DIARRA Rosalie

Email: rosadiarra2005@yahoo.fr

Affiliation: Jesuit University of Abidjan/ CERAP

Contact: +225 (07 19 93 46) 08 BP 2088 Abidjan 08

Title: CYBERSECURITY AND LEGAL INNOVATIONS IN WEST AFRICA

ABSTRACT

The digitization of African countries and particularly those in West Africa is a new opportunity for development that is offered to them. This situation also makes cyberspace insecure a reality. States must then act to secure this space in order to protect populations and also to ensure development. One of the answers is the legal one. As the digital environment is refractory to the traditional laws made for the physical world, new adapted laws are expected. This reflection analyses the weakness of the classic cyber security laws in West Africa, particularly in the fight against cybercrime. It sets out the new laws adopted by States and their innovations in cyber security. Because new laws have weaknesses, states still have to innovate by reinforcing them in order to adapt to the realities of cyberspace. It is therefore normal to ask the following question: What are the advances made by new legislations?

The consequence of Information and Communication Technology (ICT) developpement is digitalization of all the states of world. African states are not on the margins of this dynamic of the 21st century and have adopted policies for ICT growth among them to ensure the security a well-being of the populations. If this reality allows states to be on the way to emergence, it is still important to note that technologies represent a certain danger if security measures are not taken and enforced by the states. African states are particularly threatened by cyberspace insecurity. One of the most prominent of which is cybercrime. To provide a secure digital environment, states are increasingly adopting cybersecurity measures that include legislation to combat cybercrime. This action seems necessary because the classical laws made for non virtual world are not able to govern cyberspace which has its own realities. The laws of African states must then innovate to adapt and provide a secure digital environment. It is with this in mind that the African Union has adopted the "African Union Convention on Cybersecurity and Personal Data Protection" in 2014. In West Africa in particular, a Directive was adopted by the Economic Community of West African States (ECOWAS) to secure cyberspace by combating cybercrime. This part of the continent is not on the margins of a generalized dynamic of finding solutions for the introduction of a secure digital environment.

What are the advances made by new legislations? What are the innovations to do? This reflection aims at analyzing the cybersecurity legislations in West Africa and to appreciate the novelties brought as well as the challenges to be met so that the technologies are used in a secure context. It is then interesting to discover the measures adopted by the West African States in the area of cyber security, particularly in the fight against cybercrime (I). The progress made by these new legislations is analyzed (II). Finally, this reflection presents the challenges to be faced despite the existence of new legislations (III).

This study was realized by the method of comparative law which makes it possible to analyze the legislations of different countries. In concrete terms, West African legislations were collected, analyzed and compared to deduce the conclusions of the article.

This method made it possible to identify the cybersecurity situation in the countries. The convergences, divergences, strengths and weaknesses of the legislations have been discovered with a view to proposing adapted solutions.

TREE 2018, March 21-22, Abidjan, Côte d'Ivoire
Copyright © 2018 EAI
DOI 10.4108/eai.21-3-2018.2275684

I-LEGISLATIONS TO COMBAT CRIME IN WEST AFRICA

West Africa has 16 countries. Table 1 makes a presentation of legislations to combat cybercrime in this part of the continent.

I.1 Table 1: Point on legislations to combat cybercrime in West Africa[1]

Countries	Existence of Law on cybercrime	In force	Under the ECOWAS Directive on cybercrime	Adoption of the Directive on time (January 2014)
Benin	Yes partially	Yes	No	No
Burkina Faso	No	Draft	Yes	No
Cape Verde	No	Draft	No, Budapest Convention	No
Ivory Coast	Yes	Yes	Yes	Yes
Gambia	Yes partially	Yes	No	N/A
Ghana	Yes	Yes	No	N/A
Guinea	No	Draft	No	No
Guinea Bissau	No	No	No	No
Libéria	No	No	No	No
Mali	No	Draft	Yes	No
Mauritania	Yes	No Enforcement Decree	No	N/A
Niger	No	Draft	No	No
Nigéria	Yes	Yes	Yes	No
Sénégal	Yes	Yes	No	N/A
Sierra-Léone	No	No	No	No
Togo	No	Draft	No	No

I.2 INTERPRETATION

Table 1 shows that only five of 16 countries have legislation to combat cybercrime in West Africa. Two countries have partial legislation that does not cover all areas of crime. They still need to strengthen this partial legislation. In 2011, the Economic Community of West African States (ECOWAS) adopted a Directive[2] to combat cybercrime. The deadline for its transposition into domestic law by the States was January 2014. Of the five countries that have legislation to combat cybercrime, only Ivory Coast has transposed it into time (2013). Nigeria transposed it with one year late (2015). Ghana[3] and Senegal[4] have legislation adopted before the ECOWAS Directive. Mauritania is a West African country, but it is not concerned by the ECOWAS Directive because it has withdrawn from the community since 2001 but has a law since January 2016 which is waiting to be implemented. Despite the persistence of cyber threats, the Directive has not aroused enough acceptance on the part of the States. Although some countries have a bill. The problem is that the transformation of these provisions into law remains an uncertainty in the face of a rapid need for text to govern the increasing and multiformal risks of cyberspace. In addition, the existing bills do not all seek to transpose the ECOWAS directive. We could then question ourselves as to why States are not so interested in the community text while cyber-crime is wreaking havoc within them? The lack of political will can be the main reason for

[1] Some of informations in table 1 are extracted from African Union, Cybercrime & Cyber security Trends in Africa, published November, 2016 p. 53-55.
[2] Directive C/DIR/1/08/11 on combating cybercrime in the ECOWAS area, adopted at the regular session of the Council of Ministers in Abuja, Nigeria, 17-19 August 2011.
[3] Ghana has adopted its legislation on cybercrime since 2008.
[4] Sénégal also has adopted its legislation on cybercrime since 2008.

this situation. The inadaptability of conventional legislation in the face of cybercrime is the factor that explains the need to adopt new Laws. Table 2 shows the weaknesses of the laws governing the physical world in the face of cybercrime. It presents the innovations made by the new measures to secure the digital environment.

II-INNOVATIONS MADE BY LEGISLATIONS TO COMBAT CRIME

The limits of the old criminal laws have prompted States to build new legal frameworks to combat cyber offences. Table 2 shows at the same time the limits of the classical laws (substantive criminal law and criminal Procedure) as well as the replies of the laws to combat cybercrime.

II.1 Table 2: Classical and new legislations in the fight against cybercrime in West Africa

The weaknesses of the old laws		**New incriminations**	
Criminal law	**Criminal Procedure**	**Criminal law**	**Criminal Procedure**
-Attacks on information and communication Technologies - Inability to protect all property - Inability to protect intellectual property in cyberspace - Lack of classic laws in the face of cybercrimes	- Impossibility of search and seizure online - Lack of evidence-finding methods in computer systems	- Sanction of attacks on ICTs[5] -Sanctions for violations of information[6] - Reinforcement of some classic sanctions	- Admission of searches and seizures online -Computer requisitions -Interceptions - Fast Data Retention - Access to international computer systems

II.2 INTERPRETATION

Table 2 confirms the weakness of old laws to govern cybercrime. In substantial criminal law, the laws were incapable of sanctioning the attacks on ICTs as well as certain offences facilitated by them. In procedural matters it was impossible to search for evidence in the digital environment on the basis of the old legislations without being arbitrary. The perpetrators of the offences could not be punished. All of these reasons were therefore in favour of the proposal for appropriate legislation. That is why a Directive was adopted in West Africa by ECOWAS in 2011 and then a cyber security agreement at the African level in 2014. These texts have proposed an innovation of law by adapting measures to the realities of cyberspace. Thus, the confidentiality of computer systems is protected from breaches of their confidentiality (access and maintenance fraudulent), violations of their functioning (infringement of availability and integrity). The confidentiality of computer data is also protected against (falsification and computer fraud, interception and interference with computer data). The ECOWAS directive and the African Convention on Cybercrime also encourage States to adopt measures to protect personal data.

In procedural matters, the search for truth in the digital environment is possible with the admission of the search and seizure online as well as the adoption of new methods of finding evidence[7]. The electronic evidence is recognized by the new texts. All these measures help to combat the insecurity of the digital environment. However, it is important to note that there are still efforts to be made because the laws that exist still have limits.

[5] ICTS attacks are Fraudulent access and maintenance, interference with the operation of computer systems, infringement of data confidentiality.

[6] See legislations of Senegal, Ghana and Ivory Coast.

[7] On the subject of new methods of investigation, see Rosalie DIARRA "criminal laws tested by cybercrime in West Africa", thesis, Université Paris 1 Panthéon-Sorbonne, October 2017 p. 416-423.

III -CHALLENGES TO BE ADDRESSED BY THE LEGISLATION TO COMBAT CRIME IN WEST AFRICA

At this level, it is the limits of the standards as well as the problems that can hinder a security of the digital environment that are analyzed. Solutions are proposed in table 3.

III.1 Table 3: The challenges faced by existing legislation in West Africa

Challenges and solutions of criminal law		**Challenges and solutions of the criminal Procedure**	
Challenges of criminal law	Solutions	Challenges of criminal Procedure	Solutions
Measures to accompany criminal legislation	-Creation of national institutions for the protection of personal data - Creation of CERT National (Computer emergency Response Team) - Adoption of national legislation to combat cybercrime	-Insufficient methods of finding evidence -Inability to prosecute international offences - Difficulties in searching for evidence of violations at the international level	- Adoption of new evidence-finding measures to avoid arbitrary - Rethinking the laws of international criminal cooperation (surpassing them for the benefit of measures adapted to cyberspace)

III.2 INTERPRETATION

The table shows that challenges exist both in criminal law and in criminal proceedings. The solutions must be offered to States to make the fight against cybercrime a reality. In criminal law, it is true that some States have adopted legislation to combat cybercrime and the protection of personal data, but in reality these texts need to be supported by institutions of their implementation. This is the case for measures that protect personal data. Attacks on personal data in the context of automated treatments constitute cyber-crime. Of all the West African countries that have legislation to combat cybercrime, only a few have an independent[8] national structure to protect personal data. There are also a number of reasons for the lack of independent protection structures. Most of the protection structures that exist are not exclusively reserved for the protection of personal data[9]. This situation could make their protection ineffective. It should be noted that a rapid reaction of States is necessary because the abusive treatment of these data could adversely affect the privacy of citizens[10]. They may be victims of several abuses because of access to information that concerns them. Still at the level of criminal law, states which do not have specific legislation on cybercrime must adopt them quickly. If not, they will endanger the safety of people in the digital environment[11]. In addition, the creation of the Computer emergency Response Team (CERT National) will assist States in documenting threats and strengthening existing criminal provisions[12]. In Africa and particularly in

[8] See the CNIL which is an administrative authority for the protection of personal data in France.
[9] See Rosalie DIARRA "criminal laws tested by cybercrime in West Africa", thesis, Université Paris 1 Panthéon-Sorbonne, October 2017 p. 132-133.
[10] See LEROY (F.), « Réseaux Sociaux et Cle : Le commerce des données personnelles », Ed. Actes du sud, Avril 2013.
[11] See the table on the situation of States in the adoption of legislation to combat cybercrime.
[12] The role of CERT is to manage security incidents at the national level and to prevent risks. It ensures in addition a certain prevention by the spreading of security information. The information could lead to incriminating laws of certain acts.

West Africa, some states already have CERT although they do not have laws in force on cybercrime[13]. In procedural matters, it is important to note that the legalization of the standards of evidence search will help the actors to respect the legality. The non-existence of certain methods of finding evidence can push the actors to be illegal. In West Africa measures that are generally not provided by legislations are digital infiltration[14], data capture[15], the setting of encrypted[16] data[17]. In the field of international criminal cooperation, it should be noted that the West African States must provide enough effort to rethink their system of cooperation in order to adapt it to the realities of cyberspace. Indeed, the West African anti-cybercrime Directive recommends that States cooperate in the research and recognition of all criminal offences it foresees. It conditions this action in accordance with the traditional rules of cooperation[18]. The African Convention on cybersecurity and the protection of personal data do not solve the problem, as it recommends that states that do not have legal assistance measures to conclude[19] in order to assist in the search for truth in International level. The Convention also calls on States to base themselves on the standard of classical cooperation in the field of cybercrime[20]. It is clear that the laws of classical cooperation are incapable of combating crime in the digital environment[21]. Measures of international criminal cooperation such as mutual legal assistance, the Rogatory commission or principles such as double criminality are refractory to the sanction of cybercrime which requires rapid action[22]. The modalities of criminal cooperation for the sanction of cybercrimes must mainly be based on an adaptation of the traditional standards of cooperation to the realities of cyberspace[23].

In conclusion, it must be remembered that the realities of cyberspace require states to be on a permanent alert. They will be able to deal with the multiform realities of the offences. To provide a credible cyberspace for the realization of their activities to the people, the States must secure it by constantly innovating. This implies concretely that they must adopt standards to combat cybercrime and implement them effectively through the creation of necessary institutions. The digital world is one of the sure sources of development of the West Africa region and all of Africa. States must therefore be part of a dynamic of innovation to take advantage of the possibility of development proposed by cyberspace. Legal innovation is then one of the indisputable avenues of security to explore.

---

[13] See the point made by African Union, Cybercrime & Cyber security Trends in Africa, published November, 2016.

[14] Infiltration is an investigative technique that can play an important role in discovering evidence of Internet-organized gang offences such as money laundering, human trafficking, terrorism and child pornography etc

[15] This method of investigation allows by technical processes, to become acquainted with computer data and to record them without the knowledge of their owner.

[16] The encrypted data is a set of information rendered inaccessible by the author using an encryption process. The development of crime in the digital environment induces the use of the encryption technique by the offenders to operate peacefully within the States. The law must therefore enable the research actors to decipher them in case of investigations of serious crimes such as money laundering, human trafficking, terrorism.

[17] About the d"investigations measures to be adopted, See Rosalie DIARRA "criminal laws tested by cybercrime in West Africa", thesis, Université Paris 1 Panthéon-Sorbonne, October 2017 p. 424-427.

[18] See art. 33 of Directive C/DIR/1/08/11 on combating cybercrime in the ECOWAS area.

[19] Article 28 of the African Union Convention on cybersecurity calls on States to conclude bilateral or multilateral agreements.

[20] Idem.

[21] See the weaknesses of the ECOWAS Directive raised by Rosalie DIARRA, op.cit. p. p. 424-427.

[22] See the European Arrest warrant and its role in the fight against cybercrime.

[23] Rosalie DIARRA, op. cit. p.448-456.

REFERENCES

[1] DIARRA (R.) « Criminal laws tested by cybercrime in West Africa », University Paris 1 Panthéon-Sorbonne, October, 518 p (2017).

[2] African Union, Cybercrime & cyber sécurity trends in Africa, published November, (2016).

[3] QUEMENER (M.) et FERRY (J.), Cybercriminalité, défi mondial, Paris, 2eme Ed. economica, mars, 307p, (2009).

[3] QUEMENER (M.), CHARPENEL (Y.), « Cybercriminalité, droit pénal appliqué », édition économica, septembre, 259 p, (2010).

[4] ROSE (P.), « La criminalité informatique à l'horizon 2005: analyse prospective », édition l'Harmattan, 165p, (1992).

[5] TOURE (P. A.), le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal, Paris Ed. L'Harmattan, avril, 616 p, (2014).

[6] LALAM (N.), « La délinquance électronique », n°953, édition la documentation française, octobre, 120 p, (2008).

[7] LEROY (F.), « Réseaux Sociaux et Cle : Le commerce des données personnelles », Ed. Actes du sud, Avril, 263 p, (2013).

[8] FERAL-SCHUL Christiane, « Le droit à l'épreuve de l'internet », 5eme Ed. Dalloz, 15 octobre, 997 p (2008).

[9] KNOBEL (M.), « l'internet de la haine : racistes, antisémites, néonazis, intégristes, islamistes, terroristes et homophobes à l'assaut du web », Paris, Ed. Berg International, mars, 181p, (2012).

[10] LALAM (N.), « La délinquance électronique », n°953, édition la documentation, 120 p. (2008)

[11] VENTRE Daniel, cyberattaque et cyberdefense, collection cyberconflits et cybercriminalité, Edition Lavoisier, aout, 312 p, (2011).

[12] African Union Convention on cybersécurity personal data protection, (2014).

[13] Ghana, Electronic Transaction Act 772, 2008)

[14] Ghana Mutual Legal Assistance Act 807, (2010)

[15] Ghana Data Protection Act 843, (2012)

[16] Nigeria Cybercrimes Prohibition, Prevention Act, (2015).

[17] Senegal, Law N°. 2008-11 of 25 January on cybercrime (2008).

[18] Senegal, Law N°. 2008-12 of 25 January concerning the protection of personal data (2008).

[19] Additional Act A/SA 1/01/10 on the protection of personal data in the ECOWAS area, 16 February (2010).

[20] Directive C/DIR/1/08/11 on combating cybercrime in the ECOWAS area, Abuja, Nigeria, 17-19 August (2011)

[21] Ivory Coast, Law N°. 2013-451 of 19 June 2013 on cybercrime (2013).

[22] Ivory Coast, Law N°. 2013-452 of 19 June concerning the protection of personal data (2013).