

---

M.E.S., Numéro 131, Vol.2, novembre – décembre 2023  
<https://www.mesrids.org>  
Dépôt légal : MR 3.02103.57117  
N°ISSN (en ligne) : 2790-3109  
N°ISSN (impr.) : 2790-3095  
Mise en ligne le 18 novembre 2023

---



***Revue Internationale des Dynamiques Sociales***  
***Mouvements et Enjeux Sociaux***  
*Kinshasa, novembre - décembre 2023*

## LE DROIT COMMUNAUTAIRE AFRICAIN A L'ÉPREUVE DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ :

*Quel regard pour les États Africains ?*

par

**Olivier MANDUNGU NGYMA**

**ODETTIA MBUTAMUNTU MUNDEKE**

*(Tous) Assistants et Apprenants au 3<sup>ème</sup> cycle,  
Faculté des Sciences Sociales, Administratives et Politiques  
Université de Kinshasa*

### Résumé

*La lutte contre la cybercriminalité aujourd'hui constitue un défi international crucial pour tous les États du monde en général et en particulier les États Africains. En analysant les différents mécanismes législatifs de la lutte contre la cybercriminalité mis en place par les États Africains à travers les organisations régionales africaines, cet article soulève le problème de l'inadéquation du cadre législatif notamment les principes du droit communautaire africain dans la lutte contre la cybercriminalité au niveau africain. Vu la nature de la cybercriminalité, il est nécessaire d'étudier, à partir des perspectives africaines, les normes et institutions qui ont pour vocation d'encadrer, d'organiser et de réguler mais aussi de régler les différends qui mettent en cause les intérêts des divers acteurs intervenant dans le cyberspace africain. L'article souligne sur la nécessité de faire émerger une législation, une doctrine et une jurisprudence africaines qui contribuent au développement du cyberspace africain.*

**Mots-clefs :** *Doctrine, Cybercriminalité, Cyberspace, cybersécurité, Jurisprudence*

### Abstract

*The fight against cybercrime today constitutes a crucial international effort for all States in the world in general and African States in particular. By analyzing the different legislative mechanisms in the fight against cybercrime put in place by African States through African regional organizations, this article raises the problem of the inadequacy of the legislative framework, particularly the principles of African community law in the fight against cybercrime. Cybercrime at the African level. Given the nature of cybercrime, it is necessary to study from African perspectives, the norms and institutions which aim to supervise, organize and regulate but also to settle disputes which challenge the interests of various actors involved in African cyberspace. The article emphasizes the need to bring about African legislation, doctrine and jurisprudence which contribute to the development of African cyberspace.*

**Keywords :** *Doctrine, cybercrime, cyberspace, cybersecurity, jurisprudence*

### INTRODUCTION

Le développement contemporain des technologies de l'information et de la communication constitue un tournant majeur de la civilisation humaine. L'illustration la plus parfaite de l'essor des technologies numériques est sans nul doute l'avènement du réseau internet.<sup>1</sup> En effet, l'utilisation accrue des réseaux numériques, tel que l'Internet avec aujourd'hui près de deux milliards d'internautes, n'est pas seulement le fait d'individus bien intentionnés. Toute innovation technologique ouvre, en même temps, de nouvelles brèches dans lesquelles s'engouffrent les réseaux criminels. L'Internet est surtout un vecteur idéal pour faciliter les actions des délinquants, il permet d'accroître leurs profits en réduisant la prise de risques.

Aujourd'hui le recours aux réseaux numériques et en particulier à l'internet est une arme à double tranchant faite de perspectives positives mais aussi le risque et des menaces pesant sur l'activité des États, des Entreprises et sur la vie quotidienne des citoyens qui sont très souvent des internautes.<sup>2</sup> En effet, la plupart des grandes découvertes technologiques ont presque toujours engendré, à côté des progrès économiques qu'elles procurent à l'humanité, des retombées négatives parmi lesquelles figure en bonne place l'avènement de nouvelles formes de criminalité, Internet n'échappe pas à cette loi sociologique du développement.

<sup>1</sup> DUFOUR A., « internet : Que sais-je ? » éd. Le Temps des médias, Paris, 2000, p. 15

<sup>2</sup> Myriam Quemener., Cyber menaces, entreprises et internautes, éd. Economica, Paris, 2008, p. 86

Malgré le faible taux d'accès aux TIC en Afrique<sup>3</sup>, le passage de l'analogique au numérique a changé profondément la physionomie de la société traditionnelle qui s'est très vite transformée en une société de l'information.<sup>4</sup> Mais, l'essor des réseaux numériques a entraîné l'apparition d'une nouvelle forme de criminalité charriée par les premières lueurs de la société africaine de l'information, appelée « la cybercriminalité ». Fruit de la révolution numérique ou la mondialisation, la cybercriminalité se développe à grande échelle dans cet univers favorable, au point de viser aujourd'hui l'ensemble des infrastructures économiques et sociales.<sup>5</sup>

À l'heure où Internet s'imisce partout, y compris dans nos objets connectés au quotidien, la cybercriminalité à son tour monte en puissance, elle s'impose comme « la menace du XXI<sup>e</sup> siècle »<sup>6</sup> et pose aussi un défi d'une ampleur inégalée aux Etats dans le monde.

Il sied de relever que la cybercriminalité est clairement la nouvelle menace du XXI<sup>e</sup> siècle. Elle force les Etats à repenser leurs moyens d'action, à se mettre à niveau techniquement et à développer des cadres normatifs non seulement régionaux ou communautaires mais aussi transnationaux, car l'échelle devient mondiale. C'est sous cet aspect que le cyberspace est devenu criminogène. En effet, l'espace dématérialisé qu'offrent les TIC, notamment internet est de plus en plus le lieu virtuel de commission de divers agissements répréhensibles.<sup>7</sup> Le surgissement en Afrique de la cybercriminalité est symbolisé par le phénomène de l'escroquerie en ligne devenue une véritable menace pour le développement dans certains pays,<sup>8</sup> mais aussi de vols des données personnelles.

Ayant pris conscience des défis posés par la cybercriminalité dans le continent et ayant décidé d'apporter des réponses de politiques criminelles à ce fléau au niveau communautaire, l'Afrique s'est organisée dans le cadre du droit communautaire à pouvoir légiférer sur la matière, ce qui expliquerait par exemple, la prolifération de plusieurs cadres législatifs relatifs à la cybercriminalité produit par les instances des certaines organisations communautaires notamment : dans le cadre de l'Union Economique et Monétaire Ouest Africaine (UEMOA), on peut citer la loi uniforme n°2008-48 du 3 septembre 2008, relative à la répression des infractions en matière de chèque, de carte bancaire et d'autres instruments et procédés électroniques de paiement.<sup>9</sup> La Communauté Economique des Etats de l'Afrique de l'Ouest (CEDEAO) a adopté un acte Additionnel A/SA. 2/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel.<sup>10</sup> Lors de sa 66<sup>e</sup> session tenue à Abuja (Nigeria) les 17 au 19 août 2011, le conseil des Ministres de la CEDEAO a adopté la Directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO.<sup>11</sup> Dans l'espace de la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC) et de la Communauté Economique des Etats de l'Afrique Centrale (CEEAC), certains instruments juridiques abordent certains enjeux liés au phénomène cybercriminel. Il s'agit de la directive n°07/08-UEAC-133-CM-18 du 19 décembre 2008 fixant le cadre juridique de la protection des droits des utilisateurs de réseaux et des services de communications électroniques au sein de la CEMAC<sup>12</sup> et du Règlement n°02/03-CEMAC-CM du 04 avril 2003 relatif aux systèmes, moyens et incidents de paiement qui incrimine les atteintes aux systèmes de paiement.<sup>13</sup> Dans l'espace de l'Afrique centrale, la deuxième réunion des Ministres en charge des télécommunications et

<sup>3</sup> BOYER J., « la révolution d'internet », in Internet face au droit, Cahier du CRID, Bruxelles, Story Scientia, 10 novembre 1999, n° 224, p. 11

<sup>4</sup> CAPELLER W., « un net pas très net » in l'immatériel et le droit, n°143, p. 167

<sup>5</sup> Myriam Q., « Concilier la lutte contre la cybercriminalité et l'éthique », in Sécurité et stratégie, 2011, p. 67

<sup>6</sup> GHERNOUTI-HELIE (S.), La cybercriminalité : le visible et l'invisible, éd. Presses Polytechniques et Universitaires Romandes (PPUR), Lausanne, 2009, p. 42

<sup>7</sup> QUEMENER M. et FERRY J., cybercriminalité : défis mondial, éd. Economica, 2009, p. 1

<sup>8</sup> ROUJA S. « De quelques faux clics et vrais escrocs », in R.L.D.I, n°235, novembre 2000, p. 85

<sup>9</sup> La loi uniforme n°2008-48 de l'UEMOA du 3 septembre 2008, relative à la répression des infractions en matière de chèque, de carte bancaire et d'autres instruments et procédés électroniques de paiement

<sup>10</sup> L'acte Additionnel A/SA. 2/01/10 de la CEDEAO du 16 février 2010 relatif à la protection des données à caractère personnel.

<sup>11</sup> La Directive C/DIR/1/08/11 de la CEDEAO du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO.

<sup>12</sup> La directive n°07/08-UEAC-133-CM-18 du 19 décembre 2008 fixant le cadre juridique de la protection des droits des utilisateurs de réseaux et des services de communications électroniques au sein de la CEMAC

<sup>13</sup> Règlement n°02/03-CEMAC-CM du 04 avril 2003 relatif aux systèmes, moyens et incidents de paiement qui incrimine les atteintes aux systèmes de paiement

TIC des Etats membres de la CEEAC tenue à Ndjamena le 22 avril 2010 a chargé le Secrétaire Général de la CEEAC de préparer un texte sur la cybercriminalité qui a été élaboré.

L'avènement de ces cadres législatifs a motivé les Etats africains à pouvoir mettre en place un cadre normatif continental afin de bien réguler le cyberspace africain, il s'agit de la convention de Malabo.

Dans le cadre de cette étude, nous mettons en exergue ces cadres normatifs mise en place par les organisations internationales africaines pour la lutte contre la cybercriminalité en corrélation du droit international africain, cette corrélation se traduit par le truchement de grands principes du droit communautaire africain notamment : l'immédiateté de l'applicabilité (l'applicabilité immédiate) de ces cadres normatifs de lutte contre la cybercriminalité à savoir : (toutes les directives, circulaires voir même les protocoles ayant force de loi prises dans le cadre communautaire, la convention de Malabo), l'effet direct et la primauté de ces cadres normatifs sur le droit interne des Etats africains.

Cette introduction qui est close ouvre la voie aux points qui constituent le corps de cette étude avant la conclusion qui met fin à la réflexion. Le premier point traite de l'applicabilité immédiate des conventions de la cybercriminalité. Le second est consacré à la primauté de règles communautaires sur le droit national.

## **I. L'APPLICABILITE IMMEDIATE DES CONVENTIONS DE LA CYBERCRIMINALITE**

Au terme de ce point, nous analysons le principe de l'applicabilité immédiate des conventions sur la lutte contre la cybercriminalité au regard du droit communautaire.

### **1.1. L'applicabilité immédiate de la convention de Malabo**

A titre de rappel, le droit communautaire vise à harmoniser des droits nationaux souvent disparates et l'un des moyens d'atteindre ce but est le principe de l'applicabilité immédiate, qui est l'un des principes fondamentaux du droit communautaire.

Ce caractère de la règle communautaire est un principe essentiel du droit communautaire. Il est aussi appelé principe de la validité immédiate des règles communautaires ou de l'intégration immédiate.

Ce principe de l'application immédiate veut que la norme communautaire s'intègre automatiquement dans l'ordre juridique des Etats membres et qu'elle produit des effets juridiques dans le droit interne sans avoir y être transposée (soit sans procédure particulière).

En vertu de ce principe, les normes communautaires s'appliquent de plein droit, sans subir la moindre modification et doivent être appliquées sans restriction par le juge national.

En droit international, les Etats ont deux conceptions possibles de l'application immédiate de la règle internationale à savoir : le dualisme ou le monisme.<sup>14</sup>

Le dualisme part du principe que l'ordre juridique national et l'ordre juridique international sont indépendants et qu'il faut donc introduire la règle internationale dans l'ordre interne par le biais d'une norme nationale.<sup>15</sup>

Cependant que dans les pays appliquant la théorie moniste, l'ordre juridique international et l'ordre juridique interne ne sont pas indépendants.<sup>16</sup> Par conséquent, le droit international n'a donc pas à l'objet de mesures supplémentaires d'introduction pour être applicable immédiatement parmi les règles nationales. Or, l'application du droit communautaire dans les droits nationaux relève de la théorie moniste et non de la théorie dualiste.

En plus, l'immédiateté du droit communautaire s'applique aussi bien au droit originaire (les traités, les accords) qu'au droit dérivé (actes émis par les différentes institutions notamment : les directives, les protocoles, les circulaires et les décisions).

Notons que la quasi-totalité des Etats africains qui sont généralement dans le système moniste, peuvent par conséquent dans certains cas appliquer ce principe notamment sur le droit dérivé à l'occurrence : les Projets de lois Types de la Communauté Economique des Etats de l'Afrique Centrale (CEEAC) et Projets de Directives de la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC) mais dans le cas sous examen (sur l'applicabilité de la convention de Malabo), ce principe éprouve quelques difficultés, mieux quelques obstacles d'autant plus que la convention de Malabo, elle-

<sup>14</sup> Dionisio Anzilotti, Cours de droit international public, 1929, p. 225

<sup>15</sup> Heinrich Triepel, « Les rapports entre le droit interne et le droit international », RCADI, 1923, p. 175

<sup>16</sup> Hans Kelsen, « Les rapports de systèmes entre le droit international et le droit interne », RCADI, 1926, p. 96

même prévoit quelques modalités, mieux quelques formalités pour son intégration juridique dans le droit interne notamment par un instrument de ratification qui doit être déposé auprès du président de la Commission de l'Union Africaine, comme prévoit les articles 35 et 38 de ladite convention, qui dispose : « La présente Convention est ouverte à tous les États membres de l'Union, pour signature, ratification et adhésion, conformément à leurs procédures constitutionnelles respectives ».<sup>17</sup> « Les instruments de ratification ou d'adhésion sont déposés auprès du Président de la Commission de l'Union africaine. Tout État Partie peut dénoncer la présente Convention en notifiant, par écrit, son intention un (1) an à l'avance au Président de la Commission de l'Union africaine. Ce dernier notifie aux États membres toute signature de la présente Convention, le dépôt de tout instrument de ratification ou d'adhésion, ainsi que son entrée en vigueur. Le Président de la Commission notifie également aux États membres les demandes d'amendement ou de retrait de la Convention, ainsi que les réserves à celle-ci. Dès l'entrée en vigueur de la présente Convention, le Président de la Commission de l'Union africaine l'enregistre auprès du Secrétaire général de l'Organisation des Nations unies, conformément à l'article 102 de la Charte des Nations unies ».<sup>18</sup>

C'est à la lumière de ces dispositions de la convention de Malabo susmentionnée, qu'on déduit que l'applicabilité immédiate de droit originaire notamment la convention de Malabo sans quelques préalables pose problème, par opposition aux directives, protocoles et circulaires qui eux relèvent du droit dérivé peuvent être appliqué ou invoqué devant le juge national à une seule condition que l'Etat qui invoque soit partie prenante de l'organisation productrice de ces normes communautaires.

Ce qui reviendrait à dire que dans la pratique, et malgré quelques résistances, les Etats membres de la communauté finissent par déférer à ce caractère essentiel de la règle communautaire, aussi bien s'agissant du droit primaire ou originaire que du droit dérivé. S'il n'en était pas ainsi, l'égalité entre Etats membres devant la norme communautaire s'en trouverait rompue, de même que l'efficacité et l'effectivité de la réglementation communautaire. Pour garantir d'ailleurs ces dernières, la règle communautaire est dotée d'un autre caractère essentiel qui est son applicabilité directe.

## **1.2. L'applicabilité directe des règles communautaires en matière de lutte contre la cybercriminalité**

Une des caractéristiques essentielles des règles communautaires est qu'elles sont d'applicabilité directe. L'applicabilité directe est aussi appelée effet direct. Le principe de l'applicabilité directe ou de l'effet direct de la règle communautaire signifie qu'elle a l'aptitude générale à être source de droits subjectifs et d'obligations individuelles attribuables et invocables par les personnes, tant dans les rapports de particuliers à particuliers, que dans les relations juridiques des individus avec les institutions de l'Etat. Plus précisément, l'effet direct ou l'applicabilité directe implique le droit pour toute personne de réclamer à tout organe de l'Etat l'application à son égard des règles communautaires telles qu'adoptées dans l'ordre communautaire et tous les organes de l'Etat, notamment les juridictions, ont l'obligation de faire appliquer ces règles directement dans les rapports juridiques présentés devant eux.<sup>19</sup>

L'effet direct a donc une triple composante : primo, la capacité de la règle à créer directement des droits et des obligations pour les particuliers ; secundo, la possibilité pour ceux-ci d'invoquer ces garanties communautaires devant le juge national ; et tertio, l'obligation pour le juge de statuer sur les causes dans lesquelles les garanties communautaires sont invoquées par les personnes.

Dans la pratique, cette corrélation triangulaire de l'effet direct se résume essentiellement dans l'invocabilité juridictionnelle du droit communautaire par toute personne juridique dans tout ordre juridique interne des Etats membres. Par analogie, les règles communautaires sont aussi invocables devant toutes les autorités de l'Etat, notamment l'administration publique.<sup>20</sup>

Ainsi d'ailleurs que devant les organes de la communauté elle-même. Ce caractère self-executing est présumé, et en cas de doute devant une juridiction nationale, la juridiction communautaire détermine en dernier ressort si une règle communautaire est dotée de l'effet direct, par le jeu des questions préjudicielles.<sup>21</sup>

<sup>17</sup> Art. 35 de la Convention de l'UA sur la cybersécurité du 27 juin 2014

<sup>18</sup> Art. 37 Idem

<sup>19</sup> Robert Lecourt, l'Europe de juges, Bruylant, Bruxelles, 1976, p.248

<sup>20</sup> Idem

<sup>21</sup> Abdoulaye SOMA. « Les caractères généraux du droit communautaire », in Revue CAMES/SJP, n°001/ 2017, p. 1-10

Cette immédiateté de la règle communautaire la rend inconditionnelle, complète et apte en elle-même à produire des effets sans exiger une intervention préalable d'aucun organe de l'Etat pour compléter ou préciser son dispositif en vue d'en faire une source de légalité. L'effet direct des règles communautaires, qui peut être à la fois vertical, oblique, collatéral ou horizontal, n'est pas absolu, notamment par rapport aux directives. Par contre, l'effet direct est une caractéristique fondamentale de la règle communautaire dans son principe.<sup>22</sup>

Globalement, ce principe ne peut être invoqué directement dans le cas échéant devant le juge national en ce qui concerne la convention de Malabo, pour la simple raison que la convention de Malabo a prévu dorénavant quelques modalités pour sa mise en œuvre, néanmoins sur le plan du droit dérivé, il est plausible que le principe soit invoqué d'autant plus que toutes les directives, les protocoles et les circulaires de la CEEAC relatives à la cybercriminalité prévaut sur le droit interne des Etats qui sont dans le système moniste et ont possibilité d'être invoqué par les Etats membres de cette institution voir même les ressortissants de ces Etats membres.

Ainsi donc, nous pouvons déduire à cet effet que l'applicabilité directe des règles communautaires en matière de lutte contre la cybercriminalité n'est pas plausible au regard du droit primaire ou originaire tenant compte de la nature non dérogeable de ce droit, en revanche l'applicabilité directe est de facto prise en compte dans le droit dérivé notamment les directives, les protocoles, les décisions ayant traités à la cybercriminalité que produisent les organisations communautaires dans lesquelles tous les Etats sont membres.

Caractérisée à la fois par la validité immédiate et l'applicabilité directe dans son internalisation, la règle communautaire présente d'autres caractères généraux liés à son rang dans l'ordre juridique, allusion faite ici à la primauté du droit communautaire sur le droit national.

## II. LA PRIMAUTE DE REGLES COMMUNAUTAIRES SUR LE DROIT NATIONAL

Dans ce point, il sera nécessaire d'analyser de manière succincte le principe de la primauté des règles communautaires sur les lois internes de lutte contre la cybercriminalité. Nous mettrons en exergue ici la supériorité des règles communautaires vis-à-vis de ces lois internes, avant de procéder à cette dissection, il est important de rappeler les méandres de ce principe de primauté des règles communautaires.

Immédiatement valables et directement applicables dans les ordres juridiques internes respectifs des Etats membres, les règles communautaires rencontrent et confrontent forcément les règles nationales. On sait que suivant la théorie de la pyramide des normes de Kelsen<sup>23</sup>, les actes de droit interne sont rangés suivant une hiérarchie qui détermine non seulement leur validité, mais surtout leur ordre de primauté en cas de conflit dans l'application.

On en infère logiquement l'intérêt de savoir le rang des normes communautaires en matière de lutte contre la cybercriminalité dans la hiérarchie des normes internes pour établir leur régime juridique dans le système de chaque Etat membre.

Sur le sujet, un caractère général cardinal des règles communautaires est qu'elles ont primauté sur les règles de droit interne. Le principe fondamental de la primauté générale du droit communautaire sur le droit interne est largement et classiquement affirmé, aussi bien normativement que jurisprudentiellement.<sup>24</sup> Ce caractère induit le principe que les règles communautaires valablement adoptées sont appliquées dans chaque Etat membres nonobstant toute législation nationale contraire antérieure ou postérieure. Plus précisément, le droit communautaire prime sur le droit interne de tout Etat membre, y compris les normes suprêmes à valeur constitutionnelle.<sup>25</sup> Cette primauté a au moins une double fonction. Elle permet d'abord d'organiser une coexistence entre les règles de droit communautaire et les règles de droit interne. Elle permet ensuite de donner plein effet au droit communautaire qu'en droit interne. Tout serait perdu en termes de fonctionnalité et d'effectivité du droit communautaire si le

---

<sup>22</sup> Idem

<sup>23</sup> Hans Kelsen, *Théorie pure du droit*, éd. Dalloz, Paris, 1977, p. 299

<sup>24</sup> Article 6 du traité révisé de l'UEMOA du 29 janvier 2003, et article 10 du traité OHADA de Port-Louis du 17 octobre 1993

<sup>25</sup> CJUEMOA, avis du 18 mars 2003

principe de la primauté de celui-ci sur le droit interne ne venait pas renforcer et couronner sa validité immédiate et son applicabilité directe.

Ce caractère ou ce principe qui est à la fois général et absolu est institutionnellement garanti, notamment par la juridiction nationale et en dernier ressort par la juridiction communautaire elle-même, par le mécanisme du renvoi préjudiciel. A défaut d'une mise en œuvre interne de ce principe, l'Etat concerné engage sa responsabilité internationale.<sup>26</sup>

Avec les différentes perceptions de la souveraineté dans les Etats membres, il n'est pas rare que ce principe de primauté souffre parfois de quelques réticences des Etats dans des situations critiques.

Cependant, certaines Constitutions africaines de l'espace francophone aménagent une place de choix à l'intégration africaine en prévoyant la possibilité de conclure des accords comportant l'abandon partiel, voire total de souveraineté pour réaliser cette fin.<sup>27</sup>

Enfin, au regard du principe de primauté du droit communautaire, les lois communautaires sont supérieures aux lois internes.

Ainsi, l'invocation des directives, protocoles et les décisions qui émanent du droit dérivé en matière de lutte contre la cybercriminalité poserait aucun problème au regard de tous ces principes du droit communautaire évoqués, on se contentera de brandir une disposition des directives, protocoles ou décisions sans une quelconque anomalie juridique dans un différend opposant un sujet de droit présentant un élément d'extranéité, en revanche l'invocation des conventions de Malabo éprouverait quelques malaises juridiques si celle-ci n'est pas préalablement ratifiées, ce qui apparaît rédhibitoire l'invocation de la convention de Malabo devant un juge en cas de différend sans que celle-ci soit ratifiée préalablement par l'une des parties au différend.

## CONCLUSION

Il est indéniable que les Etats africains se sont lancés depuis la nuit de temps dans la réglementation du cyberspace africain. Les Etats africains n'ont cessé de produire à travers les organisations africaines plusieurs normes en matière de lutte contre la cybercriminalité sur le continent notamment : les directives, les protocoles, les circulaires et les décisions. Hormis la présence de toutes ces normes, les Etats africains doivent mettre en place une cyberstratégie communautaire africaine de lutte contre la cybercriminalité qui devra favoriser la gestion d'un véritable cyberdroit pénal, régulateur d'une société africaine à dimension humaine inclusive ouverte, aussi bien dans ces aspects substantiels que processuels.

Ce cyberdroit pénal devrait prendre en charge dans ses prévisions l'immatérialité des cybercriminels ainsi que l'anonymat des délinquants. Cependant, la cybercriminalité étant une criminalité internationale qui ignore les balises physiques des frontières étatiques, Il est donc nécessaire d'envisager en Afrique généralement un renforcement de la coopération international en matière de lutte contre la cybercriminalité. A cet égard la Convention Africaine sur la cybersécurité constitue une avancée majeure dans la lutte régionale contre le phénomène. Mais, force est de constater que la convention de l'UA n'est pas un instrument international de lutte contre le cybercrime. En l'état actuel, une brèche de solution est ouverte, les Etats africains pourraient explorer la voie de l'adhésion à la convention de Budapest du 23 novembre 2001 sur la cybercriminalité qui apparaît à ce jour comme un instrument juridique efficace sur le plan mondial devant lutter contre la cybercriminalité. En effet, cette convention est ouverte à l'adhésion même des Etats non membres du conseil de l'Europe. Par ailleurs, de nos jours, on s'accorde pour admettre qu'un traitement efficace de la cybercriminalité suppose le recours à l'approche de « cybersécurité ». Cette nouvelle démarche procède d'une approche globale et holistique de la stratégie de lutte contre la cybercriminalité intégrant toutes ses dimensions. Il s'agit au-delà de la modernisation des normes juridiques, de prendre conscience de la nécessité du renforcement des capacités et de spécialisation des autorités judiciaires en charge de la cyberdélinquance (vers une cyberpolice et vers une cybermagistrature). De l'amélioration des moyens matériels et logistiques à la disposition des organes répressifs et de la promotion de la culture de la cybercriminalité en Afrique. Cette approche globale de la répression des agissements déviants du cyberspace contribuera à inscrire les pays africains dans la

<sup>26</sup> CJCE, 19 novembre 1991, affaire Francovich et Bonifaci

<sup>27</sup> J.KAZADI MPIANA: « La problématique de l'existence du droit communautaire africain. L'option entre mimétisme et spécificité », Revue libre de Droit, 2014, p. 55

croisade internationale contre la cybercriminalité, qui constitue une sérieuse menace pour la sécurité du cyberspace africain.

#### BIBLIOGRAPHIE

- Abdoulaye SOMA. « Les caractères généraux du droit communautaire », in *Revue CAMES/SJP*, n°001/ 2017
- Acte Additionnel A/SA. 2/01/10 de la CEDEAO du 16 février 2010 relatif à la protection des données à caractère personnel
- ANZILOTTI, D., Cours de droit international public, 1929
- BOYER J., « La révolution d'internet », P.A, 10 novembre 1999, n° 224
- CAPELLER, W., « Un net pas très net » in *L'immatériel et le droit*, n°143
- CJCE, 19 novembre 1991, affaire Francovich et Bonifaci
- CJUEMOA, avis du 18 mars 2003
- Convention de l'UA sur la cybersécurité du 27 juin 2014
- Directive C/DIR/1/08/11 de la CEDEAO du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO
- Directive n°07/08-UEAC-133-CM-18 du 19 décembre 2008 fixant le cadre juridique de la protection des droits des utilisateurs de réseaux et des services de communications électroniques au sein de la CEMAC
- DUFOUR A., *Internet : Que sais-je ?*, Paris, Le Temps des médias, 2000
- GHERNOUTI-HELIE S., *La cybercriminalité : le visible et l'invisible*, Lausanne, éd. Presses Polytechniques et Universitaires Romandes (PPUR), 2009
- HEINRICH TRIEPEL, « Les rapports entre le droit interne et le droit international », in *RCADI*, 1923
- J.KAZADI MPIANA: « La problématique de l'existence du droit communautaire africain. L'option entre mimétisme et spécificité », in *Revue libre de Droit*, 2014
- KELSEN, H., « Les rapports de systèmes entre le droit international et le droit interne », in *RCADI*, 1926
- KELSEN, H., *Théorie pure du droit*, Paris, éd. Dalloz, 1977
- LECOURT, R., *L'Europe de juges*, Bruxelles, Bruylant, 1976
- Loi uniforme n°2008-48 de l'UEMOA du 3 septembre 2008, relative à la répression des infractions en matière de cheque, de carte bancaire et d'autres instruments et procédés électroniques de paiement
- MYRIAM, Q., « Concilier la lutte contre la cybercriminalité et l'éthique », in *Sécurité et stratégie*, 2011
- QUEMENER, M. et FERRY, J., *Cybercriminalité : défis mondial*, Paris, éd. Economica, 2009
- QUEMENER, M., *Cyber menaces, entreprises et internautes*, Paris, éd. Economica, 2008
- Règlement n°02/03-CEMAC-CM du 04 avril 2003 relatif aux systèmes, moyens et incidents de paiement qui incrimine les atteintes aux systèmes de paiement
- ROUJA, S. « De quelques faux clics et vrais escrocs », in *R.L.D.I*, n°235, novembre 2000
- Traité OHADA de Port-Louis du 17 octobre 1993
- Traité révisé de l'UEMOA du 29 janvier 2003, et article 10 du traité OHADA de Port-Louis du 17 octobre 1993