Revue des Sciences humaines et sociales, Lettres, Langues et Civilisations

ISSN
(E) 2958-2814
(P) 3006-306X

Numéro 007, Juin 2024

Université Alassane Ouattara
UFR Communication Milieu et Société

revue.akiri-uao.org

REVUE AKIRI
Revue des Sciences Humaines et Sociales, Lettres, Langues et Civilisations

ISSN-L: 2958-2814
ISSN-P: 3006-306X

Site web: https://revue.akiri-uao.org/

E-mail : revueakiri@gmail.com

Editeur

UFR Communication, Milieu et Société

Université Alassane Ouattara, Bouaké (Côte d'Ivoire)

ISSN-L: 2958-2814
ISSN-P: 3006-306X

INDEXATIONS INTERNATIONALES

Pour toutes informations sur l'indexation internationale de la revue ***AKIRI***, consultez les bases de données ci-dessous :

auréHAL
accès aux données de référence de HAL

https://aurehal.archives-ouvertes.fr/journal/read/id/398946

Mir@bel
"(RE)CUEILLIR LES SAVOIRS"

https://reseau-mirabel.info/revue/15150/Akiri

Scientific Journal Impact Factor

http://sjifactor.com/passport.php?id=23334

Academic Resource Index ResearchBib

https://journalseeker.researchbib.com/view/issn/2958-2814

ORCID

https://orcid.org/0009-0002-6794-1377

SJIF 2024 : 5.214

ISSN-L: 2958-2814
ISSN-P: 3006-306X

REVUE ELECTRONIQUE

AKIRI

Revue Scientifique des Sciences humaines et sociales, Lettres, Langues et Civilisations
E-ISSN 2958-2814 (Online ou en Ligne)
I-ISSN 3006-306X (Print ou imprimé)

Equipe Editoriale

Coordinateur Général : BRINDOUMI Kouamé Atta Jacob
Directeur de publication : MAMADOU Bamba
Rédacteur en chef : KONE Kiyali
Chargéde diffusion et de marketing : KONE Kpassigué Gilbert
Webmaster : KOUAKOU Kouadio Sanguen

Comité Scientifique

SEKOU Bamba, Directeur de recherches, IHAAA, Université Félix Houphouët-Boigny
OUATTARA Tiona, Directeur de recherches, IHAAA, Université Félix Houphouët-Boigny
LATTE Egue Jean-Michel, Professeur titulaire, Université Alassane Ouattara
FAYE Ousseynou, Professeur titulaire, Université Cheick Anta Diop
GOMGNIMBOU Moustapha, Directeur de recherches, CNRST,
ALLOU Kouamé René, Professeur titulaire, Université Félix Houphouët-Boigny
KAMATE Banhouman André, Professeur titulaire, Université Félix Houphouët-Boigny
ASSI-KAUDJHIS Joseph Pierre, Professeur titulaire, Université Alassane Ouattara
SANGARE Abou, Professeur titulaire, Université Peleforo Gbon Coulibaly
SANGARE Souleymane, Professeur titulaire, Université Alassane Ouattara
CAMARA Moritié, Professeur titulaire, Université Alassane Ouattara
COULIBALY Amara, Professeur titulaire, Université Alassane Ouattara
NGAMOUNTSIKA Edouard, Professeur titulaire, Université Marien N'gouabi de Brazzaville
KOUASSI Kouakou Siméon, Professeur titulaire, Université de San-Pedro
BATCHANA Essohanam, Professeur titulaire, Université de Lomé
N'SONSSISA Auguste, Professeur titulaire, Université Marien N'gouabi de Brazzaville
DEDOMON Claude, Professeur titulaire, Université Alassane Ouattara
BAMBA Mamadou, Professeur titulaire, Université Alassane Ouattara
NGUE Emmanuel, Maître de conférences, Université de Yaoundé I
N'GUESSAN Mahomed Boubacar, Professeur titulaire, Université Félix HouphouëtBoigny
BA Idrissa, Professeur titulaire, Université Cheick Anta Diop
KAMARA Adama, Maître de conférences, Université Alassane Ouattara
SARR Nissire Mouhamadou, Maître de conférences, Université Cheick Anta Diop
ALLABA Djama Ignace, Maître de conférences, Université Félix Houphouët-Boigny
DIARRASSOUBA Bazoumana, Maître de conférences, Université Alassane Ouattara
TOPPE Eckra Lath, Maître de conférences, Université Alassane Ouattara
M'BRA Kouakou Désiré, Maître conférences, Université Alassane Ouattara

ISSN-L: 2958-2814
ISSN-P: 3006-306X

Comité de Lecture

BATCHANA Essohanam, Professeur titulaire, Université de Lomé
N'SONSSISA Auguste, Professeur titulaire, Marien N'gouabi de Brazzaville
CAMARA Moritié, Professeur titulaire, Université Alassane Ouattara
FAYE Ousseynou, Professeur titulaire, Université Cheick Anta Diop
BA Idrissa, Maître de conférences, Université Cheick Anta Diop
BAMBA Mamadou, Professeur titulaire, Université Alassane Ouattara
SARR Nissire Mouhamadou, Maître de conférences, Université Cheick Anta Diop
GOMGNIMBOU Moustapha, Directeur de recherches,
DEDOMON Claude, Professeur titulaire, Université Alassane Ouattara
BRINDOUMI Atta Kouamé Jacob, Professeur titulaire, Université Alassane Ouattara
DIARRASOUBA Bazoumana, Maître de conférences, Université Alassane Ouattara
ALABA Djama Ignace, Maître de conférences, Université Alassane Ouattara
DEDE Jean Charles, Maître-Assistant, Université Alassane Ouattara
BAMBA Abdoulaye, Maître de conférences, Université Félix Houphouët-Boigny
BAKAYOKO Mamadou, Maître de conférences, Université Alassane Ouattara
SANOGO Lamine Mamadou, Directeur de recherches, CNRST, Ouagadougou
GOMA-THETHET Roval, Maître-Assistant, Université Marien N'gouabi de Brazzaville
GBOCHO Roselyne, Maître-Assistante, Université Alassane Ouattara
SEKA Jean-Baptiste, Maître-Assistant, Université Lorognon Guédé,
SANOGO Tiantio, Maître-Assistante, Institut National Supérieur des Arts et de l'Action Culturelle
ETTIEN N'doua Etienne, Maître-Assistant, Université Félix Houphouët-Boigny
DJIGBE Sidjé Edwige Françoise, Maître-Assistante, Université Alassane Ouattara
YAO Elisabeth, Maître-Assistante, Université Alassane Ouattara

Comité de rédaction

N'SONSSISA Auguste, Professeur titulaire, Marien N'gouabi de Brazzaville
KONÉ Kpassigué Gilbert, Maître-Assistant, Histoire, Université Alassane Ouattara
KONÉ Kiyali, Maître-Assistant, Histoire, Université Péléforo Gon Coulibaly
BAKAYOKO Mamadou, Maître de Conférences, Philosophie, Université Alassane Ouattara
OULAI Jean-Claude, Professeur titulaire, Communication, Université Alassane Ouattara
MAMADOU Bamba, Maître-Assistant, Histoire, Université Alassane Ouattara
TOPPE Eckra Lath, Maître de Conférences, Etudes Germaniques, Université Alassane Ouattara,
ALLABA Djama Ignace, Maître de Conférences, Etudes Germaniques, Université Félix Houphouët-Boigny,
KONAN Koffi Syntor, Maître de Conférences, Espagnol, Université Alassane Ouattara
SIDIBÉ Moussa, Maître-Assistant, Lettres Modernes, Université Alassane Ouattara
ASSUÉ Yao Jean-Aimé, Maître de Conférences, Géographie, Université Alassane Ouattara
KAZON Diescieu Aubin Sylvère, Maître de Conférences, Criminologie, Université Félix Houphouët-Boigny
MEITÉ Ben Soualiouo, Maître de Conférences, Histoire, Université Félix Houphouët-Boigny
BALDÉ Yoro Mamadou, Assistant, FASTEF, Université Cheikh Anta Diop de Dakar
MAWA Miraille-Clémence, Chargée de cours, Université de Bamenda

ISSN-L: 2958-2814
ISSN-P: 3006-306X

Contacts

Site web: **https://revue.akiri-uao.org/**
E-mail : revueakiri@gmail.com
Tél. : + 225 0748045267 / 0708399420/ 0707371291

Indexations internationales :

Auré HAL : https://aurehal.archives-ouvertes.fr/journal/read/id/398946

Mir@bel : https://reseau-mirabel.info/revue/15150/Akiri

Sjifactor : http://sjifactor.com/passport.php?id=23334

Academic Resource Index: https://journalseeker.researchbib.com/view/issn/2958-2814

ORCID : https://orcid.org/0009-0002-6794-1377

Facteur d'impact ou Impact Factor (IF)

Année 2024 : 5.214
Année 2023 : 3,023

ISSN-L: 2958-2814
ISSN-P: 3006-306X

PRESENTATION DE LA REVUE AKIRI

Dans un environnement marqué par la croissance, sans cesse, des productions scientifiques, la diffusion et la promotion des acquis de la recherche deviennent un impératif pour les acteurs du monde scientifique. Perçues comme un patrimoine, un héritage à léguer aux générations futures, les productions scientifiques doivent briser les barrières et les frontières afin d'être facilement accessibles à tous.

Ainsi, s'inscrivant dans la dynamique du temps et de l'espace, la revue « ***AKIRI*** » se présente comme un outil de promotion et de diffusion des résultats des recherches des enseignants-chercheurs et chercheurs des universités et de centres de recherches de Côte d'Ivoire et d'ailleurs. Ce faisant, elle permettra aux enseignants-chercheurs et chercheurs de s'ouvrir davantage sur le monde extérieur à travers la diffusion de leurs productions intellectuelles et scientifiques.

AKIRI est une revue à parution trimestrielle de l'Unité de Formation et de Recherches (UFR) : Communication, Milieu et Société (CMS) de l'Université Alassane Ouattara. Elle publie les articles dans le domaine des Sciences humaines et sociales, Lettres, Langues et Civilisations. Sans toutefois être fermée, cette revue privilégie les contributions originales et pertinentes. Les textes doivent tenir compte de l'évolution des disciplines couvertes et respecter la ligne éditoriale de la revue. Ils doivent en outre être originaux et n'avoir pas fait l'objet d'une acceptation pour publication dans une autre revue à comité de lecture.

ISSN-L: 2958-2814
ISSN-P: 3006-306X

PROTOCOLE DE REDACTION DE LA REVUE AKIRI

La revue ***AKIRI*** n'accepte que des articles inédits et originaux dans diverses langues notamment en allemand, en anglais, en espagnol et en Français. Le manuscrit est remis à deux instructeurs, choisis en fonction de leurs compétences dans la discipline. Le secrétariat de la rédaction communique aux auteurs les observations formulées par le comité de lecture ainsi qu'une copie du rapport, si cela est nécessaire. Dans le cas où la publication de l'article est acceptée avec révisions, l'auteur dispose alors d'un délai raisonnable pour remettre la version définitive de son texte au secrétariat de la revue

Structure générale de l'article :
Le projet d'article doit être envoyé sous la forme d'un document Word, police Times New Roman, taille 12 et interligne 1,5 pour le corps de texte (sauf les notes de bas de page qui ont la taille 10 et les citations en retrait de 2 cm à gauche et à droite qui sont présentées en taille 11 avec interligne 1 ou simple). Le texte doit être justifié et ne doit pas excéder 18 pages. Le manuscrit doit comporter une introduction, un développement articulé, une conclusion et une bibliographie.

Présentation de l'article :

- Le titre de l'article (15 mots maximum) doit être clair et concis. De taille 14 pts gras, il doit être centré.
- Juste après le titre, l'auteur doit mentionner son identité (Prénom et NOM en gras et en taille 12), ses adresses (institution, e-mail, pays et téléphones en italique et en taille 11)
- Le résumé (200 mots au maximum) présenté en taille 10 pts ne doit pas être une reproduction de la conclusion du manuscrit. Il est donné à la fois en français et en anglais (abstract). Les mots-clés (05 au maximum, taille 10pts) sont donnés en français et en anglais (key words)
- Le texte doit être subdivisé selon le système décimal et ne doit pas dépasser 3 niveaux exemples : (1. - 1.1. - 1.2. ; 2. - 2.1. -2.2. - 2.3. - 3. - 3.1. - 3.2. etc.)
- Les références des citations sont intégrées au texte comme suit : (L'initial du prénom suivi d'un point, nom de l'auteur avec l'initiale en majuscule, année de publication suivie de deux points, page à laquelle l'information a été prise). Ex : (A. Kouadio, 2000 : 15).
- La pagination en chiffre arabe apparait en haut de page et centrée.
- Les citations courtes de 3 lignes au plus sont mises en guillemet français («…. »), mais sans italique.

N.B. : Les caractères majuscules doivent être accentués. Exemple : État, À partir de …

ISSN-L: 2958-2814
ISSN-P: 3006-306X

Références bibliographiques

Ne sont utilisées dans la bibliographie que les références des documents cités. Les références bibliographiques sont présentées par ordre alphabétique des noms d'auteur. Les divers éléments d'une référence bibliographique sont présentés comme suit : NOM et Prénom (s) de l'auteur, Année de publication, zone titre, lieu de publication, zone éditeur, pages (p.) occupées par l'article dans la revue ou l'ouvrage collectif.

Dans la zone titre, le titre d'un article est présenté entre guillemets et celui d'un ouvrage, d'un mémoire ou d'une thèse, d'un rapport, d'une presse écrite est présenté en italique. Dans la zone éditeur, on indique la maison d'édition (pour un ouvrage), le Nom et le numéro/volume de la revue (pour un article). Au cas où un ouvrage est une traduction et/ou une réédition, il faut préciser après le titre le nom du traducteur et/ou l'édition (ex : 2nde éd.).

Les références des sources d'archives, des sources orales et les notes explicatives sont numérotées en série continue et présentées en bas de page.

- Pour les sources orales, réaliser un tableau dont les colonnes comportent un numéro d'ordre, nom et prénoms des informateurs, la date et le lieu de l'entretien, la qualité et la profession des informateurs, son âge ou sa date de naissance et les principaux thèmes abordés au cours des entretiens. Dans ce tableau, les noms des informateurs sont présentés en ordre alphabétique
- Pour les sources d'archives, il faut mentionner en toutes lettres, à la première occurrence, le lieu de conservation des documents suivi de l'abréviation entre parenthèses, la série et l'année. C'est l'abréviation qui est utilisée dans les occurrences suivantes :
  Ex. : Abidjan, Archives nationales de Côte d'Ivoire (A.N.C.I), 1EE28, 1899.

- Pour les ouvrages, on note le NOM et le prénom de l'auteur suivis de l'année de publication, du titre de l'ouvrage en italique, du lieu de publication, du nom de la société d'édition et du nombre de page.
  Ex : LATTE Egue Jean-Michel, 2018, *L'histoire des Odzukru, peuple du sud de la Côte d'Ivoire, des origines au XIX*^{e} *siècle*, Paris, L'Harmattan, 252 p.

- Pour les périodiques, le NOM et le(s) prénom(s) de l'auteur sont suivis de l'année de la publication, du titre de l'article entre guillemets, du nom du périodique en italique, du numéro du volume, du numéro du périodique dans le volume et des pages.
  Ex : BAMBA Mamadou, 2022, « Les Dafing dans l'évolution économique et socio-culturelle de Bouaké, 1878-1939 », *NZASSA*, N°8, p.361-372.

NB : Les articles sont la propriété de la revue.

ISSN-L: 2958-2814
ISSN-P: 3006-306X

SOMMAIRE

LANGUES, LETTRES ET CIVILISATIONS

Anglais

Études hispaniques

Lettres Modernes

SCIENCES HUMAINES ET SOCIALES

Archéologie

ISSN-L: 2958-2814
ISSN-P: 3006-306X

Histoire

Géographie

ISSN-L: 2958-2814
ISSN-P: 3006-306X

ISSN-L: 2958-2814
ISSN-P: 3006-306X

ISSN-L: 2958-2814
ISSN-P: 3006-306X

REVUE AKIRI
Revue des Sciences Humaines et Sociales, Lettres, Langues et Civilisations

ISSN-L: 2958-2814
ISSN-P: 3006-306X

Cybercriminalité et cybersécurité en Afrique : pourquoi articuler l'action techno-juridique et la responsabilité collective ?

Koffi AGNIDE
Philosophie politique et sociale
Département de philosophie - Université de Lomé
https://orcid.org/0009-0005-9753-431X
E-mail : agnidekoffi@yahoo.fr
&
Yaou Gagnon ALI
Bioéthique et Éthique des Sciences et Technologies
Département de philosophie - Université de Lomé
Identifiant : 0009-0001-9868-7829
E-mail : aligagnon9@gmail.com

Résumé

Cet article analyse la cybercriminalité en Afrique au prisme avec la responsabilité collective. En effet, les actes de cyberattaques et de cybercriminalité éprouvent les pays du monde entier de façon générale et particulièrement les États africains. Mais les réponses juridiques opposées à la cybercriminalité sont déficitaires et ont subséquemment du mal à faire face à la situation au regard du fait qu'il s'agit d'un domaine virtuel. C'est pourquoi cet article questionne la cybercriminalité au-delà du cadre juridique en l'inscrivant dans la perspective d'une vision collective de la responsabilité. Ainsi, il montre que c'est avec une responsabilité collective bien comprise, assumée et adaptée que l'Afrique peut gérer au mieux les risques liés au cyberespace et gérer la cybercriminalité. Il faut donc, au-delà des efforts politiques et juridiques de gestion de la cybercriminalité, une appropriation de la lutte contre le péril dans le cadre d'une responsabilité collective mobilisant les différents acteurs, les parties prenantes et les valeurs éthiques.

Mots clés : Cybercriminalité, Cybersécurité, Systèmes informatiques, Responsabilité collective, Cyberespace.

Cybercrime and cybersecurity in africa: why articulate techno-legal action and collective responsibility?

Abstract

This article analyzes cybercrime in Africa through the prism of collective responsibility. Indeed, acts of cyberattacks and cybercrime are affecting countries around the world in general, and African states in particular. But the legal responses to cybercrime are deficient and subsequently struggle to contain the situation given the fact that it is a virtual domain. This is why this article questions cybercrime beyond the legal framework by placing it in the perspective of a collective vision of responsibility. Thus, it shows that it is with a collective responsibility that is well understood, assumed and adapted that Africa can best manage the risks associated with cyberspace and curb cybercrime. It is therefore necessary, beyond political and legal efforts to manage cybercrime, to take ownership of the fight against the danger within the framework of a collective responsibility mobilizing the various actors, stakeholders and ethical values.

Keywords: Cybercrime, Cybersecurity, Computer systems, Collective responsibility, Cyberspace.

ISSN-L: 2958-2814
ISSN-P: 3006-306X

Introduction

Les sociétés contemporaines sont marquées par le développement des nouvelles technologies parmi lesquelles se trouve la technologie informatique ou mieux, les systèmes informatiques. Nous vivons dans un monde fait de ce qu'il convient d'appeler avec JJ. Salomon (1970), la « technonature », c'est-à-dire un monde dans lequel la technologie, l'économie et la politique se rendent des services mutuels. Le développement économique ne peut se faire sans compter sur la puissance technologique. Dans le sens de cette affirmation, l'économie s'appuie notamment sur les systèmes informatiques, surtout dans la commercialisation et l'élargissement de la clientèle. De même, les campagnes électorales ne se font pas sans l'appui des outils informatiques. Mais, au-delà des atouts des systèmes informatiques dans les administrations publiques, dans les domaines de la médicine et de la science en générale, en économie et dans les différentes sphères de la vie humaine, il y a aussi de sérieux dangers liés aux systèmes informatiques. On notera à partir de 1988, date à laquelle la première attaque cybernétique a eu lieu aux États-Unis d'Amérique, une série de cyberattaques et d'actes de cybercriminalité de tout genre. Ces attaques et actes terroristes vont affecter presque tous les domaines essentiels et menacer la sécurité et la liberté des individus, des structures étatiques, privées ou autres.

En effet, les actes de cyberattaques et de cybercriminalité éprouvent les pays du monde entier de façon générale et particulièrement les États africains. Mais les réponses juridiques et techniques à la cybercriminalité sont insuffisantes. Elles peinent à faire face à la situation en raison du fait qu'il s'agit d'un domaine virtuel sur lequel les États africains n'ont pas de grande emprise. C'est pourquoi cet article questionne la cybersécurité en Afrique au-delà du cadre techno-juridique en l'inscrivant dans la perspective de la responsabilité collective. La question principale qui structure et oriente ce travail est donc celle du renforcement de la cybersécurité en Afrique où l'approche techno-juridique peine à réduire les risques liés à la cybercriminalité. La réponse à cette question, qui constitue l'hypothèse que ce texte tente de défendre, est que pour renforcer la cybersécurité en Afrique afin de réduire les risques liés à la cybercriminalité, il faut développer, au-delà de l'approche techno-juridique, une responsabilité collective. Ainsi, c'est avec une responsabilité collective bien comprise, assumée et adaptée que l'Afrique peut gérer au mieux les risques liés au cyberespace, faire face la cybercriminalité et subséquemment renforcer sa cybersécurité.

Au regard de l'actualité du sujet, notre approche dans cet article est celle d'une philosophie de terrain. Celle-ci consiste d'une part à prendre en compte les faits réels. C'est pourquoi la rédaction de l'article s'est appuyée sur des travaux et rapports qui relatent les faits réels sur la

ISSN-L: 2958-2814
ISSN-P: 3006-306X

cybercriminalité en Afrique. D'autre part, l'approche exige une analyse critique et normative en ce sens qu'elle conduit à faire une évaluation critique de la réalité étudiée et à faire des propositions en vue de la résolution du problème soulevé par le fait étudié.

L'argumentation requise pour analyser la question et élucider notre hypothèse passe par trois points. D'abord, nous montrerons que l'Afrique est à l'épreuve des cyberattaques et de la cybercriminalité. Cela nécessite une action concrète et efficace. Les actions se sont souvent inscrites dans la logique de l'élaboration des lois et du renforcement des outils informatiques. Ces actions n'ont pas donné lieu à des résultats escomptés. C'est pour cela que nous présenterons ensuite, les difficultés de l'action techno-juridique en Afrique face à la cybercriminalité. Il faut, pour solutionner ces difficultés et rendre l'action efficace, trouver d'autres pistes. C'est pour cette raison que notre troisième point fait, enfin, de la responsabilité collective, la condition fondamentale du renforcement de la cybersécurité en Afrique.

1. L'Afrique à l'épreuve des cyberattaques et de la cybercriminalité

Les cibles de la cybercriminalité et des cyberattaques dans le monde actuel sont nombreuses et variées. Aucune société n'est durablement à l'abri du danger. Par cyberattaque, il faut entendre un effort intentionnel visant à voler, exposer, modifier, désactiver ou détruire des données, des applications ou d'autres actifs par le biais d'un accès non autorisé à un réseau, un système informatique ou un appareil numérique. Parmi les actes de cyberattaques, on note l'hameçonnage, le harponnage, le piratage de comptes, le cheval de Troie. C'est en considérant ces attaques informatiques comme des délits qu'est né le terme cybercriminalité qui désigne tout délit commis en utilisant un réseau informatique ou internet. La cybercriminalité est un fait qui touche toutes les sociétés, tous les pays et tous les continents. Cette affirmation se justifie par une double réalité propre aux sociétés contemporaines. D'une part, cela se justifie par la mondialisation à travers laquelle les pratiques et les cultures se décloisonnent, s'uniformisent et se mondialisent au même titre que les risques qui se globalisent (U. Beck, 2003). Ainsi, les mêmes pratiques et risques se retrouvent sur presque tous les continents. L'ampleur de la cybercriminalité et des cyberattaques dans le monde s'explique par le fait que les entreprises, les administrations et les citoyens dans tous les pays utilisent les systèmes informatiques. La pandémie de covid-19 a augmenté le processus de numérisation à tous les niveaux et en utilisant de façon croissante le système informatique, toutes les entreprises sont exposées aux attaques informatiques et à la cybercriminalité. On a affaire à une véritable société numérique du risque qui vient s'ajoutent aux périls de la société du risque bien analysée par U. Beck (2008).

ISSN-L: 2958-2814
ISSN-P: 3006-306X

D'autre part, on peut justifier l'affirmation selon laquelle la cybercriminalité est un fait qui touche toutes les sociétés, tous les pays et tous les continents par le fait même que les pays dans leur souci de modernisation et de développement, s'appuient sur la technologie. Ainsi, avec la bureaucratisation des services, la technologie devient l'outil incontournable dans l'administration et dans les autres secteurs de la société. Les pays utilisent les technologies informatiques dans tous les secteurs d'activités et s'exposent par le biais leur utilisation aux attaques informatiques et à la cybercriminalité. La qualité des systèmes informatiques renforce leur niveau de vulnérabilité et les expose aux attaques dans les contextes des États africains où les dispositions prises et les législations nationales ne parviennent pas à réguler les différents usages qu'on peut faire des outils informatiques. En réalité, par sa nature supranationale et globale, le cyberespace où se déploient les attaques et la cybercriminalité est, selon D. Ventre et H. Loiseau (2023 : 1) « difficile à gouverner et à sécuriser ». Car,

> Compte tenu de la quantité d'informations qui transitent sur les réseaux à chaque instant, superviser et contrôler les informations et les transactions, vérifier la légitimité et la légalité des contenus, traiter dans des délais raisonnables les plaintes ou rapports d'incidents sont autant de défis pour les organes de surveillance gouvernementaux, industriels, publics ou privés. Les phases de détection et de rétablissement peuvent être affectées par ces limites capacitaires, rendant les systèmes non opérationnels, ou les exposant à des risques multiples (D. Ventre et H. Loiseau, 2023 :1).

Tout en saluant les avantages indéniables des technologies informatiques dans les services et dans le développement des nations, il faut tout de même faire remarquer qu'elles exposent les pays aux risques liés à la cybercriminalité et aux cyberattaques. Dans son livre intitulé *La cybersécurité*, N. Arpagian (2015) a analysé les sociétés actuelles et note que la dépendance de nos données médicales et bancaires ainsi que celle de nos entreprises et de nos administrations publiques ou de nos structures militaires des systèmes informatiques renforce leur vulnérabilité à la cybercriminalité. Puisque, souligne-t-il, les États peuvent être attaqués par des personnes isolées, des citoyens et les entreprises peuvent être la cible des attaques informatiques. La sécurisation des données sensibles devient une nécessité vitale. Les données numériques deviennent un patrimoine à protéger. L'Afrique n'échappe pas à cette réalité et à ces risques. Par exemple, Medusa, Karakurt, Bianlian et d'autres groupes de « hackers » ont revendiqué des attaques contre des entreprises comme Bank of Africa et des gouvernements comme le gouvernement sénégalais (Jeune Afrique, 2023). Il convient à ce niveau de notre argumentation d'évoquer et d'analyser la réalité des cyberattaques en Afrique.

En 2020, l'Afrique a connu des cyberattaques malgré le contexte de la pandémie de covid-19. C'est ainsi que Kaspersky Lab, qui est une compagnie de cybersécurité, a noté qu'au premier

ISSN-L: 2958-2814
ISSN-P: 3006-306X

trimestre de 2020 plusieurs attaques informatiques ont touché plusieurs pays Africains. Les trois pays africains les plus touchés étaient l'Algérie, le Nigéria et la Tunisie. Les attaques informatiques dans ces trois pays concernent pour la plupart les appareils mobiles. En Algérie, 21,44% des utilisateurs de smartphones ont eu leurs machines infectées par un maliciel contre 15,58% au Nigéria et 14,94% en Tunisie (Africa Cybersecurity Magazine, 2020).

Kaspersky dans un rapport, qui remonte à 2020, fait état de 28 millions d'attaques par les logiciels malveillants et de 102 millions de détections d'applications indésirables qu'on abrège en anglais PUA[1] (Kaspersky Lab, Rapport 2020). Les chercheurs de cette compagnie internationale spécialisée dans la cybersécurité, dans leur évaluation de la menace, ont noté que les PUA attaquaient plus fréquemment les utilisateurs que les logiciels malveillants traditionnels. Cette affirmation trouve sa justification dans le rapport de l'étude réalisée par les chercheurs de cette compagnie en Afrique du Sud. Cette étude de cas a montré qu'en sept mois au cours de l'année 2020, les logiciels malveillants traditionnels ont attaqué 415000 utilisateurs alors que dans la même période, les PUA ont attaqué 736000 utilisateurs. Durant la même période cette fois-ci au Nigéria, les logiciels malveillants ont attaqué 3,8 millions d'utilisateurs contre 16,8 millions utilisateurs attaqués par les PUA. Pour toute l'année 2020, on a recensé 10 millions d'attaques des logiciels malveillants contre 43 millions d'attaques des PUA alors qu'au Kenya, on a enregistré 14 millions d'attaques liées aux logiciels malveillants et 41 millions d'attaques liées aux PUA.

Dans une étude intitulée « Étude de la maturité Cybersécurité 2021 en Afrique francophone », le cabinet Deloitte a analysé dans 11 pays 210 entreprises (Deloitte, Rapport de 2021). Dans son rapport, le cabinet note que 40% des entreprises analysées ont connu une augmentation du nombre d'incidents ou de cas de cyberattaques depuis 2019 qui coïncide avec le début de la pandémie de covid. Ces incidents oscillent entre logiciels malveillants et attaques de phishing qui sont devenus les cas les plus enregistrés. De même, Kaspersky révèle qu'entre Janvier et Août 2020, l'Afrique a enregistré 28 millions de cyberattaques. Ces 28 millions ont fait perdre à l'Afrique, estime Kaspersky, 4,12 milliards de dollars. Le 22 Juin 2023, le groupe de hackers Bianlian a volé 256 gigaoctets de données financières internes qui concerne les données de clients, rapport de crédits et prêts bancaires, dossiers administratifs et financiers, les

[1] Cette expression est anglaise et signifie Potentially Unwanted Application. En français la traduction est Application Potentiellement Indésirable.

ISSN-L: 2958-2814
ISSN-P: 3006-306X

coordonnées à la BGFI Bank, un groupe bancaire gabonais. Ceci révèle la vulnérabilité de l'Afrique aux cyberattaques (Kaspersky Lab, Rapport de 2023).

La vulnérabilité de l'Afrique en ce qui concerne les cyberattaques et la cybercriminalité se voit donc avec la vulnérabilité des entreprises privées telles que les institutions bancaires. Par exemple, le groupe de cybercriminel appelé « silence » s'attaque souvent aux institutions bancaires africaines. Ce groupe procède par envoie d'e-mail aux banques et par l'intermédiaire de ces e-mails, il installe des logiciels malveillants sur le système de sécurité afin de s'infiltrer et de voler les données. C'est ce que confirme l'étude réalisée par Dataprotect qui est une entreprise marocaine de cyberdéfense. L'étude a été réalisé auprès de 148 institutions bancaires de la zone UEMOA et dans trois autres pays d'Afrique centrale. Le rapport de cette étude a pu montrer que 85% des institutions bancaires couvertes par l'étude ont déjà été victime d'une ou de plusieurs attaques cybernétiques. Ces attaques concernes soit les fuites d'informations, l'usurpation d'identité, soit les fraudes sur les cartes bancaires, les intrusions dans les systèmes d'informations des banques.

Dans le sens même sens que l'affirmation précédente, en 2018, l'institution NSIA Banque Côte-d'Ivoire avait publié une information dans laquelle elle reconnaissait d'énormes dégâts suite à un détournement de fonds par piratage informatique. L'institution bancaire aurait perdu un montant avoisinant 1,2 milliard de franc CFA. Aussi faut-il rappeler qu'en Mars 2019, la filiale sénégalaise d'Ecobank a reconnu avoir subi une cyberattaque qui l'a fait perdre 323 millions de franc CFA (Kaspersky Lab, Rapport de 2020). Il convient de ne pas passer sous silence l'attaque de la Banque de l'Habitat du Sénégal en Février 2020 par des Nigérians qui se sont pris aux Guichets Automatiques Bancaires.

Les cyberattaques et les actes de cybercriminalité affectent au prime abord le domaine économique. La dernière édition du rapport Security Navigator d'Orange Cyberdéfense révèle une perte de 10% du PIB sur le continent africain. Ainsi, au niveau économique, l'impact des cyberattaques représente une perte énorme pour le PIB en Afrique. Ce rapport montre que le nombre d'extorsions affiche une augmentation de 70% en 2023. L'économie africaine est mise à rude épreuve par ces différentes attaques cybernétiques.

Dans un autre sens, les actes de cybercriminalité menacent la sécurité des données individuelles, la vie privée et les administrations publiques en Afrique (UA, 2014). La gestion des cyberattaques devient un défi important pour les entreprises et les administrations publiques. D'abord pour les entreprises en ce sens qu'elles doivent rassurer leurs clients et préserver leurs

intérêts. Ensuite pour les administrations publiques puisqu'elles ont l'obligation de créer pour les entreprises un cadre de sécurité et pour les citoyens, la protection et la sécurité. C'est pour relever ce défi que les entreprises investissent dans les outils informatiques plus sécurisés et les administrations publiques multiplient les lois qui régissent le cyberespace au niveau des États et à l'échelle continentale.

En Afrique comme ailleurs, certains contenus d'internet ou numériques sont produits et diffusés dans le but de recruter et de radicaliser les individus et de faire l'apologie du terrorisme. Ainsi, les technologies de l'information et de la communication assurent un rôle important dans la radicalisation. Les terroristes les utilisent

> à des fins de recrutement et de propagande, ainsi que pour la planification et l'exécution d'actes terroristes, comme les attaques ou des menaces d'attaque contre des ordinateurs, des réseaux informatiques ou autres systèmes d'information scientifique et technologique ; dans l'intention d'intimider, d'instiller la peur, ou de contraindre un gouvernement, une entreprise privée ou une frange de la population dans le seul but d'atteindre des objectifs politiques, idéologiques ou sociaux, que ce soit directement ou indirectement (CEDEAO, 2013).

L'espace numérique a un effet identitaire sur le plan individuel et collectif. On peut parler de fusion identitaire à travers les réseaux sociaux. C'est le processus par lequel l'identité de l'individu se fond dans celui du groupe radicalisé. L'individu adopte comme résultat de ce processus, le discours et le point de vue du groupe extrémiste. Ce « processus de fusion identitaire trouve une explication dans le fait que la coexistence dans l'univers numérique de pléthore d'identités virtuelles peut favoriser une rupture entre l'identité de l'individu et l'adoption d'une identité de groupe » (F. Lollia, 2021 : 5). On peut souligner aussi les situations de dépravations morales liées aux activités de sexes dans l'espace numérique en Afrique. Ces situations interpellent les acteurs notamment les responsables des entreprises et les autorités politiques et administratives.

2. La cybercriminalité et les difficultés de l'action techno-juridique en Afrique

Le domaine numérique met à rude épreuve les administrations et institutions africaines. La commission de l'Union Africaine reconnaît cette réalité et relève notamment que « les principaux défis au développement du commerce électronique en Afrique sont liés à des problèmes de sécurité » (UA, 2014 : 2). Au sujet du commerce électronique en Afrique, il faut noter d'abord les « lacunes » en matière de « reconnaissance juridique » des signatures électroniques. Ainsi, la communication des données électroniques souffre en Afrique du manque de reconnaissance juridique. Ensuite, il faut souligner « l'absence de règle juridiques spécifiques protectrices des consommateurs, des droits de propriété intellectuelle, des données

ISSN-L: 2958-2814
ISSN-P: 3006-306X

à caractère personnel et des systèmes d'information » (UA, 2014 : 2). Enfin le continent souffrait, dans le domaine fiscal et douanier, de l'absence de législations appropriées au commerce électronique.

La cybercriminalité replace les politiques contemporaines au cœur de leur premier rôle, à savoir, garantir la sécurité et la liberté des citoyens. En réalité, les philosophes du contrat social soulignaient à juste titre que le rôle de la politique est d'assurer la sécurité et la liberté des citoyens. Cette affirmation nous plonge au cœur de la pensée philosophique de T. Hobbes (2017). Pour lui, le premier rôle et la finalité de l'État est de protéger les citoyens tout en garantissant leur sécurité. Dans le même sens, J-J. Rousseau (2012) indiquait que la politique ne peut parvenir à assumer ce rôle fondamental que par la loi et non par la puissance d'un gouvernant autocratique ou d'un tyran. La loi se présente, selon J.-J. Rousseau, comme le moyen de protection et de garantie des libertés individuelles.

C'est pourquoi, les pays vont définir des cadres juridiques et politiques de protection et de garantie des libertés individuelles dans le contexte des cyberattaques et de la cybercriminalité. La loi devient, au regard des dispositions prises dans la plupart des pays, le cadre référentiel de régulation de l'usage des outils et systèmes informatiques en vue d'une solution efficace aux risques de cyberattaques et de cybercriminalité. L'objectif dans ces pays reste dans le sillage de ce que disait J.-J. Rousseau puisqu'il s'agit de réguler et de mettre en place le cadre juridique d'un usage libre et responsable des outils et systèmes informatiques et non d'interdire leur usage. Ceci montre qu'en réalité, la technologie informatique est ambivalente. Au même moment que cette technologie renforce l'efficacité des entreprises et des administrations et facilite les échanges économiques, elle rend vulnérable les sociétés contemporaines. C'est en évoquant cette ambivalence de la technologie contemporaine que H. Jonas affirme :

> Cette puissance que la technologie scientifique nous propose dans une direction qui, de prime abord, paraît toujours ou presque toujours, bienfaisante mais qui finit, lorsqu'on extrapole ses ordres de grandeurs croissants, par révéler ses aspects dangereux et parfois même catastrophiques (H. Jonas, 2000 : 134).

Cette affirmation montre à suffisance que la technologie à parait, au prime abord comme étant uniquement bienfaisante et sans conséquence négative. Mais lorsqu'on l'analyse de façon minutieuse, on saisit les dangers qui y sont liés.

Déjà en 1998, H. Jonas soulignait dans son livre *Pour une éthique du futur*, publié à titre posthume que la technologie nous apprend chaque que « le meilleur de la civilisation n'exclut pas la pire des barbaries » (H. Jonas, 1998 : 8). Cette idée n'est que le prolongement de la

ISSN-L: 2958-2814
ISSN-P: 3006-306X

dialectique de la raison évoquée par les principaux représentants de la première génération de l'École de Francfort. Selon M. Horkheimer et T. Adorno (1974), la raison humaine, dans son souci de délivrer l'humanité des forces de la nature, se transforme en raison instrumentale. Ainsi, au lieu de conduire à la félicité de l'homme et de la société, la raison se dédouble et devient raison instrumentale[2]. Tel est le sens de ce propos dénué de toute ambiguïté : « de tout temps, l'Aufklärung, au sens le plus large de pensée en progrès, a eu pour but de libérer les hommes de la peur et de les rendre souverains. Mais la terre, entièrement éclairée, resplendit sous le signe des calamités triomphant partout » (M. Horkheimer et T. Adorno, 1974). C'est ce double aspect de la raison dans ses divers déploiements qui se traduit dans l'ambivalence des outils informatiques.

Dans ce sens, le Togo s'est doté en 2018 d'une loi portant sur l'espace numérique. Il s'agit de la loi portant sur la cybersécurité et la lutte contre la cybercriminalité. Cette loi vise deux objectifs au moins. D'une part, cette loi régit le cadre de la cybersécurité au Togo. Elle vise dans ce sens à mettre « en place un dispositif permettant de prévenir et de faire face aux menaces et risques numériques tout en garantissant la promotion et le développement des technologies de l'information et de la communication » (Togo, 2018, art. 1, alinéa 1). D'autre part, cette loi vise « à assurer une protection pénale du système de valeurs de la société de l'information au Togo en mettant en place des mécanismes juridiques et institutionnels appropriés à la lutte contre la cybercriminalité » (Togo, 2018, art. 1, alinéa 2). La vision des autorités politiques togolaises est d'assurer à travers un cadre juridique et institutionnel de régulation de l'espace numérique au Togo, la sécurité des usagers des systèmes informatiques et de protéger les entreprises, les services publics et tous les citoyens. Le Togo va afficher cette volonté en créant l'Agence Nationale de la Cybersécurité (ANCy) et en adoptant, en 2022, une nouvelle loi qui modifie celle de 2018 précitée. La nouvelle loi met l'accent sur les opérateurs des systèmes informatiques.

En réalité, l'adoption de la loi sur la cybercriminalité par le Togo est une manière politique et juridique de contextualiser les décisions et dispositions de l'Union Africaine. En effet, déjà en 2014, l'organisation continentale a mis en place une convention sur la cybercriminalité et la protection des données à caractère personnel. Cette convention à l'échelle continentale a été adoptée la 23e session ordinaire de la conférence des Chefs d'État et de gouvernement de

[2] La raison instrumentale est la rationalité qu'on utilise pour évaluer les moyens les simples permettant d'atteindre une fin donnée et une efficacité maximale. Elle conduit, dans le domaine économique et social à l'exploitation de l'homme par l'homme.

l'Union Africaine à Malabo en Guinée Équatoriale le 27 Juin 2014. L'article 3 de cette convention définit la responsabilité des fournisseurs de biens et services par voie électronique lorsqu'il stipule que « L'activité de commerce électronique est soumise à la loi de l'État partie sur le territoire duquel la personne qui l'exerce est établie, sous réserve de la commune intention de cette personne et du destinataire des biens ou des services ».

Malgré, les actions juridiques et les investissements dans le renforcement des outils informatiques afin de lutter contre la cybercriminalité en Afrique, les résultats escomptés ne sont pas atteints. A. Yankey (2018) de la Commission de l'UEMOA, note trois raisons qui justifient l'écart entre les efforts juridiques, technologiques et les résultats obtenus. D'abord, il y a un faible niveau de sensibilisation à la cybersécurité en Afrique. Les petites entreprises et les usagers particuliers ne sont pas suffisamment informés sur la cybersécurité. De même, les financements dans la cybersécurité ne sont pas appropriés ni suffisants. Les petites et moyennes entreprises ont du mal à investir dans les outils informatiques plus sécurisés. Elles n'investissent pas dans la sécurisation de leurs systèmes informatiques alors même qu'elles sont de plus en plus touchées par les attaques cybernétiques. Ensuite, il y a un manque de volonté des gouvernements et de certaines entreprises privées à lutter contre la cybercriminalité. Enfin, on peut noter un manque de compétences en Afrique en cybersécurité. Cela signifie que dans les universités africaines, les jeunes qui sortent n'ont pas généralement de compétences adaptées pour faire face aux hackers dans leur volonté criminelle d'attaquer le cyberespace africain.

Ces éléments évoqués montrent à suffisance que les réponses juridiques et technologiques ont du mal à répondre efficacement au défi de la cybersécurité en Afrique. Il est question de repenser la technologie informatique ainsi que l'a souligné A. Feenberg (2004). Il faut, pour les rendre efficaces, insister sur la responsabilité collective. D'abord, celle des gouvernements, ensuite celle des entreprises et enfin la responsabilité des citoyens.

3. Responsabilité collective et renforcement de la cybersécurité en Afrique

La question de la cybersécurité est une question de portée mondiale et d'intérêt collectif au niveau international mais surtout national. Au niveau international en ce sens qu'une attaque cybernétique d'une entreprise ou d'une firme internationale peut perturber tout le commerce mondial et influencer négativement les bourses. Ainsi, la menace d'une cyberattaque dans un pays constitue de façon indirecte, voire même directe, une menace pour plusieurs pays du monde. La cybersécurité est une question d'intérêt national en ce sens que non seulement les chiffres d'affaires de tout le pays sont menacés mais aussi la sécurité nationale (puisqu'une attaque cybernétique peut ouvrir la porte à une attaque militaire), les informations classées

ISSN-L: 2958-2814
ISSN-P: 3006-306X

secrets d'État peuvent fuiter et rendre vulnérable la nation tout entière. De même, la cyberattaque constitue une menace permanente pour la vie privée des citoyens.

De ce fait, il faut analyser les stratégies de lutte contre la cybercriminalité au-delà de l'action politique et juridique. En effet et sans sous-estimer la capacité du cadre politico-juridique à lutter contre les menaces de cyberattaque, il faut noter qu'il ne s'agit là qu'une partie des actions à mener. C'est dire en réalité que l'action politico-juridique est nécessaire voire vitale dans cette lutte mais en même temps, elle est insuffisante. Le monde virtuel qui est le propre de la cybernétique et des cyberattaques met à l'épreuve le cadre juridique traditionnel des États. L'espace cybernétique étant virtuel, les lois et dispositions juridiques ont du mal à être efficaces dans la volonté de réprimer les actions des cybercriminels et de préserver la sécurité et la liberté. C'est pourquoi il faut inscrire les actions en faveur de la cybersécurité dans la logique d'une action collective. Pour y arriver, il faut comprendre et faire comprendre la cybersécurité et la cyberattaque comme relevant de la responsabilité collective. Elles engagent la responsabilité des politiques et des citoyens, ces derniers étant dans les associations de la société civile et dans les entreprises ou étant des ingénieurs informatiques ou simplement usagers des systèmes informatiques.

La réflexion sur la responsabilité face à la cybercriminalité permet ainsi d'entrevoir une stratégie de lutte contre les cyberattaques à savoir la responsabilité collective adaptée. Une responsabilité qui, comme l'affirme H. Jonas (1992), n'est pas une responsabilité théorique mais plutôt une responsabilité pratique qui appelle à l'action. Une stratégie d'adaptation intégrée inclurait donc des mesures qui prennent en compte les facteurs structurels qui déterminent la vulnérabilité des systèmes informatiques. Elle se baserait également sur les nombreuses stratégies locales de gestion des cyberattaques et les difficultés qui ont été enregistrées pour faire face aux menaces de cyberattaques.

La responsabilité collective adaptée devient ainsi une stratégie de prévention de la cybercriminalité. Elle se fonderait sur l'exploration et le partage des connaissances relatives aux processus de développement des nations à partir des nombreuses stratégies locales de gestion des attaques cybernétiques. Ces stratégies sont repérables dans différentes entreprises et nations. Une responsabilité collective adaptée est une méthode d'évaluation et de gestion des risques, dans un contexte de stress multiples tel que celui de la cybercriminalité, où l'adaptation s'intégrerait comme nouveau paramètre des stratégies de développement des systèmes informatiques, des politiques sectorielles et de gestion des systèmes informatiques. Le cadre théorique de l'adaptation intégrée, par la proximité qu'il instaure entre projet de développement

ISSN-L: 2958-2814
ISSN-P: 3006-306X

des systèmes informatiques et urgence sécuritaire locale, pourrait constituer un terrain propice de mise en œuvre de stratégies d'adaptation probablement plus opportun.

De ce fait, faire participer activement le public ou engager le public dans l'action managériale de la technologie informatique est devenu une nécessité. En 2008, A. Balmer et P. Martin, cités par B. Bensaude-Vincent (2009 : 154) dans un rapport, nous disent qu'il y a « (…) la nécessité non seulement d'informer la société civile sur ce qui est réalisé, mais aussi de faire la démonstration des avantages sociaux potentiels ». L'engagement du public dans la sphère de la technologie doit, eu égard de la puissance des systèmes informatiques, dépasser l'étape d'une simple information et entrer dans le stade d'une participation active du public en amont. Ceci étant dit, il s'agit de mettre en place des structures légitimes capables de mettre les choix des systèmes informatiques « en démocratie ». Cette attitude de gestion de la technologie informatique et de tout le projet technoscientifique requiert un processus de consultation, de dialogue et d'information aboutissant à l'identification des « enjeux avec les citoyens ».

L'engagement du public dans la gestion de la régulation de la technologie informatique n'est pas chose aisée. Les voix plaidant pour la participation du public dans la régulation de la technologie informatique risquent de rester dans le discours sans avoir de résultat concret. Pour rendre effective la participation du public aux décisions portant sur les technologies informatiques, il faut que les organisations de la société civile se mobilisent pour faire entendre leurs préoccupations. Ainsi, sans attendre l'organisation des consultations citoyennes, les associations doivent se mobiliser pour imposer le débat public sur les décisions touchant les projets informatiques. Nul ne saurait sous-estimer le poids et la puissance des actions des associations des consommateurs et des citoyens. R. Carson a, par exemple, contribué à lancer le mouvement écologiste dans les sociétés occidentales dans les années soixante à travers la publication de son livre *Le printemps silencieux* (1962) sur le scandale des pesticides. En réalité, à la suite de la publication de son ouvrage, toute une suite de mouvement contestataire a suivi en Amérique avant de s'étendre en Europe et dans le monde entier. Cet ouvrage, à la fois descriptif et prescriptif, a eu une influence sur certaine politique de « recherche-développement » que personne ne peut ignorer. Dans cette logique, les citoyens et leurs associations doivent prendre en main des initiatives pour imposer leurs interventions et les actions décisives sur les décisions dans le domaine de la régulation de l'espace informatique.

Ainsi, l'engagement des citoyens par les pouvoirs publics dans la sphère des décisions portant sur les systèmes informatiques se nourrit de la pression qu'exerce sur eux, la « solidarité citoyenne ». En effet, étant dans une société qui est le lieu des intérêts en compétitions et dans

ISSN-L: 2958-2814
ISSN-P: 3006-306X

un monde contemporain dominé par les intérêts, les seuls acteurs résolus et capables de porter la régulation de la technologie informatique sans frontière, « (…) avec pour seul justificatif, l'humanité elle-même, sont les organisations de la société civile. Elles semblent, à travers les initiatives et les actions en réseaux par lesquelles elles s'illustrent, incarner plus sérieusement l'idéal » (Y. Akakpo, 2016 : 156) de réappropriation, de réorientation humaine et de régulation de la technologie informatique. On le sait, les organisations de la société civile sont capable d'histoire et elles en donnent la preuve à travers leur capacité à dénoncer efficacement des dérives « totalitaires » de certaines lois mais aussi de certaines politiques nationales et internationales, à secouer et à faire chuter des régimes reconnus pour forts, et surtout à défendre valablement l'environnement, les travailleurs et les consommateurs. Ainsi, les organisations citoyennes et les réseaux sociaux ont un immense pouvoir que nul ne saurait sous-estimer.

Comptant sur leur immense pouvoir et leur capacité à faire l'histoire, les organisations citoyennes sont tenues de mettre la pression sur les pouvoirs publics afin que ceux-ci œuvrent pour une participation citoyenne aux décisions concernant les systèmes informatiques. Il est temps pour que les dirigeants politiques, les chefs d'entreprises et les acteurs économiques ne décident plus seuls de ce qui convient aux citoyens en matière de systèmes informatiques. On l'a noté plus haut, les pouvoirs publics ne sont pas des systèmes neutres, ils peuvent (et ils le font) céder aux pressions des acteurs économiques. De même, il est connu aujourd'hui qu'au nom du « délice technique », les scientifiques et les techniciens peuvent sacrifier les intérêts de l'humanité et de toute la collectivité des humains. L'alternative est désormais du côté des organisations de la société civile. C'est aux organisations citoyennes d'imposer l'ouverture au public, des débats portant sur les choix de développement technologique. Il faut, de ce fait, envisager la pratique de l'activité scientifique et technique dans le registre des choix de société, c'est-à-dire comme « de véritables choix de société ».

Il s'agira, pour les pouvoirs publics, de sensibiliser les citoyens sur les risques liés aux systèmes informatiques, de les amener à s'approprier le contenu des dispositions juridiques sur l'espace cybernétique. Ceci permettra aux citoyens de prendre conscience de leurs droits et devoirs dans le domaine informatique et de se rendre à l'évidence de leur responsabilité dans l'instauration d'une cybersécurité au plan national et international. Ainsi, en sensibilisant les citoyens associés aux actions politico-juridiques éclairées, on peut lutter efficacement contre la cybercriminalité et instaurer ainsi la cybersécurité tant au niveau national, régional qu'international.

Aussi, les pouvoirs publics et les grandes entreprises doivent investir dans la formation. Ainsi, il faut créer des instituts de recherche en cybersécurité, réorganiser les laboratoires et centres

ISSN-L: 2958-2814
ISSN-P: 3006-306X

universitaires existants dans les universités afin d'offrir aux citoyens et aux ressources humaines des entreprises des formations appropriées en cybersécurité. Dans ce sens, les universités doivent se restructurer afin d'aider les pouvoirs publics à relever les défis de l'heure, notamment dans le domaine de la cybersécurité. Il faut inscrire la formation de base en systèmes informatiques dans plupart des filières de formations professionnelles afin que chaque professionnel puisse avoir la capacité de détecter les menaces de cyberattaques les plus élémentaires et de déclencher les systèmes d'alarmes.

Enfin, il faut insérer ou renforcer l'enseignement de l'éthique dans les formations universitaires et professionnelles. En réalité, les dirigeants des entreprises de demain se trouvent dans les universités et centres de formations actuels. C'est pourquoi il faut les former aux valeurs éthiques et à la responsabilité éthique. Ainsi, « les nouvelles pratiques numériques des jeunes d'Abidjan, de Lagos, de Ouagadougou, de Lomé, de Cotonou, de Dakar, de Bamako, etc. appellent, au-delà de la répression juridique, un accompagnement éthique, éducationnel d'envergure et un enracinement culturel » (T. Karamoko, 2015 : 15). Il s'agit, de façon pratique, d'enseigner aux jeunes les valeurs éthiques telles que la probité, le refus du gain facile, le respect de l'autre et de ses biens, le patriotisme. En éduquant à ces valeurs les jeunes qui sont d'une part des usagers du NET et d'autre part des responsables politiques ou d'entreprises de demain, l'Afrique peut se donner la chance de gagner le combat contre la cybercriminalité. Ces valeurs éthiques sont des outils efficaces de lutte contre le terrorisme et le système de recrutement des agents terroristes à travers le NET. De même, les scènes de dépravations morales qui pullulent sur l'espace numérique en Afrique peuvent être contrées à partir des valeurs comme la probité et l'éthique du corps et de la dignité de la personne humaine.

Conclusion

En définitive, la cybercriminalité est devenue un fait social qui met en difficulté particulièrement les pays Africains. Protéger les entreprises, les administrations et les citoyens face aux menaces des hackers devient un défi supplémentaire pour les gouvernements. Ces derniers s'appuient sur le cadre juridique et institutionnel pour relever ce défi et invitent souvent les entreprises à investir dans l'amélioration des outils informatiques en place. Ce faisant, ils font des réponses juridiques et technologiques, les seuls moyens de résolution des problèmes liés à la cybercriminalité. Mais la croissance des attaques cybernétiques en Afrique en dépit de ces réponses montre que laisser à elles seules, les réponses juridiques et technologiques sont limitées. C'est pourquoi cet article a insisté sur l'importance de la responsabilité collective. Il a montré que la responsabilité collective peut dynamiser les réponses juridiques et

ISSN-L: 2958-2814
ISSN-P: 3006-306X

technologiques. Ce texte abouti à trois résultats au moins. D'abord, il aboutit au fait qu'il faut développer une responsabilité politique. Les gouvernements doivent assumer convenablement leur responsabilité en assurant la sécurité des citoyens et des entreprises. Ils doivent, par exemple, revoir les offres de formations afin de renforcer les compétences en cybersécurité. Ensuite, cet article indique la nécessité de la responsabilité des entreprises. Elles doivent assumer leur responsabilité en protégeant leurs clients et en investissant convenablement dans les outils informatiques appropriés. Puisqu'on note, par manque de responsabilité comprise et assumée, un faible niveau d'investissement par les entreprises dans les outils de sécurité informatiques. Enfin, cet article indique la responsabilité des citoyens, des chercheurs, des organisations de la société civile dans la lutte contre la cybercriminalité en Afrique.

Références bibliographiques

AKAKPO Yaovi, 2016, *Science et reconnaissance*, Paris, Présence Africaine, 169p.

ARPAGIAN Nicolas, 2015, *La cybersécurité*, Paris, PUF, 127p.

BECK Ulrick., 2003, « La société du risque globalisé revue sous l'angle de la menace terroriste », *Cahiers internationaux de sociologie*, (1), p. 27-33. DOI : 10.3917/cis.114.0027

BECK Ulrick, 2008, *La société du risque : sur la voie d'une autre modernité*, Paris, Flammarion, 528p.

BENSAUDE-VINCENT Bernadette, 2009, *Les vertiges de la technoscience*, Paris, La Découverte, 228p.

CARSON Rachel, 1962, *Printemps silencieux*, Paris, Seuil, 287p.

FEENBERG Andrew, 2004, *Repenser la technologie. Vers une technologie démocratique*, Paris, La Découverte, 244p.

HOBBES Thomas, 2017 [1651], *Léviathan*, Trad. François Tricaud, Paris, Flammarion, 240p.

HORKHEIMER Max et ADORNO Théodore, 1974, *Dialectique de la raison*, Paris, Gallimard, 294p.

JONAS Hans, 1990, *Le principe responsabilité*, Paris, Cerf, 480p.

JONAS Hans, 1998, *Pour une éthique du futur*, Paris, Payot, 128p.

JONAS Hans, 2000, *Évolution et liberté*, Paris, Rivages, 272p.

KARAMOKO Tiéba, 2015, « La société digitale et les racines de la cybercriminalité », in *Perspectives Philosophiques*, n°009, Abidjan, p. 1-19.

KIE Franck, 2020, « Pourquoi les banques devraient s'inquiéter de la cybercriminalité », *Financial Afrik*, https://www.financialafrik.com/2020/03/17/la-tribune-de-franck-kie-pourquoi-les-banques-devraient-sinquieter-de-la-cybercriminalite/.

LOLLIA Fabrice, 2021, *Terrorisme, internet et réseaux sociaux*, https://shs.hal.science/halshs-03172818.

ROUSSEAU Jean-Jacques, 2012 [1762], *Du contrat social*, Paris, Flammarion, 256p.

SALOMON Jean-Jacques, 1970, *Science et Politique*, Paris, Seuil, 408p.

VENTRE Daniel et LOISEAU Hugo (dir.), 2023, *Évolutions du cybercrime durant la pandémie de Covid-19*, Great Britain, ISTE Editions, 242p.

YANKEY Auguste, 2018, *Relever les défis juridiques de la cybersécurité en Afrique*, Commission de l'Union Africaine, 15p.

Africa Cybersecurity Magazine, 2020. https://cybersecuritymag.africa/cyberattaques-afrique-2020.

CEDEAO, 2013, *Déclaration politique et la position commune en matière de lutte contre le terrorisme*, Yamoussoukro.

DELOITTE, 2021, *Rapport de 2021*, www.deloitte.com/about.

Jeune Afrique, 2023, « Pourquoi l'Afrique est vulnérable aux cyberattaques : cinq questions pour comprendre un fléau économique », https://www.jeuneafrique.com/1457969/economie-entreprises/cyberattaques-cinq-questions-pour-comprendre-lafrique-est-vulnerable.

KASPERSKY LAB, 2020, *Rapport des activités 2020*, www.kaspersky.com

KASPERSKY LAB, 2023, *Rapport des activités 2023*, www.*kaspersky.com*

TOGO, 2018, *Loi n°2018-026 sur la cybersécurité et la lutte contre la cybercriminalité*, 23p.

TOGO, 2022, *Arrêté n°2022-040 portant adoption des règles de cybersécurité en république togolaise*, 48p.

UNION AFRICAINE, 2014, *Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel*, Malabo, 40p.