Revue africaine des Humanités

Revue Pluridisciplinaire du Département de Sociologie

ISSN : 2756-7680

03 BP 7021 Ouagadougou 03 (Burkina Faso)
Université Joseph KI-ZERBO

Volume 1 N^0 002 - Juillet 2025

Administration

Contacts

03 BP 7021 Ouagadougou 03 (BurkinaFaso)
Email : rah@ujkz.bf
Tél. : (+226) 70 21 27 18/78840523

Éditeur

Presses Universitaires de Ouagadougou
03 BP 7021 Ouagadougou 03 (Burkina Faso)

Volume 1 N^0 002 - Juillet 2025

Comité scientifique

Comité de lecture

Sommaire

Les nouvelles formes de délinquance virtuelle : la territorialité face à la cybercriminalité

Maixent Cyr ITOUA ONDET
Enseignant à l'Université Marien N'Gouabi
Brazzaville – Congo
itouaondet@gmail.com

Stéphane ALVAREZ
Enseignant à l'Université de Grenoble, France
stephane.alvarez@umpf-grenoble.fr

Résumé

Cet article traite de la cybercriminalité. Il explique que le développement des réseaux de communication et la généralisation d'internet ont conduit à l'accroissement de la cybercriminalité. Cependant, les métaphores économiques et sociales constituent de véritables formes de la délinquance en général et la cybercriminalité en particulier. Ainsi, c'est la raison pour laquelle la lutte contre la cybercriminalité fait l'objet d'un développement normatif dense. Toutefois, la norme de nature répressive, même très développée, recouvre une certaine relative quant à son efficacité. À ce titre, les frontières traditionnelles ne s'appliquent pas toujours efficacement dans le monde virtuel des cybercrimes.

Mots-clés : cybercriminalité, coopération, délinquance, norme, territorialité.

Abstract

This article deals with the issue of cybercrime. The development of communication networks and the widespread use of the internet have led to an increase in cybercrime. Economic and social metaphors constitute real forms of delinquency in general and cybercrime in particular. This is the reason why the fight against cybercrime has been the subject of intensive of intense normative development. However, the norm of a repressive nature, even it very developed, has a certain reality regarding its effectiveness. Indeed, traditional physical boundaries do not always apply effectively in the virtual world of cybercrimes.

Keywords : cybercrime, cooperation, delinquency, standard, territoriality.

Introduction

Depuis l'avènement des nouvelles technologies de l'information et de la communication, le monde se trouve centralisé dans les enjeux de l'espace virtuel porteur des progrès conséquents indéniables pour l'existence de l'homme avec l'internet. Malheureusement, toute invention humaine peut être aussi génératrice de comportements

illicites. En effet, le côté élogieux d'internet occulte sa face la plus redoutable ; et parmi les menaces liées à cet outil, une se distingue par sa dangerosité et sa complexité sur le terrain étatique : la cybercriminalité. Celle-ci est l'une des nouvelles formes de criminalité ou de délinquance sur le réseau internet. Le phénomène cybercriminel ne se résume donc plus à des actes isolés, anecdotiques ou spectaculaires. Il est désormais considéré comme un risque séculaire majeur par la plupart des experts dont les conséquences s'avèrent particulièrement graves pour la sécurité planétaire en général et étatique en particulier.

Par ailleurs, la cybercriminalité pose aussi des défis complexes et freine l'innovation technologique, tout en exigeant des investissements accrus en cybersécurité. De plus, elle peut avoir des impacts psychologiques sur les victimes et alimenter la désinformation dans la société. Le problème majeur réside dans le fait que la cybercriminalité n'a pas de frontières définies. Les cybercriminels se déplacent dans le cyberespace.

C'est pour cela que le choix de cet article est motivé par les effets relatifs de la cybercriminalité et les difficultés éprouvées pour localiser les cybercriminels dans un territoire donné afin d'appliquer les sanctions requises sinon les adapter aux faits des incriminés. C'est d'ailleurs ce que ROSE C (2006) qualifie de *« la troisième grande menace au monde après les armes chimiques, bactériologiques et nucléaires »*. Ainsi, cette réflexion consacrée à la cybercriminalité est d'une actualité indéniable et sans cesse renouvelée. En effet, au regard du développement des nouvelles formes de délinquances, notamment dans le cyberespace, cet article présente naturellement un intérêt théorique et pratique.

Au plan théorique, la territorialité en matière de cybercriminalité soulève des questions complexes concernant la compétence des autorités, en raison des différences entre les politiques nationales et les divergences d'opinion sur la manière de concilier la souveraineté des États avec la nécessité de trouver des solutions efficaces, afin de poursuivre les criminels, tout en respectant les principes de souveraineté nationale et en favorisant la coopération internationale.

De même, du point de vue pratique, en raison de ses implications sur la sécurité des individus, la protection des données personnelles et la confiance dans l'environnement numérique. Dans cette optique, apparaît l'intérêt pratique aux rapports de la coopération internationale, la nature transnationale de la cybercriminalité nécessite une coopération étroite entre les pays pour enquêter sur les crimes, poursuivre des criminels et le partage d'informations, la coordination des enquêtes, le développement des normes et de protocoles communs, la formation et le renforcement des capacités, en partenariat-public-privé.

Face à l'émergence de la cybercriminalité et à la remise en question des frontières physiques dans le cyberespace ; dans quelles mesures la notion de la territorialité s'applique-t-elle à la répression de la délinquance virtuelle, et quelles sont les implications de cette application ?

Il ressort que, l'arsenal législatif congolais en la matière est abondant, mais le manque des moyens d'accompagnement et la lenteur dans la mise en œuvre par les pouvoirs publics de ces réformes contribue à l'inertie de l'activité des décideurs. De même, l'établissement des preuves et même des poursuites en matière de cybercriminalité

demeurent un exercice difficile pour les États en raison de la prééminence de leur souveraineté.

La méthode utilisée ici s'est consacrée à l'étude documentaire et textuelle. Celle-ci a été complétée par les enquêtes de terrain. L'analyse des textes, ont permis de mettre un relief l'applicabilité des textes internationaux en ce domaine. Cependant, pour ce qui est de la recherche documentaire, les rayons des bibliothèques sont beaucoup plus riches dans d'autres matières que celle de cette recherche ; laquelle s'est enrichie grâce à l'outil informatique, internet notamment, qui a permis d'accéder à certains travaux. Enfin, quant aux enquêtes de terrain, nous nous sommes orientés vers les services techniques des administrations publiques et privées qui gèrent les communications électroniques, à l'instar de la Cellule de recherche et d'analyse criminelle chargée de faciliter les actions criminelles (CRAC) et Mobile Téléphonie Networks (MTN), opérateur de téléphonie mobile en Afrique, notamment au Congo. « *La méthode accompagne la théorie et les faits émergent que lorsqu'ils sont sollicités par un questionnement. »* (ITOUA ONDET, 2019, p. 136).

Le début du XXIe siècle a fait prendre conscience aux nombreux États du danger que pouvait représenter le développement d'internet, même s'ils étaient loin d'imaginer toutes les possibilités que cela pouvait laisser transparaître. Ainsi, dès 2001, ils ont été beaucoup à adopter la Convention du Conseil de l'Europe sur la cybercriminalité, plus connue sous le nom de « Convention de Budapest », premier accord international de l'histoire visant à lutter contre les activités criminelles en ligne. Dans la foulée, l'Union européenne n'a cessé de réglementer la cyberespace en coordination avec d'autres pays externes afin d'en limiter les menaces. C'est alors qu'une première directive de sécurité des réseaux et des systèmes d'information (SRI) a été adoptée en 2016, et conformément à la clause de révision, celle-ci a été révisée pour laisser place à SRI 2 en 2022. Cette nouvelle directive promeut des objectifs de coopération renforcée entre les États membres, met l'accent sur l'anticipation et la sensibilisation à la cybersécurité et élargit le champ d'application matériel.

Cependant, l'histoire de la cybercriminalité en Afrique remonte à l'initiative de l'élaboration des textes encadrant la répression de la cybercriminalité clairement exprimée lors de la Conférence extraordinaire de l'Union Africaine des Ministres en charge de la Communication et des Technologies de l'Information à Johannesburg, le 5 novembre 2009.

C'est dire que cette volonté de lutter contre la cybercriminalité a évolué grâce aux déclarations telles que : la Déclaration d'Abidjan du 22 février 2012, la Déclaration d'Addis-Abeba du 22 juin 2012 adoptant le projet de loi sur l'harmonisation des cyber-législations en Afrique et la déclaration de Khartoum du 6 septembre 2012. Ainsi, l'Union Africaine (UA) a cherché à encourager une approche continentale pour lutter contre la cybercriminalité par le biais de Convention sur la cybersécurité et la protection des données à caractère personnel connue sous le nom de Convention de Malabo. En raison de la nature transfrontalière et internationale de la cybercriminalité, l'UA soutient que *« la nature de législation nationale ne peut être rédigée de manière isolée et les gouvernements nationaux doivent chercher à harmoniser les législations, les réglementations, les normes et les directives nationales sur les questions de cybersécurité* » (ALIEN, 2019, p. 12).

En effet, les nouveaux défis auxquels, les États sont confrontés, de même que les difficultés qu'ils doivent surmonter pour les relever sont réels. Les réseaux numériques démultiplient le nombre d'infractions et les délinquants se jouent souvent des frontières en commettant leurs délits dans des pays où la législation est inexistante ou embryonnaire. En revanche, l'une des difficultés pour la lutte contre la cybercriminalité est que cette forme de délinquance mondiale défie les règles classiques de compétences législatives fondées en grande partie sur la souveraineté des États.

Face à la cybercriminalité, les États ont de tout temps inscrit leur compétence pénale dans une logique territoriale qui permet en effet de faire correspondre une criminalité à un espace donné, délimité et sur lequel s'exerce une souveraineté nationale. Or, cette fonction est, à l'époque de cyberespace, de plus en plus bousculée. D'autant plus que la cybercriminalité est souvent considérée comme un nouveau domaine, même si bon nombre de textes existants ont vocation à s'appliquer à la matière numérique. En effet, le droit de l'internet n'est pas une nouvelle branche, mais les États ont dû l'adapter en raison des particularités nouvelles qu'il a générées et de ses acteurs diversifiés afin de sanctionner les dérives qu'il induit (Charbonnier, 1972, p, 42). Ce principe constitue une des traductions du pouvoir de souveraineté nationale des Etats sur leur territoire respectif. Toutefois, en raison de l'internationalisation croissante de la délinquance, il est de plus en plus fréquent que des infractions comportent des éléments d'extranéité.

1. La territorialité dans le cadre des infractions cybercriminelles

La territorialité donne compétence à un État dès lors qu'une infraction est commise sur son territoire, et ce quelle que soit la nationalité des auteurs ou des victimes. Lorsqu'on s'attaque à la cybercriminalité, on distingue généralement deux types de crime. D'une part, les crimes particuliers faisant intervenir des ordinateurs et des réseaux ; encore appelés infractions directement liées aux nouvelles technologies d'information et de communication dans lesquelles l'informatique est l'objet du délit ; d'autre part, il y a les infractions dont la commission est liée ou facilitée par les nouvelles technologies de l'information et de la communication et sur lesquelles l'informatique n'est qu'un moyen.

Cependant, les nouvelles technologies de l'information et de communication occupent actuellement une place importante dans les entreprises, quels que soient la taille ou les domaines d'activité de ces dernières. Elles participent positivement au développement de l'économie. Par ailleurs, elles sont à l'origine d'une nouvelle criminalité qui menace la sécurité et l'intégrité des systèmes informatiques dans l'entreprise. En effet, l'explosion du nombre des cybercrimes a contraint le Congo à adopter une véritable politique de défense afin de protéger ses systèmes d'information. En ce sens, que toute action frauduleuse est réprimée, mais aussi les atteintes à l'intégrité des données d'un système d'information de la part de celui qui est entré illégalement, ou de la part de celui qui, ayant régulièrement pénétré, pose des actes dommageables. C'est dans ce sens que la Loi française considère le fait d'accéder à un réseau de cartes France Télécoms où un individu avait utilisé des numéros d'une carte appartenant à autrui afin d'obtenir des services de

télécommunication, comme un fait qui tombe sous l'accès illicite aux systèmes.
Ainsi, l'introduction frauduleuse dans un système informatique est punie d'un an au moins à cinq ans au plus d'emprisonnements et de cinq millions soit (5 000 000) à dix millions (10 000 000) de francs CFA d'amende ou de l'une de ces peines seulement. Il en est de même, lorsqu'il résulte soit de l'effacement ou de modifier des données contenues dans le système informatique, la peine est d'un an au moins ou cinq ans au plus d'emprisonnements et de cinq millions (5 000 000) et à dix millions (10 000 000) de francs CFA d'amende ou de l'une de ces deux peines. Enfin, les infractions liées aux NTIC sont établies afin de se prévenir contre d'éventuelles atteintes des systèmes d'information. Toutefois, les infractions relevant directement des NTIC se caractérisent aussi par des violations dangereuses des données confidentielles.

1.1. **Les atteintes à la confidentialité des données**

L'évolution vertigineuse des technologies de l'information et de la communication a engendré une augmentation significative des crimes en ligne à l'échelle mondiale. Au fur et à mesure de leur développement, les différentes infractions liées aux NTIC présentent cependant de nouveaux risques touchant aux données personnelles. En effet, les données personnelles correspondent à des informations individuelles sur des situations personnelles ou factuelles d'une personne physique définie ou reconnaissable. Par exemple : le nom, l'adresse, le numéro de compte, de pièce d'identité ou de téléphone, l'immatriculation, l'adresse électronique ou encore l'adresse IP sont des données personnelles. En revanche, les données ne permettent pas l'identification de la personne ne sont pas des données personnelles. Cependant, les violations aux données à caractère personnel peuvent prendre diverses formes, notamment la violation de données personnelles ; des données commerciales ; de la confidentialité médicale ; de la confidentialité en ligne ; les atteintes à la confidentialité des communications. Ainsi, la fraude est l'une des plus anciennes formes d'attaques contre l'intégrité des données. Parmi celles-ci, on peut toutefois citer l'attaque qui s'est produite en 2008 et qui a fait la première page de l'actualité mondiale. Il s'agissait là d'un abus de confiance combinée à l'utilisation non autorisée et la falsification des systèmes informatiques de la banque Société Générale par un trader qui travaillait au sein même de l'organisation en France. Cette attaque a entraîné des pertes de 4,9 milliards d'euros. Par ailleurs, la délinquance est ici, en relation indirecte avec un réseau de télécommunication, c'est-à-dire que cet outil se comprend comme un moyen pour commettre l'infraction (Bourdieu, 1986, p.69). C'est pour cela, le devoir de protection des citoyens, des entreprises et des administrations publiques demeure primordial pour les États.
C'est dire que la démocratisation de l'accès à l'informatique et la globalisation des réseaux ont été des facteurs de développement des crimes en ligne. Le cybercrime est donc toute infraction commise par l'entremise d'un système informatique ou d'internet. C'est dans ce sens que déclare LEMAN-LANGLOIS (1996), *ce sont en fait des crimes relativement conventionnels dont les auteurs ont adopté des outils modernes pour arriver à leurs fins.* La cybercriminalité n'est ici qu'un moyen de commission des faits classiques. On peut s'approprier

une infinité de biens physiques, de valeurs symboliques et d'informations confidentielles dans le monde tangible, et l'idée de le commettre avec une technologie procurant de nouveaux outils et de nouvelles cibles n'est particulièrement difficile à formuler ni à mettre en pratique.
Ces crimes classiques en ligne se catégorisent par la cybercriminalité individuelle, la cybercriminalité contre la propriété et la cybercriminalité gouvernementale. En effet, les méthodes utilisées et les niveaux de difficulté varient selon leurs catégories. En premier lieu, la criminalité contre la propriété qui est un cas réel ou un criminel possède illégalement les coordonnées bancaires ou de carte de crédit d'une personne. En second lieu, la cybercriminalité individuelle qui est une catégorie de cybercriminalité impliquant une personne qui distribue des informations malveillantes ou illégales en ligne. Enfin, la cybercriminalité gouvernementale, la moins répandue, mais c'est la délinquance la plus grave.

1.1.1. **Le rapprochement territorial**

Malgré la complexité de la délimitation territoriale dans le cyberespace, les critères de rattachement territoriaux sont nécessaires pour permettre la répression de la cybercriminalité.
Ainsi, les États adoptent les lois visant à étendre leur compétence territoriale pour englober les actes commis sur leur territoire, mais également ceux qui ont des répercussions sur leur territoire, même s'ils sont commis à l'étranger. Cette extension de la compétence territoriale est illustrée par la loi française qui réprime les actes de cybercriminalité commis à l'étranger, mais ayant des répercussions en France.
Sur le plan interne, les critères de rattachement en la matière : territorial, personnel ; réel, universel, confrontés à l'universalité de l'internet, sont naturellement applicables aux cybercrimes et aux cyberdélits.
Enfin, le rapprochement territorial à la répression de la cybercriminalité se concentre sur la façon dont les États collaborent et coordonnent leurs efforts pour lutter contre les crimes commis via les technologies numériques qui transcendent les frontières nationales. Le caractère mondial d'internet et des cybercrimes pose des défis uniques, nécessitant un rapprochement, une approche coordonnée et coopérative entre les Etats en matière de juridiction.

2. Les limites de la territorialité dans la répression de la cybercriminalité.

L'une des caractéristiques fondamentales de la délinquance numérique est sa nature transnationale. Cette dernière se manifeste par les faits automatisés et à une échelle sans précédent de délinquants et de victimes qui résident respectivement à des milliers de kilomètres les uns les autres. Par contraste avec cette capacité d'innovation criminelle exploitant au même rythme que les startups de la *Silicon Valley,* les NTIC, les Etats semblent avoir beaucoup plus de difficultés à s'adapter aux changements induits par un environnement numérique en constante mutation.
En effet, la cybercriminalité transcende les frontières nationales, ce qui remet en question l'efficacité des règles traditionnelles de territorialité.

Cependant, les activités criminelles sur internet peuvent être perpétrées à partir d'un territoire donné, mais avoir des répercussions mondiales (PEREIRA, 2016). Ainsi, l'application des normes est rendue ici, difficile dans la lutte contre la cybercriminalité en raison du caractère transnational des cybercrimes qui rend leur répression complexe d'une part, et la nécessité d'une coopération étroite entre les Etats d'autre part.

2.2. La complexité de la nature de la cybercriminalité

La norme juridique est d'inspiration sociale (Bourdieu 1980), elle vient répondre à une nécessité bien précise. Les changements que subit une société font qu'aucune société n'est figée (Balandier, 1970) ; et une constante mise à jour est cruciale au maintien de l'ordre et du bon fonctionnement des institutions. Les bouleversements technologiques font partie des moteurs de changements abolissant toute notion de frontières ; internet a beaucoup influencé le paysage juridique du XXIe siècle, démontrant l'incapacité des normes existantes à déterminer la compétence territoriale en matière de cybercriminalité.

En effet, la particularité de la criminalité commise sur les réseaux sociaux numériques est qu'elle a pour cible un territoire quasi sans limite puisque là où internet est accessible, la criminalité l'est également. De ce fait naît une réalité bien sombre, à savoir que les cyberdélinquants ont la possibilité de commettre les attaques dans un pays où les normes juridictionnelles semblent encore inexistantes ou beaucoup plus souples. Cependant, les difficultés liées à l'application des normes sont au fait, la localisation des infractions recouvre une importante capitale quant à l'identification des cyberdélinquants. Néanmoins, traiter de la localisation des cyber infractions revient à concilier le caractère délimité de la règle au niveau de l'espace et le caractère universel des réseaux numériques. Car, ces derniers offrent l'ubiquité et l'immédiateté des échanges d'informations.

Par ailleurs, le caractère protéiforme de la cybercriminalité a une particularité, la façon d'opérer qui utilise ou cible un système d'information et qui peut prendre des proportions différentes selon des pays par rapport aux actes commis. Cependant, le caractère protéique se traduit souvent par la difficulté de définir un territoire. Celle-ci s'explique par la facilité que la technologie offre dans la commission des actes de délinquance. Un simple clic informatique suffit pour passer à l'acte ou atteindre à distance la victime potentielle, même si la mise en scène et la technique utilisées sont souvent très peu élaborées. Seulement de nos, ces derniers tendent à être maîtrisés de plus en plus grâce à la démocratisation d'internet et l'accessibilité des supports informatiques. Ainsi, une personne avec un niveau intellectuel limité peut utiliser les nouvelles technologiques, car celles-ci sont conçues pour viser le plus grand nombre de consommateurs. Toutefois, la forme multidimensionnelle de la cybercriminalité sur le territoire donné peut présenter certaines difficultés. Cela pose la question de la compétence des États à réprimer des actes, notamment, lorsque les infractions commises en ligne ont des conséquences dans plusieurs juridictions.

À ce titre, la loi pénale française est applicable aux infractions commises ou réputées commises sur le territoire de la République française. Il en est de même des autres Etats, la tendance consistant à étendre le critère de compétence de territorialité pour sanctionner les

crimes localisés même partiellement sur un territoire. Il s'ensuit que, le répressif demeure une expression territorialisée de la souveraineté des États. Dans ce contexte, la jurisprudence a abordé la question de l'extraterritorialité des cybercrimes. Par exemple, l'arrêt de la cour internationale de Justice dans l'affaire Lotus en 1927 a établi le principe de la territorialité objective, selon lequel un Etat ne peut exercer sa souveraineté que sur son propre territoire sauf en cas de règles contraires. Cet arrêt a posé les fondements de la limitation de la compétence des États en matière d'extraterritorialité, ce qui complique la répression des cybercrimes à l'échelle internationale.

Les infractions commises dans le cyberespace sont réprimées par les normes nationales territorialement compétentes. Néanmoins, même étendue, l'applicabilité du principe de territorialité souffre de certaines limites face à l'universalité d'internet. Ces limites tiennent moins à ''un inquiétant vide judiciaire en raison du caractère insaisissable des flux transfrontaliers''.

En outre, on observe la multiplicité des actes cybercriminels et que l'expression du principe de territorialité diffère selon les infractions. En réalité, tous les États du monde sont susceptibles de se déclarer compétents à travers l'application du principe de territorialité, ce qui conduit à des conflits de compétences. De même, la technologie démultiplie les effets de la criminalité, en permettant simultanément, d'attaquer de nombreuses cibles et en bénéficiant de la rapidité de propagation que permet l'outil informatique quel que soit son support, que ce soit un ordinateur, une tablette ou encore un téléphone. L'on ajoute à cela l'impunité dont bénéficie son auteur, qui jouit le plus souvent d'un anonymat fortement protégé, et de l'extranéité qui résulte de la localisation des serveurs et du lieu de stockage des données des principaux prestataires d'internet.

Enfin, ces difficultés tiennent au fait que les règles de compétence ne prennent pas en compte, en tout cas pas suffisamment, l'universalité d'internet. Il en résulte de fâcheuses incohérences et une réelle insécurité juridique. Les incohérences concernent l'articulation entre les différents critères de compétence. Alors qu'il a longtemps été prétendu, à tort, que le Web a créé un inquiétant vide juridique en raison du caractère insaisissable des flux transfrontaliers d'information, c'est plutôt d'un encombrant trop plein qu'il s'agit désormais, du fait précisément de l'ubiquité dans le cadre du *'' cloud computing''.*

Conclusion

L'étude de la délinquance virtuelle qu'est la cybercriminalité a permis de relever que celle-ci est la commission des cybercrimes, et alternativement le fait d'un individu isolé ou d'une bande organisée. Ce qui fait intervenir des acteurs à des niveaux différents.

Cela dit, il convient de relever une certaine ambiguïté de la nature de cybercriminalité. D'une part, on note que la cybercriminalité peut se manifester uniquement dans les limites territoriales d'un État et, d'autre part, le cybercrime se présente comme un phénomène transfrontalier. Les auteurs et leurs complices peuvent se trouver dans deux ou plusieurs États, la répression de la cybercriminalité doit se faire à l'aune des infractions en cause et surtout de la zone géographique considérée. C'est pourquoi on observe une variation des sanctions. On doit aussi souligner que le caractère transfrontalier de

certaines de ces sanctions ne fait pas obstacle à la prise en compte des particularismes de chaque État.

Par ailleurs, le champ d'application des normes est inévitablement élargi et nécessite des sanctions et des éclaircissements pour chacune des évolutions. La cybercriminalité dépasse le seuil des réseaux numériques et électroniques puisqu'elle prend une part importante dans les objets connectés. Encore une fois, les modifications des habitudes sont les portes ouvertes aux actes malveillants. Dans ce contexte, les objets connectés tels que les montres, notamment de luxe, sont de nouvelles cibles de contrefaçon ou de détournement de la part des personnes mal intentionnées. Cela soulève la question d'éventuelles adaptations sans fin dans le domaine de la cybercriminalité. Ce souci est la première difficulté qui s'ajoute à la technicité de la matière à encadrer. (Auzuret 2017, p. 394).

En effet, l'application de la territorialité à la répression de la cybercriminalité soulève des enjeux majeurs en matière de coopération internationale. La diversité des lois nationales, la question de la souveraineté des États, la difficulté à identifier les auteurs des actes malveillants en ligne et la compétence extraterritoriale des États constituent autant des défis à surmonter pour assurer une répression efficace de la cybercriminalité à l'échelle internationale.

En outre, l'absence des normes internationales claires en matière de répression de la cybercriminalité et de coopération judiciaire internationale entrave également l'efficacité des poursuites dans ce domaine. Les différentes législations et les procédures entre les pays rendent souvent difficile la coordination des actions. Cette difficulté a été mise en évidence dans l'affaire de la société Microsoft Corporation contre United States, où la Cour suprême des États-Unis a dû se prononcer sur la question de savoir si les mandats de perquisition émis en vertu de la législation américaine pouvaient contraindre Microsoft à fournir des données sur des serveurs situés en dehors du territoire américain. Enfin, les limites de l'application de la territorialité dans la répression de la cybercriminalité transfrontalière sont exacerbées par la rapidité avec laquelle les délinquants de web peuvent opérer et se déplacer à l'échelle mondiale. Cette mobilité virtuelle rend aussi difficilement efficaces des mesures nationales et des mécanismes de poursuite traditionnelle (Arcado, 2007, p.36). Tout bien considéré, l'application de la territorialité dans la répression de la cybercriminalité présente des limites significatives en raison de la nature complexe et mondialisée du cyberespace. Ces limites mettent en lumière la nécessité d'une coopération internationale renforcée et de l'élaboration des normes internationales pour lutter efficacement contre ce fléau à l'échelle mondiale (MORSA, 2016, p. 82-84). Il est essentiel de reconnaître que la cybercriminalité transcende les frontières nationales et nécessite une approche coordonnée au niveau international.

Somme toute, étant donné l'évidence de la délinquance électronique en République du Congo, il appartient au législateur de renforcer et moderniser les dispositifs législatifs sécuritaires en la matière. Au gouvernement congolais de ratifier les instruments juridiques de lutte contre la cybercriminalité et de multiplier des accords avec d'autres États dans le domaine de la coopération contre ce fléau qui, mettant en évidence un réseau transnational de communication, internet, ne serait totalement neutralisé que par une politique internationale, tous azimuts.

Références bibliographiques

AECADO Jérôme, (2007), « Du bon usage des échelles d'équivalence. L'impact du choix de la mesure », Informations sociales, n° 135, 2009, pp.7-9

AUZURET Claire (2017), Analyse des processus de sortie de la pauvreté. Thèse de doctorat de sociologie, Université Bretagne Loire, Nantes, France.

BALANDIER Georges, (1970), Sociologie des mutations, Paris Anthropos.

BALANDIER Georges, (1974), Anthropo-logique, Paris, PUF

BOURDIEU Pierre, (1986), « L'illusion biographique », Actes de la recherche en sciences sociales, vol.62-63, n°1, pp. 69.

CARBONNIER Jean, (1972), Sociologie juridique, Paris, éd. A. Colin.

DURKHEIM Emile, (2004), De la division sociale du travail, Paris, PUF.

FERRI Enrico, (1995), La sociologie criminelle, Paris, Alcan

ITOUA ONDET Maixent Cyr, (2019), Genre et Paix au Congo. Paris, Beaulieu, Éditions Universitaires Européennes, EUE.

LEMAN-LANGLOIS Stéphane, (1996), Notion de criminalité, Paris, Hermès.

MORSA Marc, (2016), Le travail détaché dans l'Union Européenne : enjeux juridiques et européennes », Informations sociales, n°194, pp. 82-94.

PEREIRA Brigitte, (2016), La lutte contre la cybercriminalité, de l'abondance à la norme, à sa perfectibilité, Revue internationale de droit, p.387

ROSE Colin, (2006), Essai sur la notion de cybercriminalité, Paris, IEHEI.

Loi, 2003-12 abrogation ordonnance 2001-11 portant création de la société des télécommunications du Congo ;

Loi n°11-2009 du 25 novembre 2009 portant création de l'agence de régulation des postes et des communications électroniques ;

Loi n°9-2009 du 25 novembre 2009 portant réglementation du secteur des communications électroniques ;

Ordonnance n°2012-293 du 21 mars 2012 sur les Télécommunications et les Technologies de l'Information et de la Communication en Côte d'Ivoire ;

Décret n°2013-213 du 3 mai 2013, contre toute personne coupable de crime se rapportant à la cybercriminalité au Bénin ;

Loi n°30-2019 du 10 octobre 2019 portant création de l'agence nationale des systèmes d'information ;

Loi n°29-2019 du 10 octobre 2019 portant protection des données à caractère personnel ;

Loi n°26-2020 du 5 juin 2020 relative à la cybersécurité ;

Loi n°27-2020 du 5 juin 2020 portant lutte contre la cybercriminalité.

Conventions et Directives

A. Conventions

Convention de Budapest sur la cybercriminalité du 23 novembre 2001

Convention de Malabo du 27 juin 2014 portant sur la lutte contre la cybercriminalité en Afrique

Protocole additionnel de la convention de Budapest du 26 janvier 2013.

B. Directives

Directive européenne n°95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Directive C/D/R/1/08/11 portant lutte contre la cybercriminalité dans l'espace CEDEAO.

Directive n°07/08-UEAC-133-CM-18, fixant le cadre de juridique de la protection des droits des utilisateurs de réseaux et de services communications électroniques au sein de la CEMAC.