

## Habermasian Democracy in the Age of ICTs: A Cyber-Optimist and Cyber-Realist Reading in the ECOWAS Community Space

Affian Job Kouadio<sup>1</sup>, Gnyambi Franck Tchouda<sup>2</sup>

---

Science Step Journal / SSJ

2026/Volume 4 - Issue 14

**To cite this article:** Kouadio, A. J., & Tchouda, G. F. (2026). Habermasian Democracy in the Age of ICTs: A Cyber-Optimist and Cyber-Realist Reading in the ECOWAS Community Space. Science Step Journal, 4(14). ISSN: 3009-500X.  
<https://doi.org/10.5281/zenodo.22118745>

---

### Abstract

The current digital revolution is leading to new ethical questions that everyone is invited to address. Today, the internet offers us almost unconditional access to information as well as opportunities for virtual debates on various societal issues. In a rapidly technological society, no one can ignore the effects of communication and information sciences on intersubjective relations. Today, within ECOWAS, the man of advanced modernity is faced with a dilemma: on the one hand, the cyber-optimists who are in favour of the opportunity offered by ICTs to express themselves and exercise unlimited freedom of communication with the rest of the world, and on the other hand, the cyber-realists, who, for their part, consider ICTs as tools for alienating democracy. In this article, it is a question of showing, through the politics of deliberative democracy, through the theory of discussion which is embodied in the concept of an ideal procedure of deliberation and decision-making through pragmatic reflection, compromise, discussion, collective agreement, that relating to justice, argumentation and communication offered by the internet and social networks to men is sometimes presented as an alienated and pathological freedom of communication. This is why we would like to propose an approach to analytic philosophy through Habermasian deliberative politics in order to understand the relationship between democratic society and ICTs (first part), in order to better understand the challenges of cybercrime within ECOWAS (second part), and finally the security measures put in place by them. This article aims to show that the unlimited freedom of communication offered by the internet and social media may, from the perspective of Habermas's theory of discourse, turn out to be an 'alienated and pathological' freedom rather than pure democratic progress.

**Keywords:** Habermas's Democracy, ECOWAS, Public space, ICT, cyberdemocracy, cyber-optimists, cyber-realists, cybercrime.

---

<sup>1</sup> Doctoral Student in Political and Social Philosophy, Faculty of Communication, Environment and Society (UFR), Alassane Ouattara University, Côte d'Ivoire; Email: [affianjob09@gmail.com](mailto:affianjob09@gmail.com)

<sup>2</sup> Assistant Lecturer, Péléfro Gon Coulibaly University, Côte d'Ivoire. Email: [tgfranck02@gmail.com](mailto:tgfranck02@gmail.com)

## **Démocratie habermassienne à l'épreuve des NTIC : Une lecture cyber-optimiste et cyber-réaliste dans l'espace communautaire de la cedeao**

Affian Job Kouadio, Gnyambi Franck Tchouda

### **Resumé**

La révolution numérique en cours conduit à des questionnements éthiques inédits dont chacun est invité à se saisir. Internet nous offre aujourd'hui un accès quasi-inconditionnel à l'information ainsi que des possibilités de débats virtuels sur diverses thématiques sociétales. Dans une société en plein essor technologique, nul ne peut ignorer les effets des sciences de la communication et de l'information dans les rapports d'intersubjectivité. Aujourd'hui, au sein de la CEDEAO, l'homme de la modernité avancée se trouve devant un dilemme : d'une part, les cyber-optimistes qui sont pour l'opportunité qu'offrent les NTIC afin de s'exprimer et d'exercer une liberté de communication illimitée avec le reste du monde et d'autre part, les cyber-réalistes, qui, quant à eux, considèrent les NTIC comme des outils d'aliénation de la démocratie. Dans ce texte, il est question de montrer, à travers la politique de la démocratie délibérative par la théorie de la discussion qui s'incarne dans le concept d'une procédure idéale de délibération et de décision grâce à la réflexion pragmatique, le compromis, la discussion, l'entente collective, celle relative à la justice, l'argumentation et la communication de Jürgen Habermas, que la liberté de communication illimitée qu'offrent Internet et les réseaux sociaux aux hommes, se présente parfois comme une liberté de communication aliénée et pathologique. C'est pourquoi nous voudrions, ici, proposer comme approche la philosophie analytique à travers la politique délibérative habermassienne afin de comprendre le rapport de la société démocratique et des NTIC (première partie) pour mieux cerner les défis de la cybercriminalité au sein de la CEDEAO (seconde partie) et enfin les moyens sécuritaires mis en place par celle-ci pour une bonne gouvernance (troisième partie). L'article se propose de montrer que la liberté de communication illimitée offerte par Internet et les réseaux sociaux peut, sous l'angle de la théorie de la discussion de Habermas, se révéler être une liberté « aliénée et pathologique » plutôt qu'un progrès démocratique pur.

### **Mots clés**

Démocratie habermassienne, CEDEAO, Espace public, NTIC, cyberdémocratie, cyber-optimistes, cyber-réalistes, cybercriminalité.

## Introduction

Le XXI<sup>e</sup> siècle est marqué par la consécration des nouvelles technologies de l'information et de la communication (NTIC). Cette révolution contemporaine est notamment liée à la structure même d'Internet et de l'espace virtuel qu'il génère, *le cyberspace*<sup>3</sup>. Ce dernier est communément défini comme un ensemble de données numérisées constituant un univers d'information et de communication, lié à l'interconnexion mondiale des ordinateurs, plus précisément défini comme « un ensemble de réseaux commerciaux, réseaux publics, réseaux privés, réseaux d'enseignement, réseaux de services, qui opèrent à l'échelle planétaire » (LEBERT M-F., 1999). Les technologies de l'information et de la communication (TIC) sont aujourd'hui omniprésentes et la tendance à la numérisation va grandissante. L'ère numérique ignore désormais toutes les frontières. Elle permet l'accès à la culture et à la connaissance et favorise les échanges entre les personnes. Elle rend possible la constitution d'une économie en ligne et rapproche le citoyen de son administration. Les technologies numériques sont porteuses d'innovation et de croissance, en même temps qu'elles peuvent aider ou accélérer le développement des pays émergents comme ceux de la CEDEAO.

Cependant, un certain pessimisme vient tempérer cette approche idéaliste. Tous les progrès génèrent aussi de nouvelles fragilités et vulnérabilités propices aux menaces ou aux risques, car ils aiguisent l'imagination des criminels, des cybercriminels. La cybercriminalité est désormais une réalité. Elle est d'autant plus dangereuse qu'elle pénètre au sein des familles, là où la délinquance ordinaire n'avait pas accès jusqu'à présent. De ce qui précède, ressort la question essentielle de ce texte : L'internet peut-il être un complément de la démocratie en Afrique subsaharienne ? En d'autres termes, Internet est-il, de façon plus radicale, un vecteur de transformation de la démocratie ? Les NTIC, en facilitant la participation citoyenne à la vie politique, peuvent-elles contribuer à l'amélioration et au renforcement de la démocratie face aux défis de la cybercriminalité au sein de la CEDEAO ? C'est à travers une approche de la philosophie analytique appliquée à la politique délibérative habermassienne que nous allons mener notre réflexion.

### 1. Démocratie habermassienne et NTIC

Quel est le sens de la démocratie chez Habermas ? Quels liens établit-il entre la démocratie, l'État de droit et les NTIC ?

Il convient, pour mieux cerner la perspective habermassienne de la démocratie, de prendre le terme « *démocratie* » dans son sens juridico-institutionnel et non dans son sens éthique, c'est-à-dire dans un sens plus procédural que substantiel. C'est en ce sens que Norberto Bobbio parle de démocratie formelle et de démocratie substantielle (Norberto BOBBIO, 1997, p. 45). En effet, Norberto Bobbio arrive à la dissociation de la démocratie formelle de la démocratie substantielle en faisant ressortir du terme « démocratie » deux sens prédominants suivant lesquels la

---

<sup>3</sup> - Dérivé de l'anglais « Cyberspace », contraction des mots « Cybernétique » et « Espace », ce terme a été introduit pour la première fois par l'auteur américain William Gibson dans son roman de science-fiction « Neuromancer », 1984.

démocratie est soit l'ensemble des règles dont le respect est nécessaire afin que le pouvoir fasse effectivement l'objet d'une distribution touchant la majorité des citoyens, soit l'idéal auquel un gouvernement démocratique devrait aspirer, à savoir celui de l'égalité.

L'idée dominante chez Jürgen Habermas, c'est bien entendu les impasses de la modernité dans nos sociétés modernes d'aujourd'hui, avec le constat que la raison a cessé d'avoir son siège dans l'histoire. Alors que nous attendions de l'état de droit une protection contre tous ces maux, il se trouve en être le contraire avec des États écartelés entre les règles (normes) et la factualité (les faits) qui ne répondent pratiquement plus qu'aux impératifs du nouveau pouvoir économique et de la domination politique. Pour Habermas, la démocratie ou du moins la *démocratie délibérative* ne peut se passer de la raison procédurale, de même qu'une autocritique de la raison qu'est l'activité communicationnelle qu'il pose comme condition et origine dans notre société, qui permet en outre la compréhension intersubjective grâce à laquelle sont définis les normes sociales, les valeurs et les rôles nécessaires à toute communauté, c'est dans ce contexte que les questions du droit et de la démocratie prennent toutes leurs mesures. La démocratie délibérative est caractérisée comme un paradigme de la théorie démocratique qui défend la thèse selon laquelle la délibération publique et libre entre citoyens égaux est le fondement de la légitimité politique.

La démocratie délibérative habermassienne se base sur la souveraineté populaire. La seule façon de rendre cette souveraineté possible est l'attribution à la majorité des citoyens du droit de participer directement et indirectement à la prise des décisions collectives dans la société contemporaine marquée par la puissance et l'omniprésence des technologies. Ainsi, pour Habermas (1968, p. 88) :

On entendra par *démocratie* les formes institutionnelles garanties d'une communication universelle et publique qui est consacrée à la question pratique de savoir comment les hommes peuvent et veulent vivre ensemble dans le cadre des conditions objectives déterminées par le pouvoir immensément accru dont ils disposent sur les choses.

Habermas (1987, p. 75) considère la sphère publique comme un principe structurant l'ordre politique. Elle est de ce fait « structurée par la représentation » qui était le modèle du Moyen Âge.

Le concept de *démocratie* implique l'égalité devant la loi et l'égalité des droits. Ce principe d'égalité fait partie intégrante des moyens constitutifs et d'application de l'État de droit et lui est inhérent. De même, Habermas se réfère au « principe démocratique » pour une compréhension de la démocratie. En effet, ce principe confère une force légitime au processus d'instauration de l'État de droit.

Selon Habermas, il faut une nouvelle façon de comprendre la démocratie qui tienne compte de la complexité des sociétés présentes, par exemple du rôle des médias. Les médias sont certes un pouvoir qu'il faut contrôler, mais permettent aussi la communication simultanée d'une multitude

de personnes qui ne se connaissent pas. L'espace politique doit pouvoir intégrer les voix marginales, être réceptif au monde vécu privé. Pour cela, il ne s'agit pas de s'orienter vers l'intérêt général en citoyen vertueux ni de s'aligner sur le modèle du marché. Les États doivent parvenir à un accord sur la façon dont ils veulent comprendre ce qu'ils ont déclaré en commun être « les droits de l'homme ». Ainsi, l'espace public permet une revitalisation de l'État de droit par la délibération constante et publique des individus à travers les médias et les NTIC.

En quelques années seulement, les technologies de communication en sont venues à irriguer la quasi-totalité de la surface de nos vies. Les NTIC sont d'une importance capitale dans la consolidation de la démocratie habermassienne du point de vue de la discussion au sein de l'espace public et du renforcement de la liberté du « *Quatrième pouvoir* » (Jürgen Habermas, 1978, p. 45). L'objectif de la démocratie électronique est d'utiliser les nouvelles technologies de l'information et de la communication (NTIC) pour améliorer la démocratie et les institutions démocratiques. De ce fait, la démocratie électronique permet au citoyen de participer à cette démocratie avec les dirigeants. Cependant, comment la pratique citoyenne de l'espace public, par des discussions « au caractère imprécis » (Catherine Audard, 2002, p. 115), peut-elle influencer le pouvoir politique officiel ?

En tant que communication sans contraintes, « le pouvoir communicationnel signale et problématise de nouveaux thèmes publics » (HABERMAS Jürgen, 1997, p. 386), contribue à former la volonté politique et est donc une source de légitimation du pouvoir étatique. Il lui revient d'influencer le pouvoir administratif, sans être canalisé par celui-ci, car seule l'ouverture illimitée des thèmes débattus (selon les principes de neutralité et de publicité) accorde une force démocratique innovante à l'opinion publique. Dans les sociétés actuelles, la communication ne peut plus s'effectuer que par le biais des médias de masse. Les partis politiques doivent en particulier se tourner vers les médias et les NTIC pour apporter leurs projets et leurs positions à la population. Les démocraties ne se caractérisent plus principalement par la communication directe, mais plutôt par la communication médiatique. C'est justement pour cette raison que les médias sont considérés comme étant le « *quatrième pouvoir* » après les pouvoirs judiciaire, législatif et exécutif ; car ils constituent l'instrument de contrôle le plus important de l'opinion publique.

La liberté d'expression et de communication est d'autant plus précieuse que son exercice est une condition de la démocratie et l'une des garanties du respect des autres droits et libertés. Elle est *la garantie même des garanties*. Dans une société démocratique, le rôle des médias est incontournable. Historiquement, les médias ont été identifiés comme étant des diffuseurs d'informations indispensables aux citoyens pour les aider à comprendre ce qui se passe dans leur société et à prendre des décisions éclairées. Les médias, en tant qu'outil démocratique, auraient le mandat d'offrir des comptes rendus véridiques et complets au sujet des événements qui touchent les citoyens. Ils ont la responsabilité de contextualiser ces événements afin de leur donner leur

sens véritable. Les médias et les NTIC doivent aussi servir de lieu d'échange de commentaires et de critiques qui permettent le renforcement de la démocratie.

Les NTIC offrent la possibilité à un seul individu de s'adresser à beaucoup d'autres (one-to-many) via les sites web que, du moins en principe (ce n'est pas le cas en pratique), chacun peut créer, ce que font les gouvernements, les hommes d'affaires, les acteurs financiers, les groupes d'intérêt, les activistes politiques et civiques, les amateurs et clubs de fans. Internet contribue donc à l'expression des citoyens ordinaires qui contournent ainsi les corps intermédiaires, la parole profane prenant place aux côtés de celle des experts consacrés (politiques, journalistes, spécialistes), ce phénomène s'inscrivant dans le prolongement du format des talk-shows. Il existe sur Internet une pluralité d'espaces publics qui agissent sur l'organisation démocratique de nos sociétés et qui participent à la montée de la démocratie d'opinion à travers ce que Jürgen Habermas a appelé *la théorie de la discussion* qui s'incarne dans le concept d'une procédure idéale de délibération et de décision grâce à la réflexion pragmatique, le compromis, la discussion, l'entente collective, celle relative à la justice, l'argumentation et la communication. C'est justement ce que Jürgen Habermas (1997, p. 326) fait remarquer dans ce qui suit :

Le cœur de la philosophie délibérative réside en effet dans un réseau de discussions et de négociations dont le but est d'apporter une solution rationnelle aux questions pragmatiques, morales et éthiques : plus précisément, aux problèmes accumulés d'une intégration à la fois fonctionnelle, morale et éthique de la société, qui a échoué à d'autres niveaux.

Cette méthodologie est utile en ce sens qu'elle nous permet de montrer, selon Kouadio K. Décaïrd (2015, pp. 388-389), que « la politique délibérative que présente Habermas est un moyen de radicaliser le processus démocratique actuel qui semble être dans une impasse ».

## **2. La CEDEAO face à la cybercriminalité**

L'amélioration de la gouvernance au sein de la CEDEAO reste au cœur de la paix, de la sécurité et de la transformation économique et numérique de son espace. Elle se reflète dans la forte interface entre la meilleure gouvernance et le progrès économique de ses États membres et dans l'exigence citoyenne croissante de démocratie, de responsabilisation, de libertés civiles et d'état de droit. Cet état de droit confère aux citoyens la liberté d'expression, d'accès quasi inconditionnel à l'information et d'échanges entre les personnes. Cette forme de liberté occasionne parfois des comportements et attitudes maladroits, répréhensibles par la loi.

En droit, tout comportement humain ou toute action humaine qui cause du tort à autrui est répréhensible. Les actes humains pouvant tomber sous le coup de la répression sont assez variés. On distingue aujourd'hui la criminalité ordinaire d'une criminalité spécifique qu'on désigne sous le vocable de la *cybercriminalité*. Celle-ci s'entend d'un ensemble d'actes humains liés à l'usage des Nouvelles Technologies de l'Information et de la Communication (NTIC).

Les définitions de la cybercriminalité dépendent surtout des fins recherchées en utilisant ce terme. Un nombre limité d'actes contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques représente l'essentiel de la cybercriminalité. Toutefois, les actes liés à l'informatique commis pour un profit personnel ou financier, ou pour porter préjudice, y compris des formes de crimes liés à l'identité et les actes liés au contenu informatique (*tous ceux qui sont inclus dans le sens le plus large du terme cybercriminalité*) ne facilitent pas l'établissement des définitions légales du terme global. Certaines définitions sont requises pour les principaux actes de cybercriminalité.

La cybercriminalité a longtemps été considérée comme un tabou qui ne pouvait toucher que les grandes entreprises et les États. Il en va autrement de la réalité du terrain car tous autant que nous sommes, nous nous trouvons aujourd'hui confrontés à ce phénomène qui a trouvé son berceau aux États-Unis dans la Silicon Valley. Pour faire face à un éventail croissant de cybermenaces et de défis, les gouvernements africains en général et ceux de la CEDEAO en particulier ont adopté des stratégies de cybersécurité qui favorisent la collaboration et la confiance entre les acteurs civils et les secteurs de la sécurité publique et privée. La CEDEAO est confrontée à une multitude croissante de cybermenaces provenant de l'espionnage, du sabotage des infrastructures critiques, de l'innovation de combat et de la criminalité organisée. En effet, l'absence d'une agence fonctionnelle chargée de faire quelque chose d'aussi fondamental que de veiller à ce que les adresses IP des différents pays membres de la CEDEAO soient gérées par ses pays membres constitue une menace directe pour l'accès à Internet au sein de la communauté. Malheureusement, la quasi-totalité des pays de la CEDEAO n'a pas encore élaboré de politique nationale en matière de cybersécurité. Les quelques-uns qui se sont dotés de stratégies de cybersécurité n'arrivent pas à s'adapter à l'évolution des différents domaines de menace de la cybercriminalité.

Les actes de cybercriminalité sont peut-être uniques parmi les délits en général, car il existe des mesures de prévention répandues basées sur la technologie, y compris des antivirus, des produits de sécurité des réseaux et des pare-feu<sup>4</sup>. Le rôle de ces produits est généralement basé sur l'analyse, l'identification et le filtrage de certaines signatures électroniques. Ceci peut être basé sur le contenu ou sur le trafic, comme les communications allant ou venant d'adresses IP sur les listes noires<sup>5</sup>. Plusieurs produits incluent aussi une détection heuristique qui examine le comportement de connexions et de fichiers suspects dans des conditions prédéterminées. La tentative de commettre des actes d'accès illégal à un système informatique, ou d'interférence illégale avec des données ou des systèmes informatiques, peut être détectée par ces produits qui génèrent une riposte.

---

<sup>4</sup> - Voir OCDE. 2002. *Recommandations du Conseil concernant les lignes directrices pour la sécurité des réseaux et des systèmes d'information vers une culture de la sécurité* 25 juillet 2002 – C (2002)131/FINAL

<sup>5</sup> - Callanan, C., Gercke, M., De Marco, E., et Dries-Ziekenheiner, H. 2009. *Etude sur le blocage d'internet, équilibrer les ripostes à la cybercriminalité dans les sociétés démocratiques*. Aconite internet Solutions, octobre 2009.

Aussi, les pays membres de la CEDEAO doivent créer des centres intégrés sous-régionaux de signalement spécialisés en matière de cybercriminalité, comme un site web ou une ligne d'assistance pour les victimes d'un cyberdélit, même si des sites de signalement volontaire pour les victimes sont également de plus en plus nombreux dans les pays en développement, comme en Afrique de l'Ouest<sup>6</sup>.

Par conséquent, il faut faire des enquêtes sur la victimisation liée aux délits, qui sont généralement considérées comme l'un des moyens les plus efficaces de collecter des statistiques sur les délits. Les enquêtes sur la victimisation des délits sont généralement considérées comme l'un des moyens les plus efficaces de collecter des statistiques sur les délits. Elles éliminent, en principe, l'incertitude créée par le '*chiffre noir*' des délits qui ne sont pas signalés à la police, en recueillant les informations directement auprès de la population des victimes potentielles<sup>7</sup>.

Ces enquêtes sur la victimisation par des délits doivent prendre en compte, entre autres, « des expériences négatives lors de l'utilisation d'internet », « des incidents liés à des logiciels malveillants » ou « des menaces d'agressions liées à l'informatique » ou « des fraudes sur Internet »<sup>8</sup>. Les enquêtes régionales doivent aussi inclure des questions sur la « réception de courriels frauduleux demandant de l'argent », « des fraudes en ligne où les biens achetés ne sont pas livrés, sont contrefaits ou sont distincts de ceux annoncés », « le piratage de compte de messagerie ou de profils de réseaux sociaux » ; « les fraudes de cartes de crédit en ligne, »<sup>9</sup> ; « les vols de données commis sur internet »<sup>10</sup>. D'autres enquêtes internes à chaque pays membre de la CEDEAO doivent prendre couvrir les délits connexes qui peuvent ou non impliquer des données ou des systèmes informatiques, comme le « vol d'identité »<sup>11</sup> ; « clonage de cartes bancaires »<sup>12</sup> et « la prédation sexuelle des enfants liées à l'informatique » qui se réfère à des actes qui impliquent l'utilisation d'un système informatique pour proposer une rencontre à un enfant qui n'a pas atteint la majorité sexuelle, à des fins sexuelles.

Les institutions académiques et les organisations intergouvernementales sont également des intervenants importants dans la prévention et la lutte contre la cybercriminalité. Ces institutions peuvent notamment apporter une contribution par le partage et le développement des connaissances ; le développement de politiques et de lois ; le développement de normes techniques

---

<sup>6</sup> - Voir <http://www.cybercrime.interieur.gouv.ci/?q=node/4>

<sup>7</sup> - Pour une révision générale de la méthodologie des enquêtes sur la victimisation des délits, voir ONUDC/CEE 2010. Manuel sur les enquêtes de victimisation.

<sup>8</sup> - Hong Kong EIVC. 2010. Rapport final du EIVC de 2006 de Hong Kong.

<sup>9</sup> - Symantec. 2012. Rapport Norton sur la cybercriminalité 2012.

<sup>10</sup> - McAfee/ Alliance nationale de cybersécurité. 2012. Enquête sur la cybersécurité en ligne.

<sup>11</sup> - Département de Justice des États Unis, Bureau des statistiques judiciaires. 2008. Supplément sur le vol d'identité de l'enquête nationale sur la victimisation des délits 2008.

<sup>12</sup> - INEGI. 2012. Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública 2012 (ENVIPE), Cuestionario Principal.

et de technologie ; la fourniture d'assistance technique et la coopération avec les services répressifs.

Le partage et le développement des connaissances liées à la cybersécurité et à la cybercriminalité permettent de promouvoir « l'éducation et la formation de jeunes adultes et de futurs professionnels relatives à la sécurité informatique et aux questions techniques »<sup>13</sup>. La prévention de la criminalité fait référence aux mesures et aux stratégies qui visent à réduire le risque de commettre des délits et leurs effets potentiels nocifs sur les individus et la société, par le biais d'interventions qui influent sur les multiples causes de criminalité<sup>14</sup>. Les principes directeurs applicables à la prévention du crime des Nations Unies soulignent le fait que le leadership du gouvernement joue un rôle important dans la prévention de la criminalité, ainsi que la coopération et le partenariat entre les ministères et les autorités, les organisations communautaires, les organisations non-gouvernementales, le milieu des affaires et les citoyens<sup>15</sup>. Une bonne pratique en matière de prévention de la criminalité commence par des principes basiques comme le leadership, la coopération et l'état de droit, suggère des formes d'organisation comme des plans de prévention de la criminalité, et met en œuvre des méthodes comme le développement d'une base de connaissances solide et des approches qui incluent la réduction des opportunités criminelles et le durcissement des cibles.

### **3. Mécanismes de la gouvernance sécuritaire au sein de la CEDEAO**

La CEDEAO présente la particularité de compter quelques-uns des États du continent africain avec une multitude de problèmes de sécurité : conflits violents récurrents, régimes autoritaires qui perdurent. C'est pourquoi les États d'Afrique de l'Ouest ont été sélectionnés pour faire partie d'un nouveau programme de développement lancé à la fin des années 90 et qui, pour la première fois, prenait en compte la question de la sécurité. L'expression « Réforme du Secteur de la Sécurité »<sup>16</sup> (RSS) est apparue et a été inscrite au programme d'un projet international visant à promouvoir une paix et un développement durables dans les sociétés en transition sortant d'un conflit et/ou d'un long régime autoritaire. La raison principale de l'insécurité en Afrique est l'effondrement des systèmes de gouvernance, dû pour une large part au favoritisme et à l'utilisation abusive des instruments gouvernementaux de coercition afin d'ancrer l'exclusion politique et sociale. Au mieux, tout en gardant une apparence de confiance et de stabilité, cette situation a abouti à la répression des populations locales assujetties au pouvoir des régimes autoritaires en place, l'objectif premier étant de préserver le régime plutôt que d'assurer la sécurité de l'État et de ses

---

<sup>13</sup> - Questionnaire de l'étude sur la cybercriminalité (OIG et universités). Q70.

<sup>14</sup> - Principes directeurs pour la prévention du crime, annexe à la Résolution 2002/13 du Conseil économique et social des Nations sur les actions pour promouvoir une prévention efficace de la criminalité, 24 juillet 2002, paragraphe 3.

<sup>15</sup> - Ibid. Arts. 7 et 9.

<sup>16</sup> - Alan Bryden, Boubacar N'Diaye et 'Funmi Olonisakin (dir. publ.) Gouvernance du secteur de la sécurité en Afrique de l'Ouest : les défis à relever ; Centre pour le contrôle démocratique des forces armées – Genève (DCAF), Rue de Chante poulet 11, CP 1360, CH-1211 Genève 1, Suisse, p.03.

citoyens. Au pire, cela a déclenché des conflits armés et donné lieu à des catastrophes humanitaires.

Cependant, au cours des deux dernières décennies, l'Afrique de l'Ouest a connu des changements sans précédent dans la vie politique intérieure des États et les rapports entre ces derniers. L'on a assisté à une relative démocratisation dans la région. Quels principes sous-tendent la bonne gouvernance du secteur de la sécurité ? Quelle est l'importance de promouvoir l'application du principe de bonne gouvernance au cyberspace ?

La gouvernance du secteur de la sécurité (GSS) renvoie à « l'exercice du pouvoir et de l'autorité dans le contexte d'un secteur de sécurité nationale en particulier »<sup>17</sup>. Il s'agit d'un concept analytique qui ne repose pas sur un engagement à respecter des normes ou des valeurs spécifiques. Le concept de bonne GSS renvoie aux actions mises en œuvre pour optimiser l'efficacité et la responsabilité du secteur de la sécurité étatique dans le cadre d'un contrôle civil et démocratique et dans le respect de l'État de droit et du principe de l'État de droit<sup>18</sup>. En outre, le concept de bonne GSS repose sur l'idée selon laquelle le secteur de la sécurité doit être tenu de respecter les mêmes normes élevées que celles imposées aux autres prestataires de services du secteur public. Par conséquent, le non-respect de ces normes par le secteur de la sécurité peut nuire à la stabilité politique, économique et sociale d'un État. Il est important de reconnaître que les individus et les communautés ont des besoins de sécurité différents, y compris dans le cyberspace.

Pour ce qui est des normes, la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), ayant radicalement changé d'attitude depuis les années 90, insiste sur l'étroitesse des liens existants entre la sécurité et la bonne gouvernance politique<sup>19</sup>. Cette position s'est matérialisée par l'adoption de plusieurs instruments juridiques portant sur la paix, la sécurité et le développement, destinés à servir de cadre aux efforts déployés pour mettre en place la RSS au niveau national.

Dans sa mise en œuvre, la RSS implique des réformes structurelles et de long terme afin de stabiliser durablement le système sécuritaire d'un pays. La synthèse des différentes doctrines énumérées ci-dessus permet d'identifier comme suit les objectifs poursuivis dans le cadre de la réforme des systèmes de sécurité<sup>20</sup> :

---

<sup>17</sup> - CERT africains. Disponible sur : <https://www.africacert.org/african-csirts/>, P.11

<sup>18</sup> - Idem

<sup>19</sup> - Mohamed Ibn Chambas, « Foreword » dans *West Africa's Security Challenges: Building Peace in a Troubled Region*, dir. publ. A. Adebajo et I. Rashid (Boulder: Lynne Rienner, 2004, xiii.

<sup>20</sup> - sous la direction de Hugo Sada, avec la collaboration de Boubacar Issa Abdourhamane, Organisation internationale de la Francophonie, Paris, Rapport sur l'état des pratiques de la démocratie, des droits et des libertés dans l'espace francophone, Septembre 2008, pp.170-171.

- ✓ Établir une gouvernance démocratique et transparente du secteur de la sécurité dans le respect des droits de l'Homme et de l'État de droit ;
- ✓ Améliorer les capacités des institutions de sécurité et de justice et la qualité des services qu'elles fournissent grâce au renforcement du professionnalisme, de la compétence et de l'éthique des forces de leurs agents ;
- ✓ Répondre aux besoins de sécurité de l'État comme des populations ;
- ✓ Assurer l'appropriation locale des réformes ;
- ✓ Développer des stratégies plurisectorielles supposant à la fois la coordination des réformes engagées dans chacun des secteurs des systèmes de sécurité et la coordination étroite de l'aide apportée par les bailleurs internationaux.

L'instrument de la CEDEAO le plus élaboré du point de vue de son lien avec la paix, la sécurité et le développement est le Protocole de Dakar de 2001 sur la démocratie et la bonne gouvernance, addendum au Protocole relatif au Mécanisme de prévention, de gestion, de règlement des conflits, de maintien de la paix et de la sécurité, adopté à l'origine en 1999. Le Protocole établit les conditions préalables pour la paix et la sécurité dans 50 articles qui abordent de grands thèmes comme le rôle des forces armées et de sécurité dans une démocratie, les élections, l'État de droit, les droits de l'homme et la bonne gouvernance, et soulignent l'importance de disposer de forces armées et de sécurité bien formées, non partisans, apolitiques, autonomes et subordonnées.

En outre, une responsabilisation efficace repose sur un contrôle démocratique et civil. Celui-ci peut être exercé par les parlements nationaux et plus généralement par la société civile. Cette forme de contrôle joue un rôle clé pour assurer la responsabilité du secteur de la sécurité. Or, dans le cyberspace, le contrôle civil et démocratique du secteur de la sécurité est souvent affaibli pour diverses raisons. Le contrôle démocratique est souvent confronté aux obstacles suivants<sup>21</sup> :

- ✓ La complexité des réseaux en ligne constitue un premier obstacle au contrôle démocratique.
- ✓ La nécessité d'acquérir des connaissances techniques pour élaborer et mettre en œuvre une réglementation efficace
- ✓ Les complexités juridiques inhérentes au cyberspace en matière notamment de juridiction et d'attribution de compétences. La nature interconnectée et « sans frontières » du cyberspace soulève de véritables défis pour les cadres d'application de la loi traditionnellement définis sur une base territoriale. Les données et les

---

<sup>21</sup> - See Buckland, B., F. Schreier, and Th. H. Winkler, op. cit., pp. 18-19. Disponible sur : <https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf>

cyber-activités peuvent basculer de serveurs situés dans un État vers ceux situés dans un autre pays littéralement à la vitesse de la lumière.

Pour pallier ce déficit, il faut une bonne gouvernance et de la transparence du secteur de la sécurité. De manière générale, la transparence poursuit un double objectif : favoriser le partage d'informations de façon à assurer l'efficacité des institutions du secteur de la sécurité et contribuer de manière essentielle à leur responsabilisation. En outre, les nouvelles technologies de l'information et de la communication (NTIC) constituent, en elles-mêmes, un outil de promotion et de renforcement de la transparence qui facilite l'accès du public aux informations comme le préconise Habermas. La bonne gouvernance du secteur de la sécurité est un processus et elle constitue l'objectif de la réforme du secteur de la sécurité.

## Conclusion

Le désir d'une démocratie forte exprimé par l'homme l'a amené à emprunter le chemin de l'électronique et du numérique pour améliorer la communication et son accès à l'information. Aujourd'hui, la percée des Nouvelles Technologies de l'Information et de la Communication (NTIC) au sein du cyberspace nous donne l'image d'une société en progrès continu, avec des découvertes toujours nouvelles pour accroître la liberté de l'homme. Le numérique apparaît aujourd'hui comme une question fondamentale pour les démocraties. Les politiques l'ont compris, et ils multiplient les forums et les conférences sur la question du numérique, et sur son utilisation politique. La CEDEAO n'est pas en marge de cette révolution numérique.

Le cyberspace est un domaine mondial qui offre de très nombreuses ressources, informations et opportunités. Il est devenu un élément tellement essentiel de la vie quotidienne que le Conseil des droits de l'homme des Nations Unies a affirmé, en 2016, que :

Les mêmes droits dont les personnes disposent hors ligne doivent être aussi protégés en ligne, en particulier la liberté d'expression, qui est applicable indépendamment des frontières et quel que soit le média que l'on choisisse, conformément à l'article 19 de la Déclaration universelle des droits de l'homme et du Pacte international relatif aux droits civils et politiques<sup>22</sup>.

Le développement contemporain des NTIC constitue un tournant majeur de la civilisation humaine. L'objectif de ce rapport était d'explorer diverses questions liées à l'utilisation de la technologie en lien avec la question de la sécurité numérique et de la gouvernance démocratique en Afrique subsaharienne, en mettant plus particulièrement l'accent sur la façon dont les NTIC peuvent apporter un plus à l'amélioration et à la promotion d'une démocratie délibérative et garante des droits et libertés individuels et de l'état de droit sous-régional. Pour atteindre cet objectif, il faut une approche équilibrée, combinant réalisme et optimisme, pour façonner des

---

<sup>22</sup> - La promotion, la protection et l'exercice des droits de l'homme sur Internet, 32e session du Conseil des droits de l'homme (27 juin 2016), A/HRC/32/L.20

politiques favorables à une démocratie plus dynamique et inclusive au sein de la CEDEAO. Cette approche nuancée nous permet d'exploiter les avantages des NTIC tout en préservant les principes fondamentaux de la démocratie habermassienne tels que la communication libre et égalitaire, la participation citoyenne et la délibération politique au sein de la CEDEAO. Les mécanismes de coopération inclus dans les instruments régionaux et internationaux contre la cybercriminalité doivent être placés dans le contexte plus large de la coopération internationale. Bien que de nombreux instruments puissent servir de base juridique pour des actes de coopération spécifiques, il ne faut pas oublier que les États parties aux instruments sont également parties à des accords bilatéraux et multilatéraux concernant la coopération en matière pénale ; cela inclut les traités tels que la Convention sur la criminalité organisée.

Nonobstant ce progrès numérique dont la clé de voûte est Internet, la société court le risque de dépersonnalisation et de déstructuration des relations humaines. L'homme de la modernité avancée est sous l'emprise des NTIC qui le tiennent en esclavage et l'aliènent. Sa liberté illimitée de communiquer et d'accès à l'information à partir d'Internet est une liberté pathologique dans laquelle il est en cage sans possibilité de se mouvoir. C'est le lieu d'éveiller la conscience de nos sociétés soumises à la dictature des relations virtuelles au détriment des relations physiques. Ainsi, pour que le monde du numérique soit utile à l'homme, une adaptation progressive et profonde rationnelle s'impose à lui. Il est difficile de nos jours de disqualifier le monde du numérique et des réseaux sociaux qui nous mobilisent et nous tiennent captifs ; c'est-à-dire que se mettre en marge du monde numérique signifie s'extraire de cet espace qui fonde de plus en plus, aujourd'hui, notre sociabilité. C'est pourquoi, face à cette aliénation dans laquelle s'enlisent les hommes et les femmes, nous en appelons à la raison et à la mesure pour le bon usage d'Internet et des réseaux sociaux.

## Références Bibliographiques

- AfricaCERT. (n.d.). African CSIRTs. <https://www.africacert.org/african-csirts/>
- Audard, C. (2002). Le principe de légitimité démocratique. Dans Habermas : L'usage public de la raison (p. 115). Presses Universitaires de France.
- AusCERT. (2008). Enquête sur la sécurité des utilisateurs d'ordinateurs particuliers 2008.
- Bobbio, N. (1997). Libéralisme et démocratie.
- Bryden, A., N'Diaye, B., & Olonisakin, F. (Eds.). (2008). Gouvernance du secteur de la sécurité en Afrique de l'Ouest : Les défis à relever. Geneva Centre for the Democratic Control of Armed Forces (DCAF).
- Buckland, B., Schreier, F., & Winkler, T. H. (n.d.). On cyberwarfare. Geneva Centre for the Democratic Control of Armed Forces.  
<https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf>
- Callanan, C., Gercke, M., De Marco, E., & Dries-Ziekenheiner, H. (2009). Étude sur le blocage d'Internet : Équilibrer les ripostes à la cybercriminalité dans les sociétés démocratiques. Aconite Internet Solutions.
- Chambas, M. I. (2004). Foreword. In A. Adebajo & I. Rashid (Eds.), West Africa's security challenges: Building peace in a troubled region (p. xiii). Lynne Rienner.
- Gibson, W. (1984). Neuromancer. Ace Books.
- Habermas, J. (1968). La technique et la science comme idéologie. Suhrkamp Verlag.
- Habermas, J. (1978). L'espace public : Archéologie de la publicité comme dimension constitutive de la société bourgeoise. Payot.
- Habermas, J. (1987). Théorie de l'agir communicationnel. Fayard.
- Habermas, J. (1997). Droit et démocratie : Entre faits et normes. Gallimard.
- Hong Kong EIVC. (2010). Rapport final de l'EIVC de Hong Kong.
- Instituto Nacional de Estadística y Geografía. (INEGI). (2012). Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE): Cuestionario principal.
- Kouadio, K. D. (2015). Jürgen Habermas : L'éthique de la communication : Vers une théorie discursive de la démocratie. Presses Académiques Francophones.
- Lebert, M.-F. (1999). De l'imprimé à Internet (Doctoral dissertation). Éditions 00h00.
- McAfee & National Cyber Security Alliance. (2012). Enquête sur la cybersécurité en ligne.
- Ministère de l'Intérieur de Côte d'Ivoire. (n.d.). Cybercriminalité.  
<http://www.cybercrime.interieur.gouv.ci/?q=node/4>
- Organisation for Economic Co-operation and Development. (2002). Recommendation of the Council concerning guidelines for the security of information systems and networks: Towards a culture of security (C(2002)131/FINAL).
- Organisation internationale de la Francophonie. (2008). Rapport sur l'état des pratiques de la démocratie, des droits et des libertés dans l'espace francophone.
- Questionnaire de l'étude sur la cybercriminalité (OIG et universités). (n.d.). Questionnaire de recherche.
- Symantec. (2012). Norton cybercrime report 2012.
- United Nations Economic and Social Council. (2002). Guidelines for the prevention of crime (Resolution 2002/13).
- United Nations Human Rights Council. (2016, June 27). La promotion, la protection et l'exercice des droits de l'homme sur Internet (A/HRC/32/L.20).
- United Nations Office on Drugs and Crime, & Conference of European Statisticians. (2010). Manual on victimization surveys.

- U.S. Department of Justice, Bureau of Justice Statistics. (2008). Identity theft supplement to the National Crime Victimization Survey (NCVS).