need to go into excesses of language, it suffices to state generally, as the UNCITRAL Model Law on Electronic Commerce does, that if any law provides for anything (not just invoicing) to be done in writing, then that law shall be deemed to be complied with if the presentation of the information required to be written is done in electronic format.

"Article I – 35: Where the legal provisions of Member States have not laid down other provisions, and where there is no valid agreement between the parties, the judge shall resolve proof related conflicts by determining by all means possible the most plausible claim regardless of the message base employed.

Comment17: Meaning and purpose?
What is the purpose of this clause and what does it mean?

"Article I – 39: Subject to legal provisions to the contrary, no one shall be compelled to undertake a legal act by electronic means."
Comment18:Repetition
This is a repetition of Article 1-23

"Section II: Legal framework for personal data protection. Chapter 1: Objectives of this Convention with respect to personal data
Article II – 2: Each Member State of the African Union shall put in place a legal framework with a view to establishing a mechanism to combat breaches of private life likely to arise from the gathering, processing, transmission, storage and use of personal data. The mechanism so established shall ensure that any data processing, in whatsoever form, respects the freedoms and fundamental rights of physical persons while recognizing the prerogatives of the State, the rights of local communities and the interest of enterprises."
Comment19:Meaning
What is the 'the interest of enterprises'?

"Article II – 16: The protection authority shall comprise parliamentarians, deputies, senators, senior judges of the Tribunal of Accounts, Council of State, Civil and Criminal Appeal Court, personalities qualified as a result their knowledge of computer science, as well as professional networks or sectors."
Comment20: Legislative overkill
The best (or is 'worst') example of the Convention's invasive approach to domestic legislation runs from this Article to Article 27. Not only does it decree the creation of a special authority to protect personal data, it goes on to prescribe the individuals/institutions that should comprise its membership (no consideration being made of the inquisitorial judicial approach used in civil law countries versus the adversarial approach used in Commonwealth countries, or the separation of powers among the three arms of government, the Article provides for the Judiciary arm to be represented in the membership of the special authority) how the Authority shall exercise its functions, invoking the authority's allegiance to the Convention rather than to the relevant domestic law, providing for infringing conduct and prescribing punishments.

"Article II – 17: Sworn agents may be invited to participate in audit missions in accordance with extant provisions in Member States of the African Union.
Comment21:Meaning and purpose
What is the meaning and purpose of this Article? Who is a 'sworn agent'?

"Article II – 19:
Membership of a protection authority shall be incompatible with membership of Government, the exercise of the functions of enterprise executive and shareholding in enterprises of the computer or telecommunication sector."
Comment22: Self-contradiction
Presuming that this Article means that a person in Government or in the computer or telecommunication sector may not serve in the protection authority, would that not be contradicting Article II-16 which provides for certain Government offices to be represented in the authority?"

"Article II – 20: Members of a protection authority shall enjoy full immunity for views expressed in the exercise or on the occasion of the exercise of their functions. Members of the protection authority shall not receive instructions from any authority in the exercise of their functions.
Comment23:
Different member states may have different domestic laws governing the establishment of state-sponsored institutions – such as the protection authority. It would suffice to leave the member states to use such domestic laws to make provisions for the status, functions and operations of the protection authority.

Part IV: Obligations relating to the conditions governing the processing of personal data. Chapter 1: [This part proceeds to give six principles titled "Basic principles governing the processing of personal data". Under each principle, some explanatory text is given which includes very particular statements that would best serve as

the text of domestic law. The principles are: a. Consent and legitimacy; b. Honesty c. Objective, relevance and conservation of processed data; d. Accuracy; e. Transparency; f. Confidentiality and security

Comment 24: Broad and purposive statements

It should suffice to just state the principles in broad terms and leave the rest of the legislative magic to domestic legislation.

"PART III – COMBATING CYBER CRIME. Section 1: Basic principles. Chapter 1: Definitions. Article III – 1: For the purpose of this Convention: …3) Racism and xenophobia in ICTs means any written matter, picture or any other representation of ideas or theories which advocates or encourages hatred, discrimination or violence against a person or group of persons for reasons of race, color, ancestry or national or ethnic origin or religion, where these serve as pretext for either racism and xenophobia or as motivation thereof."

Comment 25

A definition of a term is not complete if that term is included in the definition. Here we have a definition of the term 'racism and xenophobia' that includes the words 'racism and xenophobia'.

"Chapter 1: National cyber security framework

Article 1: National policy Each Member State, in collaboration with key stakeholders comprising all levels of Government, industry and professional organizations, the civil society and citizens in general, shall put in place a national cyber security policy which recognizes the importance of essential information infrastructure for the nation, identifies the risks facing the nation in using the all-risk approach and broadly outlines the way by which the objectives are to be implemented."

Comment26: It would suffice to state the broad subject matter of the policy that states are required to pass. States need not be patronized about what procedures they will use to formulate the policy and the composition of the consultative group that will be involved.

"Article III – 1 – 3: Democratic principles: In adopting legal measures in the realm of cyber security and establishing the framework for implementation thereof, each Member State shall ensure that the measures so adopted will not compromise the rights of citizens guaranteed by their national constitution and protected by international conventions, especially the African Charter on Human and Peoples' Rights, and other rights such as freedom of expression, respect for private life, the right to equitable education, etc."

Comment27: There should be no place for that tenuous term 'etc.' in any legal instrument, much less in an international convention….and to use it in reference to human rights is to aggravated the injury.

"Article III – 1 – 5: Harmonization: Each Member State shall ensure that the legislative measures adopted in respect of substantive and procedural provisions on cyber crime reflect international best practices and integrate the minimum standards contained in extant legislations in the region at large so as to enhance the possibility of regional harmonization of the said legal measures.

Comment28: The broad principles that define the 'international best practices' referred to here are what the convention should be about, and no more.

"Article III – 1 – 6: Double criminality

The cardinal principle of cooperation in the application of the law against cross-border crime reposes on the fact that the laws under which such cooperation is sought by each Member State should be uniform in terms of prohibited conduct and application procedure. Each Member State shall adopt such legal measures as respect the principle of double criminality.

Comment29: What is 'the principle of double criminality'? It could have been included in the definitions section of the convention."

"Article III – 1 – 12: Public awareness-raising

1) Each Member State shall adopt an effective national cyber security awareness building programme with a view to promoting cyber security awareness in the public and key stakeholders; establish relation with cyber security professionals for the purpose of sharing information on cyber security initiatives and developing collaboration on cyber security issues.

2) During development of awareness-raising programme, Member States shall take

into account:
i) Stakeholders' support and commitment to develop and establish relations of confidence between industry, Government and the academia for the purpose of scaling up the level of cyber security awareness;
ii) Coordination and collaboration on cyber security activities in the entire
government outfit; and
iii) Communication with bodies both internal and external: other governmental agencies, industry, educational institutions, domestic computer users and the wider public.
3) To raise the level of awareness on cyber security issues, political leaders and other cyber security stakeholders shall:
i) Establish public-private partnerships when necessary;
ii) Launch large-scale publicity campaign to reach out to the greatest possible number of persons;
iii) Use NGOs, institutions, banks, FAI, bookshops, local commercial organizations, community centers, computer shops, community colleges and adult education programmes, school as well as parents' associations to inculcate the message of appropriate cyber comportment."
Comment30: This article is another good (or is it 'bad'?) example of legislative overkill. It would be enough to merely oblige states to conduct public information, education and awareness campaign on cybersecurity. The prescriptions on how the campaigns should be done and the institutions that should be engaged in the campaigns are legislative presumptuousness.

"Article III – 1- 14: Institutional framework
1) Each Member State shall adopt such measures as its deems necessary to establish appropriate institutions to combat cyber crime, conduct surveillance in response to cyber crime incidents and early warning, for coordination of national and cross-border cyber security problems and for global cooperation.
2) Organizational structures may assume any of the following forms: National Cyber Security Council (NCC), National Cyber Security Authority (NCA) and a National CERT and/or CSIRT. Each Member State may adapt its structures for the purpose of introducing "a specific adjustment" depending on their level of ICT development, availability of resources and of public-private partnerships. These structures may exist under other or different nomenclatures."
Comment31:If NCCs, NCAs, CERTs and CSIRTs are different institutional models for combating cybercrime, what is the definition and profile of each one of these and what makes each model different from the other? What are the full forms of the terms CERt and CSIRT?

"Article III – 9: Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of using the data obtained with a full knowledge of a case."
Comment31: What does this mean?

"Article III – 11: Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact, even out of negligence, of processing or causing the processing of personal data without having undertaken the preliminary formalities for the processing as prescribed by the law on personal data enacted to that effect in each Member State."
Comment33: Provisions have been made elsewhere in the convention on personal data protection – rather than or in addition to referring states to their domestic laws on this subject, this Article should also have made to those provisions of the Convention.

"Article III – 12: Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of producing, selling, importing, possessing, disseminating, offering, ceding or circulating a computer equipment, programme, any device or data designed or specially adapted to commit an offense, or a password, access code or similar computerized data allowing access to the whole or part of a computer system."
Comment34: There are many acts of 'producing, selling, importing, possessing, disseminating, ceding, or circulating a password, access code ... or data allowing access to a computer system' that do not infringe on a private right or a public good. Indeed, there are many instances of those acts that are essential and native to the operation of a computer system. Online service providers generate and give passwords to their users; individuals share their access codes to computer data with trusted friends or relatives; employers give shared access codes to a common online resource accessed by their employees, etc. The rationale behind criminalizing such innocuous acts is either poorly conceived or lost in the obscurity of the language used in the Article.

"Article III – 17: Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of facilitating access to pictures, documents, sounds or representation of pornography of a minor. "
Comment35: Consistency in the use of terms. 'Child pornography', 'infant pornography' and 'pornography of a minor' have been used to interchangeably apparently to refer to the same thing. Consistency in the use of technical terms is essential for clarity of legislation.

"Chapter II: Adapting certain information and communication technologies offenses Section 1: Violation of property
Article III - 24: Each Member State of the African Union shall take the legislative measures required to set up as an aggravating circumstance the use of ICT to commit common law offenses such as theft, fraud, possession of stolen goods, abuse of trust, extortion of money, terrorism, money laundering, etc."
Comment36: If the use of the term 'common law' here is meant to refer to the common law-versus-civil law dichotomy, then its use is an anachronistic faux pas considering that the African Union is comprised of states with varying legal systems – common law, civil law, Islamic, customary law, etc. The term has been used again in Article III-29.

"Article III – 26: Each Member State of the African Union shall take the legislative measures required to expressly include "means of digital electronic communication" such as the internet in the enumeration of the public dissemination facilities defined in the penal texts of Member States."
Comment37:Would it not suffice to merely provide for Member States to legislate the legal recognition of electronic documents, whatever the means of their dissemination?

"Article III – 26: Each Member State of the African Union shall take the legislative measures required to expressly include "means of digital electronic communication" such as the internet in the enumeration of the public dissemination facilities defined in the penal texts of Member States. "
Comment37:Would it not suffice to merely provide for Member States to legislate the legal recognition of electronic documents, whatever the means of their dissemination?

"Article III – 27: Each Member State of the African Union shall take the legislative measures required to expressly integrate the new intangible facilities such as "digitalized data" or "computerized files" which have to be kept secret in the interest of national defense.
Comment38: What states usually keep secret is certain types of information. 'Digitalized data' and 'computerized files' are but the medium in which that information is stored. If legislation needs to be made to protect such media, it would take the form of restrictions on access to protected systems which have been designated to be critical national defence infrastructure because they store computerized files containing critical national security information."

"Article III – 31: Each Member State of the African Union shall take the measures required to ensure that the offenses defined in this Convention attract maximum prison sentence of one (1) to five (5) years at least.
Comment39:The Convention need not restrict the liberty of Member States to prescribe the appropriate sentences. Even if it were appropriate for the convention to prescribe a maximum sentence for any offence, it is a misnomer to give, as this Article purports to do, two 'maximum' sentences. What is the need for the reference to one (1) year when five (5) years is also prescribed? Would it not suffice to state instead that the maximum prison sentence should be five years? Or did the Convention intend to prescribe one years as the minimum and five years as the maximum?"

"Section II: Other penal sanctions. Article III – 33: Each Member State of the African Union shall take the measures required to ensure
that, in the event of conviction for an offense committed by means of digital communication facility, the

investigating jurisdiction or the judge handling the case gives a ruling imposing additional punishment."
Comment40: What 'additional punishment'? Any provision of law giving any authority to impose a punishment should meet the highest standard of clarity. Judicial discretion in the meting out of punishments for offences should be discretion in the severity and not in the type of sentence to impose. This Article also contradicts Article III-31 which prescribes a maximum sentence for offences under the Convention.

"Article III – 34: Each Member State of the African Union shall take the measures required to set up as a penal offense, the violation of the aforementioned prohibitions pronounced by the judge."
Comment 41: It is fairly well established now that the disobedience of court orders is contrary to the law and every state would have a procedure for enabling the courts to enforce compliance with their own orders. Orders with respect to cybercrimes. No special legislation needs to be enacted in this regard for the enforcement of orders issued by a court in a cybercrime case.

"Article III – 35:
Each Member State of the African Union shall take the measures required to ensure that, in the event of conviction for an offense committed by means of digital communication facility, the judge handling the case makes a further binding ruling for the dissemination of the decision by extract and via the same facility at the expense of the convicted person, in accordance with the modalities prescribed in the legislations of Member States.
Comment 42: My understanding of this provision: African Union countries are required to provide, for instance, that if subject A posts a xenophobic article on his blog or social media profile, then if he is tried and convicted for the offence of publishing xenophobic material, he is to post the ruling of the court on his blog or his social media page at his own expense. It find nothing wrong with the merits of this provision, but it can be drafted with better clarity."

"Section III: Procedural law. Article III – 36: Each Member State of the African Union shall take the measures required to ensure that where the data held in a computer system or in a facility that allows for the conservation of computerized data in the territory of a Member State, are useful in revealing the truth, the investigating judge can conduct a search or access a computer system or part of the system or any other computer system where the said data are accessible from the original system or available to the initial system."
Comment43:In countries that have a system of law descended from the British Westminster system (Common Law countries) courts use the adversarial system of resolving disputes with judges being merely arbiters and not investigators of the claims presented to them. This is compared with Civil Law countries which have an inquisitorial approach to judicial decision making in which judges take an active part in discovering evidence. This Article (as well as Article III-37) wrongly presumes the universality of the latter system among African Union member states.

Posted 20th August by Michael Murungi

0 Add a comment

Enter your comment...

Comment as: Google Account

Publish Preview