REVUE BENINOISE DES SCIENCES JURIDIQUES ET ADMINISTRATIVES

R.B.S.J.A. N° 45
Année 2022

Sommaire

DOCTRINE :

LEGISLATION :

JURISPRUDENCE :

Revue Semestrielle publiée par l'Ecole Nationale d'Administration et de Magistrature (E.N.A.M.) et les Facultés de Droit et de Sciences Politiques des Universités Publiques du Bénin

ISSN : 1840-5169

Revue Semestrielle publiée par l'Ecole Nationale d'Administration et de Magistrature (E.N.A.M.) et les Facultés de Droit et de Sciences Politiques des Universités Publiques du Bénin

COMITE SCIENTIFIQUE

REVUE BENINOISE DES SCIENCES JURIDIQUES ET ADMINISTRATIVES

DOCTRINE

LE PRINCIPE DE TERRITORIALITE DE LA LOI PENALE ET LA CYBERCRIMINALITE AU BENIN

Par

Malick Oluchègoun FALOLA

Docteur en Droit privé
Assistant à la Faculté de Droit et de Sciences politiques,
Université d'Abomey-Calavi (Bénin)

SOMMAIRE

Résumé

Les infractions liées à la cybercriminalité ne sont plus à l'abri des poursuites judiciaires en raison de l'extension du principe de territorialité de la loi pénale aux infractions commises à l'étranger. En matière de la cybercriminalité, la loi de la République est applicable aux infractions liées à la cybercriminalité commises à la fois sur le territoire et à l'étranger. La compétence juridictionnelle est fondée d'une part, sur les principes d'indivisibilité et d'assimilation des faits constitutifs des infractions liées à la cybercriminalité commises à l'étranger et d'autre part, sur la réciprocité d'incrimination. L'exception au principe de territorialité de la loi pénale a pour objectif d'instaurer des mécanismes de poursuites des infracteurs de la cybercriminalité. Cet objectif ne sera pas atteint sans la résolution de la responsabilité pénale internationale des auteurs et complices des cybercrimes. Il a fallu la mise en place d'une coopération internationale favorisant l'obtention des preuves issues des enquêtes policières et l'extradition des suspects accusés pour être jugés vers les Etats victimes de la cybercriminalité. Les infractions liées à la cybercriminalité sont des infractions commises au moyen des réseaux Internet, constituées d'un élément légal, matériel, et d'élément intentionnel. **Mots-clés :** Loi pénale ; cybercriminalité ; juridiction compétente ; loi compétente ; extradition.

Abstract:

Cybercrime offences are no longer immune to prosecution because of the extension of the territoriality principle of criminal law to offences committed abroad. With regard to cybercrime, the law of the Republic is applicable to offences related to cybercrime committed both at home and abroad. Jurisdiction is based on the principles of indivisibility and assimilation of the facts constituting offences related to cybercrime committed abroad and on reciprocity of criminality. The exception to the territoriality principle of the criminal law aims to establish mechanisms for the prosecution of cybercrimers. This objective will not be achieved without the resolution of the international criminal responsibility of the perpetrators and accomplices of cybercrimes. It was necessary to establish international cooperation to obtain evidence from police investigations and the extradition of accused suspects in order to be tried in States that are victims of cybercrime. Cybercrime offences are offences committed through

Internet networks, consisting of a legal, material, and intentional element.

Keywords : Criminal law; cybercrime; competent jurisdiction; competent law; extradition.

INTRODUCTION

Le développement des réseaux d'information et d'*Internet*[1] en particulier semble avoir créé un nouveau terrain potentiel de conflit, dénommé cyberspace[2], qui est une source de multiples menaces[3]. Les systèmes d'information et de communication, sans cesse plus complexes, sont désormais omniprésents, ce qui entraine une dépendance croissante de la société civile à leur égard[4]. Au cœur de cette dimension nouvelle évoluent des délinquants avec leurs méthodes, leurs outils pour passer à l'acte et commettre ainsi des crimes et des délits en utilisant l'informatique comme moyen ou comme cible de leurs méfaits[5].

Avec la progression du taux de pénétration internet, l'Afrique de l'Ouest sera donc de plus en plus confrontée aux défis de la cybersécurité, qu'elle soit la cible ou l'émetteur des menaces[6]. La

---

[1]C. CHAWKI, « *Etude approfondie sur le phénomène de la cybercriminalité et sur les mesures de lutte mises en place par la communauté internationale* », éd. Dar El-Nahda El- Arabia, 2015, n°1, p.5.Le mot « Internet » est composé du préfixe « Inter » qui indique un lien entre deux éléments et le mot « Net » qui est traduit de l'anglais par « réseau ». En fait, il s'agit du plus grand réseau informatique de la planète. Il regroupe une multitude de réseaux régionaux, gouvernementaux et commerciaux. Tous ces réseaux discutent entre eux par le biais du même protocole de communication, TCP/IP (transmission Control Protocol Over Internet Protocol). La connexion est effectuée par l'utilisation de lignes, des câbles, et des satellites comme jonction des lignes téléphoniques. Contrairement aux appels téléphoniques traditionnels, qui transmettent l'information par le circuit communication. L'internet transmet l'information par la « parquet commutation » ; dans ce monde, les communications sont changées en petits signaux. Après ils sont envoyés aux paquets de bénéficiaires, en arrivant à destination par des routes différentes, la communication est alors reconstruite à la fin du récepteur.

[2] Le terme « *cyberspace* » renvoie à son accession usuelle, c'est-à-dire « un ensemble de données numériques constituant un univers d'information et un milieu de communication lié à l'interconnexion mondiale des ordinateurs ». Les racines du mot cyberespace proviennent de l'anglais cybernétiques ou science du gouvernement (1834), décliné du grec kubemetoké, de kubernan, gouverner. M. QUEMENER, Cybermenaces, entreprises et internautes, Paris, économica (2008), p.9.

[3] Ibid., p. 7.

[4]L'économie numérique représente désormais 5,2% du produit intérieur brut, concentre 3,7% des emplois (900000) au sein de 100 000 entreprises de 10 salariés ou plus. A lui seul, le commerce électronique concerne 128000 sites marchands et correspond à 75000 emplois directs ou indirects, pour un chiffre d'affaires de 56 milliards d'euros en 2012 (FEVAD, janvier 2013). La même année, 64% des sociétés disposaient d'un site web ou d'une page d'accueil sur Internet (INSEE). Voir Protéger les internautes, rapport sur la cybercriminalité, 2014, disponible à l'adresse suivante : « wwww.ladocumentationfrançaise.fr », (consulté le 12/10/2014).
A noter également que 35.2% de la population mondiale est connectée, dont 68.06% d'Européens (Internet Word stats, 2013).

[5]M. QUEMENER, « *Cybermenaces, entreprises et internautes* », Paris, économica, éd. 2008, p. 9.

[6] J. Dechanet, M. Ludmann, C. Rossi *« Afrique de l'ouest : le défi de la cybersécurité* », avril 2017, p. 8.

cybercriminalité, principalement les arnaques et escroqueries[7], se développe ainsi rapidement[8]. Selon le Bureau fédéral américain d'investigation (FBI), trois pays africains seraient même classés parmi les dix premières sources de cyber arnaques : le Nigeria (3ème), le Ghana (7ème) et le Cameroun (9ème)[9].

Les infractions informatiques ont le plus souvent un caractère international, alors que les informations en elles-mêmes sont des données régies par le droit interne[10]. Dans cette optique, chaque législateur essaie soit de se protéger sur son territoire, soit d'abdiquer sa compétence législative face à ces actes illicites, soit d'observer et de légiférer aussi peu que possible, ce qui constitue une solution efficace[11]. Cependant, cette situation est insatisfaisante, car elle plonge les internautes dans un réseau de normes multiples, sources d'insécurité juridique[12]. En 2013, sept millions de Français ont été victimes d'actes cybercriminels selon une étude de Symantec[13]. Ces dernières années, et en particulier depuis 2007 avec les cybermenaces ayant frappé l'Estonie, puis de multiples systèmes d'informations de groupes industriels, le cyberspace fait l'objet d'attention et de mise en place de stratégies dédiées. La France a ainsi lancé un « nouveau champ stratégique » en décidant de s'armer en matière de cyber défense et de protection des systèmes d'information[14].

Il semble que les droits positifs ne définissent pas la cybercriminalité[15]. Cependant, certaines notions proches, telles que la criminalité

[7]On distingue généralement les infractions spécifiques aux technologies de l'information et de la communication, les infractions qui y sont liées et les infractions plus traditionnelles qu'elles facilitent.

[8]J. Dechanet, M. Ludmann, C. Rossi *« Afrique de l'ouest : le défi de la cybersécurité* », *op.cit*., p. 8.

[9]« Cybercrime : huit pays africains classés parmi les plus risqués de la planète », http://www.agenceecofin.com/securite/1409-13605-cybercrime-huit-pays-africains-fiches-parmi-les-plus-risquesde-la-planete, Agence ecofin, consulté le 5 août 2022.

[10]S. BRENER et B. KOOPS, « Approches *to Cybercrime Juridiction »*, J. High Tech. L., (2004), Vol. IV, n°1.

[11]N. GAUTHRAUD, « *Internet, le législateur et le juge »*, Paris, Gaz. Pal, (1996).

[12]C. CUTAJAR, « *La loi pour la sécurité intérieur »* éd. Paris, Dalloz, (2003).

[13]M. QUEMENER, « *Protéger les internautes, Rapport sur la cybercriminalité »*, R.I.D.I, numéro 107, Août-Septembre 2014, p. 64.

[14] Ibid. En 2001, on ne trouvait que 20% des foyers français connectés à Internet. Le nombre d'internautes est passé en France de 11,8 millions en 2001 à près de 56 millions en 2013.

[15]CHAWKI l'a affirmé en 2006. Selon le Ministère de l'Intérieur français, et plus particulièrement selon l'OCLCTIC, la cybercriminalité recouvre « l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunication en général et plus particulièrement sur les réseaux partageant le protocole TCP-IP, appelés communément l'Internet »

informatique, l'infraction informatique, la question de l'assimilation ou de la distinction du crime et de la cybercriminalité. Selon le ministère français de l'Intérieur, la cybercriminalité recouvre « l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunications en général et plus particulièrement sur les réseaux partageant le protocole TCP-IP, appelés communément l'Internet »[16]. Selon l'O.N. U, la cybercriminalité doit recouvrir « tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent », et dans une acception plus large « tout comportement illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec un système informatique »[17].

Mondial par nature, l'*Internet* permet aux délinquants de se livrer à presque n'importe quelle activité illicite au plan international. Il est donc essentiel que tous les pays fassent évoluer leurs moyens de lutte sur le plan national de façon à ce que les infractions commises dans le cyberspace ne demeurent pas hors d'atteinte[18]. L'utilisation d'*Internet* par des insoumis, en particulier pour inciter à la rébellion et pour recruter, fait peser une grave menace sur la sécurité, tant au niveau national qu'international[19].

La particularité de la délinquance des réseaux numériques est qu'elle a pour cible un territoire désormais sans frontière et mondialisé[20]. Les cyberdélinquants vont par exemple commettre des attaques dans un pays où la légalisation est encore inexistante et les effets de leurs actions vont se faire sentir à l'autre bout du monde, ce qui rend souvent très complexe le déroulement des enquêtes[21].

---

[16]Désigne les protocoles communs de communication utilisée par l'internet, permettant l'interconnexion généralisée entre réseaux hétérogènes. Le ministère de l'Intérieur français. Disponible sur http://www.intérieur.gouv.fr/

[17] Dixième Congrès des Nations Unies, à Vienne, sous le titre « la prévention du crime et le traitement des délinquants », (10-17 avril 2000).

[18]Le Cameroun, à la suite d'autres Etats africains tel que le Sénégal ayant promulgué la loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité. Loi n°09-04 du 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication en Algérie, in S. TEPI « *La cybercriminalité au Cameroun en quête d'efficacité, Paris, édition l'harmattan* », 2020, p.23.

[19]M. QUEMENER Y. CHARPENEL, *Cybercriminalité, Droit pénal appliqué*, pratique du droit, éd., économica, septembre 2010, n°63, p. 14.

[20]J. Dechanet, M. Ludmann, C. Rossi *« Afrique de l'ouest : le défi de la cybersécurité* », *op.cit*., p. 24.

[21]M. QUEMENER Y. CHARPENEL, *op.cit*., n°64, p. 14.

La cybercriminalité est par essence mondiale, puisque les infractions peuvent être commises simultanément dans plusieurs pays. Cette criminalité planétaire pose de nouveaux défis aux Etats qui prennent progressivement conscience de la nécessité d'une approche transfrontalière de cette délinquance des réseaux numériques[22]. Les actions délictueuses sont en effet commises par des individus qui peuvent habiter dans des pays différents de ceux où les effets de ces infractions vont se faire sentir[23].

Une mobilisation des Etats et un renforcement des moyens de lutte apparaissent dès lors indispensable et on assiste actuellement à des évolutions dans ce domaine même si une marge de progression est nécessaire au niveau mondial afin que les crimes et délits commis via les réseaux numériques ne restent impunis[24]. La poursuite des acteurs de la cybercriminalité devient un enjeu pour des Etats en raison de son caractère international. L'infraction de cybercriminalité présente des liens avec plusieurs Etats dès lors que le cybercriminel a commis l'infraction dans un Etat alors que les victimes sont domiciliées dans plusieurs Etats. Les critères de la nationalité de l'auteur de la cybercriminalité, la nationalité des victimes et l'Etat de la commission de cette infraction constituent des obstacles à la mise œuvre du principe de territorialité.

La territorialité est la règle selon laquelle le champ d'application d'une loi est limité à un espace territorial. Aucune loi nationale n'a d'effet hors de son territoire. Un rattachement est nécessaire pour permettre l'application d'une loi à une situation donnée. La territorialité de la loi pénale découle du principe de souveraineté des Etats que chaque Etat est libre de fixer sa sphère de compétence territoriale[25]. Mais la mondialisation n'est pas sans incidence sur l'application des règles de droit pénal et bouleverse en particulier le principe de la territorialité de la loi pénale et tend à remettre en cause la conception traditionnelle du droit pénal qui est l'expression de la souveraineté des Etats[26]. La cybercriminalité qui ne connaît pas les frontières s'inscrit parfaitement dans ce nouveau mouvement et bouleverse fondamentalement ce grand principe, les infractions pouvant être commises en même temps

[22]J. Dechanet, M. Ludmann, C. Rossi *« Afrique de l'ouest : le défi de la cybersécurité* », *op.cit*., p. 24.
[23]M. QUEMENER Y. CHARPENEL, *op.cit*., n°66, p. 14.
[24]M. QUEMENER Y. CHARPENEL, *op.cit*., n° 67, p. 14.
[25]Cour permanente de justice internationale, Lotus, 1927.
[26]M. QUEMENER Y. CHARPENEL, *op.cit*., n°695, p.157.

dans plusieurs pays. En effet, compte tenu de la virtualisation et de la dématérialisation des données, le lieu de la perpétration de la cybercriminalité n'est pas forcément situé sur le territoire national ou dans le ressort où se manifestent concrètement les conséquences de cette infraction[27].

La localisation des infractions recouvre une importance capitale quant à l'applicabilité de la norme sur le plan territorial et à l'identification des cyber délinquants. Toutefois, traiter de la localisation des cyber infractions revient à concilier le caractère délimité de la règle pénale au niveau de l'espace et l'universalité des réseaux numériques. Ces derniers offrent l'omniprésence et l'instantanéité des échanges d'informations. Or, au sein du cyberespace mondial, l'efficacité du droit répressif souffre d'une certaine relativité compte tenu de son caractère essentiellement souverainiste[28]. En dépit d'une coopération interétatique, la cybercriminalité est régie par les droits pénaux nationaux. Si les conventions internationales permettent de s'acheminer vers l'harmonisation des législations, les souverainetés nationales coexistent, de même que leurs expressions sous forme de réserves étatiques. Ainsi, le droit répressif demeure une expression territorialisée de la souveraineté des Etats. Dès lors se pose la question de savoir si le critère de la territorialité répond sûrement aux enjeux de la lutte contre la criminalité[29]. Dans la mesure où l'infraction peut être localisée sur le territoire national, la loi et les juridictions de l'Etat visé sont compétentes. Ainsi, la loi pénale béninoise est applicable aux infractions commises ou réputées commises sur le territoire de la république du Bénin[30]. Il en est de même dans les autres Etats, la tendance consistant à étendre le critère de compétence de territorialité pour sanctionner les crimes et délits localisés même partiellement sur un territoire[31]. Les infractions commises dans le cyberespace sont alors réprimées par les normes nationales territorialement compétentes[32]. Cependant, même

[27]Ibidem
[28]M. DELMAS-MARTY, *« Les forces imaginantes du droit, t.1, Le relatif et l'universel* », Paris, Le Seuil, 2004, p. 336.
[29]B. PEREIRA, « *La lutte contre la cybercriminalité* : de l'abondance de la norme à sa perfectibilité », n° 2-2, p. 399.
[30]Article 10 alinéa 1er de la loi n° 2018-16 du 28 décembre 2018 portant code pénal en république du Bénin.
[31]D. REBUT « *Droit pénal international* », 2ème éd., précis Dalloz, Paris, Dalloz, 2014 ; Cass. crim. 12 février 1979, Bull. crim. n°60 ; 1er octobre 1986, n°262 ; 26 septembre 2007, n°224.
[32]Cass. crim., 11 septembre 2007, n° 07-82018 ; 4 février 2004, Bull. crim. n°32, D. 2005, p.621, note V. Malabat ; 6 août 2008, n°08-83490.

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 juridique en raison du caractère insaisissable des flux transfrontaliers » qu'à la multiplication des normes et juridictions compétentes[33]. En réalité, tous les Etats du monde sont susceptibles de se déclarer compétents à travers l'application du principe de territorialité, ce qui conduit à des conflits de compétences, en dépit du principe *non bis in dem*. Dès lors, l'harmonisation des législations nationales n'empêche pas les juridictions et les Etats de se déclarer compétents en dépit de la chose jugée à l'étranger[34]. Il en ressort des risques de chevauchement des poursuites. Le Conseil de l'Union européenne a également adopté, le 24 février 2005, une décision cadre relative aux attaques visant les systèmes d'information. Cette décision-cadre vient d'être remplacée par la Directive du 12 août 2013, 2013/40/UE du Parlement européen et du Conseil relative aux attaques contre les systèmes d'information[35]. Dans le cadre de la CEDEAO, la Directive communautaire du 19 août 2011, portant lutte contre la cybercriminalité dans l'espace de la CEDEAO, a érigé en infractions spécifiques les atteintes aux systèmes informatiques dans ses articles 5 à 8[36]. En Afrique, quelques rares pays ont prévu des dispositifs de protection pénale des systèmes informatiques particulièrement inspirés de la loi française[37]; il s'agit notamment du Burkina Faso[38] et du Niger[39], du Cameroun et du Bénin.

Plus concrètement, les infractions commises dans le cyberespace mettent en cause un réseau électronique. La question se pose sur la localisation de ces infractions : « Les règles nationales attributives de compétence législative et juridictionnelle en matière pénale répondent en apparence aux nécessités de répression, le principe étant celui de la solidarité de ces compétences ». Il en est donc plus particulièrement, « en cas d'application du critère de compétence

---

[33]J. FRANCILLON, « *Cybercriminalité-Aspects de droit pénal international »*, Revue électronique de l'Association internationale de droit pénal, 2014, RH-7, 37 pages, spéc. p.7.
[34]Conseil de l'Europe, Rapport d'évaluation : les dispositions de la Convention de Budapest sur la criminalité concernant l'entraide, adopté par le T-CY, comité de la Convention de cybercriminalité, Strasbourg, 3 décembre 2014, p. 216.
[35]Journal de l'union européenne L. 218/8 du 14 août 2013.
[36]P. A. TOURE, *« Le traitement de la cybercriminalité devant le juge, l'exemple du Sénégal* », Paris, éd. l'harmattan, 2014, p. 50
[37] Loi française du 5 janvier 1988 relative à la fraude informatique.
[38]La loi du Burkina-Faso du 13 nov. 1996 portant code pénal (art. 541 à 543).
[39]La loi nigérienne n°2003-25 du 13 juin 2003 modifiant le Code pénal (articles 399.2 à 3999.4)

territoriale, dès lors que l'infraction peut être localisée sur le territoire national, en totalité, ou en partie seulement ». Or, sur ce point, la jurisprudence est controversée. Si l'on se reporterait au lieu d'émission des informations ou au lieu d'origine, cela conduirait les cybercriminels à s'établir dans des pays à la législation permissive ; si l'on se référait au lieu de la réception, celui où le site étranger peut être accessible, cela permettrait à tous les pays dans lesquels le site est accessible de se déclarer territorialement compétents : il s'agirait alors d'un questionnement de superposition de compétences et corrélativement d'une insécurité juridique[40]. Dans un premier temps, et celui de l'accessibilité des sites s'agissant d'Internet (apologie des crimes de guerre)[41]. Puis, la jurisprudence est allée dans le même sens en matière d'infractions relatives à la presse[42]. Il en a été de même dans une affaire de dépréciation de produits pharmaceutiques[43] et en matière d'infractions à la réglementation des jeux et paris en ligne[44].Le principe de la territorialité du droit et de la procédure pénale découle de l'autonomie des Etats. Les lois pénales sont l'expression d'une prérogative des Etats, donc de leur souveraineté. Elles sont exclusivement d'applications nationales[45]. Cette affirmation est encore à nuancer au regard de la théorie d'ubiquité qui permet aux juridictions françaises de déclarer les lois de ce pays compétentes toutes les fois qu'un élément constitutif de l'infraction a lieu sur le territoire ou lorsque l'infraction produit des effets, sur le territoire français[46]. Les lois pénales classiques connectent les faits répréhensibles à un Etat.

Les TIC, notamment, l'Internet est partout, sur tous les territoires à la fois : « Il emprunte les lignes téléphoniques de tous les pays sans considération de frontières et son maillage est tel qu'il n'est pas possible de déterminer a priori le chemin que suivront les données

---

[40] M. VIVANT « *Cybermonde : droit et droits des réseaux* », JCP, 1996, I, 3969.

[41]TGI Paris, référé, 22 mai et 20 novembre 2000, Comm.com. électr. 2000, comm. N° 92 ; TGI Paris, 17è ch. 26 février 2022, n°77, obs. A. Lepage ; CA Paris, 11è ch., 17 mars 2004, Comm. Com. électr. 2002, n°77, obs. A. Lepage ; CA Paris, 11è ch., 17 mars 2004, Comm.com. électr. 2005, comm. N°72, obs ; A. Lepage.

[42]TGI Paris, 13 novembre 1998, Gaz. Pal.2000, 1, doctr. P.697 ; Limoges, 8 juin 2000, BICC 2001, p. 210 ; Paris, 11è ch. 17 mars 2004, arrêt préc.

[43]Cass. crim., 15 janvier 2008, Bull. crim. n°5.

[44]T. corr. Nanterre, 15è ch., 15 mars 2007, Revue des sciences criminelles 2008, p. 101, obs. J. Francillon.

[45]Hormis certaines règles pénales de protection des droits de l'homme à l'instar du droit belge qui se donne une vocation internationale. Cette loi est donc compétente en cas de crime contre l'humanité quel que soit l'endroit de sa commission.

[46]M. QUEMENER Y. CHARPENEL « *Cybercriminalité, Droit pénal appliqué* », pratique du droit, éd., économica, septembre 2010, n°63, p. 158.

pour être acheminées d'un point à un autre de la planète. Ensuite son architecture est distribuée et non hiérarchique, il fédère une multitude de réseaux différents quant à leurs natures, origines et fonctionnements. Les ordinateurs qui y sont connectés appartiennent indifféremment à des personnes physiques ou morales, de droit public ou privé. Le réseau n'appartient donc à personne, il connaît une gestion décentralisée, il est impossible d'identifier un responsable de la toile. Il échappe à un contrôle global des Etats, dont les compétences sont limitées par les frontières, car l'Internet ignore celles-ci et fait de l'intégralité de la planète, son domaine »[47].Cette technologie outrepasse les frontières nationales et fait du concept de village « *village planétaire* »[48] une réalité. Certains parlent « *d'aterritorialité* »[49] d'*Internet*.

Il est donc difficile, voire impossible pour l'Etat, d'exercer son pouvoir de sanction par des lois qui se limitent à un espace donné sur des phénomènes qui dépassent le cadre de ses frontières. Cela ne fait aucun doute dans un concept du droit où la sanction, la contrainte font partie des prérogatives réservées aux Etats. Quelles règles s'appliqueront aux actes répréhensibles commis sur ce territoire illimité ? L'*Internet* n'ayant pas de territoire, il en découle que les infractions qui y sont commises ont une grande portée et sont réfractaires à l'expression de l'indépendance des Etats par leurs lois pénales. Pourtant le cyberspace n'est pas forcément une zone de non-droit.

En octobre 2016, la Commission de la CEDEAO[50] et le Conseil de l'Europe, à travers un échange de lettres, ont convenu d'aider les États membres pour le renforcement de leur législation interne sur la base de la «Convention de Budapest sur la cybercriminalité» et de la «Convention N°108 sur la protection des données» du Conseil de l'Europe, outre la «directive C/DIR 1/08/11 de la CEDEAO sur la lutte contre la cybercriminalité au sein de l'espace de la CEDEAO" et d'autres textes comme "l'Acte additionnel A/SA.1/01/10 sur la protection des données à caractère personnel au sein de la CEDEAO"

---

[47]P.-M. REVERDY, « *La matière pénale à l'épreuve de la délinquance informatique* », thèse de doctorat de droit privé, Toulouse, I, 2005, p. 16.
[48] MEIR, *op.cit.*, p.143.
[49]UIT, « Guide de la cybersécurité pour les pays en développement », édition 2007, p.9, disponible en ligne sur : www.iut.int/IUT-D/cyb/cybersecurity/legislation.htlm Consulté le 15/5/12.
[50]Communauté Economique Des Etats de l'Afrique de l'Ouest. (CEDEAO)

et "l'Acte additionnel A/SA.2/01/10 sur les transactions électroniques dans l'espace de la CEDEAO " ainsi que pour l'élaboration de politiques et stratégies de lutte contre la cybercriminalité[51].

Dans l'affaire Yahoo, c'est ce que la juridiction française saisie a tenté de démontrer en se déclarant compétente pour une infraction qui a causé préjudice aux demandeurs alors que l'auteur de la faute se trouvait hors du territoire[52]. Ces mécanismes permettent aux Etats d'imposer leurs lois à des personnes cibles en dehors de leur territoire constituent une exception qui n'est pas toujours gagnée d'avance[53]. La question de la compétence des juridictions pénales françaises est un problème majeur pour la performance et le rayonnement de la loi française. Ainsi, plus les juridictions françaises sont compétentes, plus le rayonnement de la loi française est grand. Le principe de territorialité a ainsi été étendu de différentes manières, notamment par assimilation et indivisibilité. S'agissant du principe de l'extension par indivisibilité du principe de territorialité, la jurisprudence de la Cour de cassation a jugé que le délit d'association de malfaiteurs reproché à un prévenu de nationalité étrangère et commis à l'étranger, est indivisiblement lié aux infractions à la législation sur les stupéfiants commises en France dès lors que celui-ci savait que le projet auquel il était associé pouvait le conduire à entrer dans les eaux territoriales françaises[54]. S'agissant de l'extension par assimilation du principe de territorialité, la jurisprudence de la Cour de cassation a jugé qu'une infraction est réputée commise sur le territoire de la république dès lors qu'un de ses faits constitutifs a été commis sur le territoire[55]. L'extension par assimilation du principe de territorialité est fondée sur l'article de 10 du Code pénal béninois[56].La dérogation du principe de territorialité de la loi pénale par la double incrimination est fondée sur l'article 14 du code pénal béninois[57].

[51]Action globale sur la cybercriminalité élargie, harmonisation de la législation sur la cybercriminalité et les preuves électroniques, avec des garanties pour l'état de droit et les droits de l'homme, conférence régionale conjointe entre la CEDEAO et le conseil de l'Europe, avec la participation des Etats membres de la CEDEAO, 11-13 septembre 2017 à Abuja, Nigéria Avec l'appui du projet GLACY+ (activité 3.2.3)

[52]TGI de Paris, 22 mai, 2000, UEFJ et Licra c/ Yahoo. Inc ; et Yahoo France.

[53]R. DIARRA*, « La répression de la cybercriminalité en Afrique de l'Ouest* », p.18.

[54]Cass. Crim., 11 juin 2008, FS-P+F, n° 07-83.024

[55]Cass. Crim., 9 nov. 2011, P+F, n° 05-87.745 et 09-86.381

[56]Article 10 de la loi n° 2018 portant code pénal béninois « La loi pénale est applicable aux infractions commises sur le territoire de la République du Bénin ». L'infraction est réputée commise sur le territoire de la République du Bénin dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire ».

[57]Article 14 de la loi n° 2018 portant code pénal béninois « La loi pénale est applicable à quiconque s'est rendu coupable sur le territoire de la République, comme complice, d'un

Dans cette condition, la poursuite des infractions de cybercriminalité ayant un caractère international n'échappe pas à la compétence juridictionnelle de la république du Bénin. Le principe de territorialité de l'Etat ayant son fondement dans celui de la souveraineté de l'Etat ne constitue plus un obstacle à la poursuite voire à la répression des auteurs ou complices des infractions commises hors du territoire national de la république du Bénin. L'enjeu est de taille en matière de la répression des cybercriminels, l'Etat est convaincu qu'il y a lieu d'admettre la dérogation du principe de territorialité de la loi pénale dans la poursuite des auteurs des infractions liées à la cybercriminalité. Il convient d'analyser la détermination de la compétence juridictionnelle et la spécification législative en matière de la cybercriminalité (I) la recherche des preuves et la responsabilité pénale internationale en matière de la cybercriminalité (II).

I) La détermination de la compétence juridictionnelle et la spécification législative

La compétence des juridictions est l'aptitude à instruire ou à juger une affaire, à en connaître » est une notion d'ordre public qui peut être soulevée à tout moment de la procédure et même d'office[58]. La question de la compétence territoriale est fondamentale dans le traitement policier et judiciaire de cybercriminalité car dans de nombreuses affaires, les investigations sont transfrontalières. Le caractère international de ces infractions est souvent source de difficultés pour déterminer quelle va être la juridiction territorialement compétente pour juger de l'affaire. Ainsi que le souligne le rapport explicatif de la Convention du Conseil de l'Europe relative à la cybercriminalité : « *le caractère international des infractions en question- par exemple celles commises au moyen de l'internet-se heurte à la territorialité des institutions nationales de répression.* »[59].

En matière des infractions de la cybercriminalité, la question de la détermination de la juridiction compétente reste d'actualité dans le cadre de la poursuite des acteurs des infractions de la cybercriminalité. Le caractère international de la cybercriminalité justifie l'exclusion du respect du principe de territorialité de la loi pénale

---

crime ou d'un délit commis à l'étranger si le crime ou le délit est puni à la fois par la loi béninoise et par la loi étrangère et s'il a été constaté par une décision définitive de la juridiction étrangère ».

[58]S. GUINCHARD J., BUISSON « *Procédure pénale* », 3ème édition, Litec, 2005, n°1051.

[59]M. QUEMENER Y. CHARPENEL, *op.cit.*, n°696, p.157.

à la cybercriminalité. Cela relève du droit pénal international précisant les critères juridiques de la détermination de la compétence juridictionnelle (A) et la spécification de la loi applicable (B).

A) La détermination de la compétence juridictionnelle

Au Bénin, en particulier, la Cour de répression des infractions économiques et du terrorisme est compétente pour juger des infractions liées à la cybercriminalité[60]. Au Sénégal les juridictions de jugement sont compétentes à connaître des infractions liées à la cybercriminalité[61]. Les juridictions des Etats de l'Afrique de l'Ouest sont compétentes dès lorsque les infractions de cybercriminalité sont commises sur leurs territoires par les étrangers[62]. La nature mondiale de la cybercriminalité admet la délimitation de la compétence juridictionnelle des infractions de cybercriminalité fondée sur les principes d'indivisibilité et d'assimilation des faits constitutifs des infractions commises à l'étranger (1) et la compétence juridictionnelle fondée sur la réciprocité d'incrimination dans le cadre de la poursuite des auteurs de la cybercriminalité (2).

1) Une compétence juridictionnelle fondée sur les principes d'indivisibilité et d'assimilation

La convention de l'union africaine sur la cybersécurité et la protection des données à caractère personnel adoptée à Malabo en guinée équatoriale le 27 juin 2014, ne règle pas la question de compétence de juridiction lorsque les infractions sur la cybersécurité commises impliquent plusieurs Etats[63]. Les juridictions béninoises sont compétentes lorsque les délits ont été commis par des Béninois hors du territoire de la République du Bénin si les faits sont punis par la législation du pays où ils ont été commis[64]. Elles sont compétentes

[60] Article 5 alinéa 6 nouveau de la loi portant organisation judicaire au Bénin « les infractions commises par des moyens de communication électronique portant gravement atteinte à l'ordre public, à la sécurité nationale, au moral des troupes et au patrimoine de l'Etat ou des particuliers ».

[61] TRHC Dakar, n°4241 du 18 septembre 2009, affaire *Pneumeca, inedit*.

[62] Le 5 août 2007, des individus de nationalité nigériane accusé d'être des auteurs d'escroquerie via internet ont été arrêtés au Sénégal par la Gendarmerie à Dakar Yoff. Les auteurs de ces faits ont été arrêtés et déférés au parquet de Dakar.

[63] ISSA-TOURE, Rapporteur de la commission des relations extérieures et de la coopération ; du parlement de la République Togolaise « Rapport de l'étude au fond du projet de loi autorisant la ratification de la convention de l'union africaine sur la cybersécurité et la protection des données à caractère personnel, adoptée à Malabo en guinée équatoriale le 27 juin 2014 ».

[64] Article 597 alinéa 3 de la loi n° 2017-20 portant code du numérique en République du Bénin

également lorsque tout délit puni d'emprisonnement, a été commis par un Béninois ou par un étranger hors du territoire de la République du Bénin lorsque la victime est de nationalité béninoise au moment de l'infraction[65].

Les règles de compétence des juridictions béninoises contenues dans le code pénal sont complètes et permettent de poursuivre et de sanctionner des actes commis hors des frontières de la République béninoise, y compris ceux commis par des personnes de nationalité étrangère. Les infractions de la cybercriminalité ne sont pas exclues car ces règles de compétence juridictionnelle leur sont applicables. La cybercriminalité s'opère dans un monde immatériel. Les infractions de cybercriminalité sont constituées des éléments constitutifs ayant des liens étroits avec plusieurs Etats, excluant l'application du principe de territorialité de la loi pénale. La poursuite des acteurs de la cybercriminalité commise hors du territoire d'un Etat est de la compétence juridictionnelle des infractions de cybercriminalité fondée sur le principe d'indivisibilité des faits constitutifs des infractions commises à l'étranger et sur le principe d'assimilation des faits de complicité perpétrés en France.

Aux termes de l'article 10 du code pénal béninois, la loi pénale béninoise s'applique, par principe aux infractions commises ou réputées commises sur le territoire de la République béninoise[66], ce qui détermine dans le même temps la compétence du juge pénal béninois, par application du principe de la solidarité des compétences législatives et judiciaires porté par l'article 639 alinéa 1, 2 et 4 du code béninois de procédure pénale[67]. Certes, les juridictions répressives peuvent connaître dans certains cas de crimes et délits commis à l'étranger, mais c'est seulement lorsqu'une règle de compétence extraterritoriale (personnelle, réelle, universelle ou *sui generis*) est applicable. Tel est le cadre général qui permet d'ordonner la compétence internationale du juge pénal béninois. Cela étant, la

---

[65]Article 597 alinéa 4 de la loi n° 2017-20 portant code du numérique en République du Bénin
[66]Article 10 de la loi n° 2018-16 portant code pénal en république du Bénin.
[67]Article 639 alinéa 1 ; 2 et 4 de la loi n° 2012-15 du 18 mars 2013 portant code de procédure pénale en république du Bénin « Tout citoyen béninois qui en dehors du territoire de la République s'est rendu coupable d'un fait qualifié crime par la loi béninoise peut être poursuivi et juge par les juridictions béninoises. Tout citoyen béninois qui en dehors du territoire de la République s'est rendu coupable d'un fait qualifié délit par la loi béninoise, peut être poursuivi et jugé par les juridictions béninoises si le fait est puni par la législation du pays où il a été commis. Les dispositions des alinéas I et, 2 et 3 sont applicables à la personne qui n'a acquis la qualité de citoyen béninois que postérieurement au fait qui lui est imputé ».

jurisprudence développe une conception extensive de la compétence territoriale en admettant que les tribunaux français puissent connaître d'une infraction commise à l'étranger lorsque celle-ci forme «un tout indivisible»[68] avec une infraction localisée en France[69]. Ce rattachement fictif au territoire a été mis en œuvre dans différentes configurations, que l'infraction source ou d'origine soit située à l'étranger[70] ou sur le territoire français. L'indivisibilité exprime un lien plus fort que la connexité[71], comme le montre d'ailleurs en droit interne béninois l'article 643 du code de procédure pénale[72], notion dont elle est cependant très proche[73]. Toutefois, si la connexité s'avère insuffisante à étendre la compétence territoriale du juge pénal français à des infractions commises à l'étranger[74], comme nous le reverrons, l'indivisibilité se voit investie de cette puissance d'attraction[75].

Forgée par la Cour de cassation au XIXème siècle[76], l'indivisibilité a été définie en procédure pénale comme exprimant « un rapport mutuel de dépendance » en procédure pénale comme exprimant « un rapport mutuel de dépendance » entre des infractions, « un lien tellement intime » que l'existence d'une infraction ne se comprendrait pas sans l'existence de l'autre[77]. Répétée a de nombreuses reprises[78], cette définition, bien que jugée insuffisante en doctrine[79], a été ainsi appliquée en 2016 par la Chambre criminelle qui, dans un contexte international, a jugé que l'indivisibilité est caractérisée lorsque que « des faits (…) sont rattachés entre eux par un lien tel que l'existence des uns ne se comprendrait pas sans l'existence des autres »[80].

---

[68]Crim. 13 déc. 1933, Bull. crim n°237 ; Crim. 23 avr. 1981, n°79-09.346 et 81-90.489, Bull. n°116 ; RSC 1981.609, obs. A. Vitu.

[69]V. D. REBUT*, « Droit pénal international »*, 2ème éd. Précis, Dalloz, 2015, n°59, p.41

[70]Ex. Crim. 15 janv. 1990, n° 86-96.469, Bull. crim. n° 22 ; Crim., 15 mars 2006, n°05-83.556, Bull. crim. n°78 ; AJ pénal 2006.269, obs. M.-E. C.

[71]R. MERLE A. VITU, *Traité de droit criminel. Procédure pénale*, 5ème éd., Paris, Cujas, 2001, n°707 s.

[72]L'article 643 de la loi n°2012-15 du 18 mars 2013 portant code de procédure pénale en république du Bénin « Est réputée commise sur le territoire de la République, toute infraction dont un acte caractérisant un de ses éléments constitutifs a été accompli en République du Bénin ».

[73]M. Gobert, La connexité en procédure pénale, JCP 1961. I. 1607.

[74]D. Rebut*, op. cit*., n° 60, p. 42.

[75]V. not. Crim.24 mars 1875, Bull. crim. n° 239

[76]V. not. Crim. 24 juin 1875, préc.

[77]Crim. 24 mars 1875, préc.

[78]V. not. Crim. 13 juin 1958, n°68-90.382, Bull. crim. n°196.

[79] V. not. Rebut, *op. cit.,* n°59

[80]Crim. 31 mai 2016, n°15-85.920, Bull. crim. n°165; D. 2016. 1989, note D. Rebut.

L'extraterritorialité est ce qui permet à la France et le Bénin d'étendre leur juridiction sur des territoires situés dans un pays étranger. Le droit international permet d'encadrer ce pouvoir et de le limiter à certains champs d'application, ce afin d'éviter des abus de pouvoir ou des cas d'ingérence. L'article 14 du code pénal béninois[81] étend le principe de territorialité de la loi pénale au complice sur le territoire de la République du bénin d'une infraction commise à l'étranger. Il existe néanmoins une réserve quant à la définition de ces infractions. Il doit s'agir de crimes ou délits dont l'incrimination est réciproque. De plus, l'infraction principale doit avoir été jugée de façon définitive à l'étranger. Il en résulte que le principe de territorialité aurait dû conduire à exclure la compétence française mais si ce complice est français et parce que la France n'extrade pas ses nationaux, cela aboutissait à ne pas poursuivre ce complice français coupable en France d'actes de complicité d'une infraction commises à l'étranger[82]. L'article 640 du code béninois de procédure pénale est applicable dans les mêmes conditions au complice d'une infraction de cybercriminalité commise à l'étranger dont l'auteur principal est jugé par une décision définitive par la juridiction étrangère pour une infraction de la cybercriminalité punie à la fois par la loi béninoise et la loi étrangère[83]. Lorsque ces conditions sont réunies les juridictions béninoises sont compétentes.

2) Une compétence juridictionnelle fondée sur la réciprocité d'incrimination

Les juridictions béninoises sont compétentes lorsque la personne physique ou morale s'est rendue coupable sur le territoire de la République du Bénin, comme complice, d'un crime ou d'un délit commis à l'étranger si le crime ou le délit est punis à la fois par la loi béninoise et par la loi étrangère et s'il a été constaté par une décision définitive de la juridiction étrangère[84].

---

[81] Article 14 du code pénal béninois précité

[82]cours-de-droit.net/principe-de-territorialite-de-la-loi-penale-a121607262/

[83]L'article 640 de la loi n° 2012-15 du 18 mars 2013 portant code de procédure pénale en république du Bénin « Quiconque s'est, sur le territoire de la république rendu complice d'un crime ou d'un délit commis à l'étranger, peut être poursuivi et jugé par les juridictions béninoises, si le fait est puni à la fois par la loi étrangère et par la loi béninoise, à la condition que le fait qualifie crime ou délit soit et constaté par une décision définitive de la juridiction étrangère ».

[84]Article 597 alinéa 2 de la loi n° 2017-20 portant code du numérique en République du Bénin

En matière de compétence extraterritoriale des juridictions nationales, la double incrimination signifie que le délit commis à l'étranger et poursuivi en France doit être également punissable dans l'Etat sur le territoire duquel il a été commis[85], tandis qu'en matière de coopération pénale internationale la double incrimination se définit comme « le fait que le comportement qui est l'objet de la coopération soit constitutif d'infraction tant dans l'Etat requérant que dans l'Etat requis»[86]. En droit international public, la réciprocité est «la situation dans laquelle un Etat assure à un autre Etat ou à ses ressortissants un traitement équivalent à celui que lui réserve ce dernier» ou qu' «un Etat pratique envers un autre Etat lorsqu'il bénéficie en fait, sur le territoire de cet Etat, du même traitement»[87]. En droit international, la réciprocité est également l'un des plus fameux principes gouvernant les relations internationales et plus notamment en matière de coopération inter-étatique. L'extradition est ainsi régie par ce principe primordial qui est celui de la réciprocité. Ce principe fait obstacle à l'extradition lorsque l'Etat requis ne reçoit pas d'engagement formel de l'Etat requérant garantissant qu'il est disposé à accueillir favorablement une demande d'extradition du même genre. Cela en fait d'ailleurs un principe plutôt politique que juridique[88].

En droit pénal international, l'utilisation de ce terme de réciprocité semble conduire à exiger une sorte d'incrimination commune aux deux Etats. Le juge français est alors chargé de vérifier la présence d'une incrimination équivalente au sein de la loi étrangère. Le professeur LOMBOIS précisant pourtant à ce propos que *«point n'est besoin, dans les deux lois, d'une identité de termes et, pas même, d'une identité de structure de l'infraction»*[89]. En somme peu importe l'identité de la qualification ou de la sanction[90].

L'article 14 du Code pénal béninois « La loi pénale est applicable à tout crime commis par un béninois hors du territoire de la République. Elle est applicable aux délits commis par des béninois hors du territoire de la République si les faits sont punis par la législation du pays où ils

---

[85]E. DREYER, « *Droit pénal général* », 3ème édition, LexisNexis, 2014, p. 1251, n° 1864.
[86]D. FLORE, « *Droit pénal européen les enjeux d'une justice pénale européenne* », Larcier, 2009, p. 413.
[87]G. CORNU, Vocabulaire juridique, 11ème édition, puf, 2016.
[88]Xème congrès de l'Association internationale de Droit pénal, Les problèmes actuels de l'extradition, RIDP, 1968. Plus particulièrement : Hans Schutlz, rapport général, p. 785 et s.
[89]C. LOMBOIS, « *Droit international* », 2ème éd. Dalloz, 1979, p. 485, n°378 et s.
[90]W. JEAN DIDIER, « *Droit pénal général* », 2ème édition, Montchrestien, 1991, n° 164.

ont été commis ». Il résulte que les délits perpétrés par des béninois à l'étranger sont susceptibles d'être poursuivis uniquement lorsque « les faits sont punis par la législation du pays où ils ont été commis ». Cette règle de la réciprocité des incriminations est d'ordre public. La réciprocité d'incrimination n'est exigée qu'en matière de compétence personnelle active et pour les seuls délits[91].Un ressortissant français, Grégory M., était incarcéré en France, et purgeait une peine de deux ans d'emprisonnement pour des faits de vols et d'escroquerie en réunion. La police suisse, dans le cadre d'une enquête sur des faits similaires commis en Suisse à la même époque, identifia le suspect comme étant Grégory M... Le procureur décida de poursuivre le délinquant, et la Cour d'appel d'Aix-en-Provence, dans un arrêt en date du 7 septembre 2009, condamna ce dernier à deux ans d'emprisonnement pour vols aggravés et escroquerie, en récidive. Cette poursuite requiert une phase diplomatique de transmission des dossiers entre ministères de la justice relativement lourde. Il en est de même au sein de l'Union Européenne, avec la Convention Européenne d'entraide judiciaire en matière pénale du 20 avril 1959. Cette dernière a été interprétée par la chambre criminelle comme n'apportant « aucune dérogation au principe de la dénonciation entre ministère de la justice »[92]. Cette jurisprudence est applicable dans l'espace matériel. Dans l'espace immatériel, il n'est plus difficile de déterminer les auteurs et complices des infractions de cybercriminalité. La Befti met désormais à disposition des entreprises des techniciens qui font les constatations sur place car, dans ce domaine, les preuves sont fragiles. *« Il suffit d'un clic pour supprimer la trace de l'infraction »,* prévient le commissaire, qui n'hésite pas à rappeler que l'efficacité de l'action de traçabilité nécessite aussi *« la conservation, pendant un an, de deux données essentielles : l'adresse IP et le lien entre cette adresse et la ligne téléphonique »*. Ces éléments devront être précisés dans la loi sur la société de l'information (LSI)[93]. En effet, le tribunal de grande instance de Paris[94], s'est montré plus affirmatif, dans un jugement du 24 juin 2009, en affirmant que l'adresse IP est une donnée personnelle qui permet de retrouver la personne physique qui a mis en ligne un contenu. Il y a moins d'obstacle dans

[91]A. GUIDICELLI « *Droit pénal international* », in Revue de science criminelle et de droit pénal comparé, 2018/2 N°2, p. 557-567.
[92]Crim. 26 mai 2010, n°09-86.4999, F-P+F
[93] https://www.lesechos.fr/2002/06/cybercriminalite-infractions-en-vrac-693532
[94]TGI Paris, 3ème ch.3è sect. 24 juin 2009, J.-Y. Lafesse et autres c/ Google et autres, legalis. net.

la poursuite d'un cybercriminel lorsqu'il opère avec une connexion privée. La police peut le localiser à partir de l'adresse IP. Alors il peut être interpellé et arrêté aux fins de répondre de ses actes de la cybercriminalité perpétrés à l'étranger sur le fondement de la réciprocité d'incrimination. L'absence de réciprocité des systèmes juridiques est également un obstruction à la poursuite du cybercrime, et l'extension américaine de l'affaire Yahoo! en a donné une illustration éloquente.

B) La spécification de la loi applicable

En droit béninois, la loi pénale s'applique par principe à toutes les infractions commises sur le territoire national indépendamment de la nationalité de l'auteur ou de la victime[95]. La finalité est d'assurer l'ordre sur le territoire national. La législation béninoise admet une extension du principe de la territorialité de la loi pénale. Cette possibilité lui permet de s'appliquer à partir du moment où seulement l'un des éléments constitutifs de l'infraction se réalise sur le territoire national[96]. Il convient d'analyser la loi applicable aux infractions de cybercriminalité commises sur le territoire de la République (1) et la loi applicable aux infractions liées à la cybercriminalité commises hors du territoire de la République (2).

1) La loi applicable aux cyber infractions territoriales

La prolifération des textes juridiques relatifs à la cybersécurité est une réalité commune au sein de l'espace francophone. En effet, l'écart manifeste entre les pays ayant en partage l'usage du français dans le passage au modèle de la société d'information est partiellement comblé au niveau du cadre juridique de la cybersécurité. Le code du numérique en république du Bénin s'applique aux infractions de la cybercriminalité commises sur le territoire de la république[97]. La République de la Côte d'ivoire a institué une loi du 19 juin 2013 relative à la lutte contre la cybercriminalité[98]. La république Togolaise a également institué une loi n° 2018-026 sur la cybersécurité et la

[95]Article 10 al. 1er de la loi n° 2018-16 portant code pénal en République du Bénin « La loi pénale est applicable aux infractions commises sur le territoire de la République du Bénin ».
[96]Article 10 al. 2 de la loi n° 2018-16 portant code pénal en République du Bénin « L'infraction est réputée commise sur le territoire de la république du Bénin dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire ».
[97]Loi n° 2017-20 portant code du numérique en République du Bénin
[98]Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité publiée au journal officiel de la république de côte d'ivoire le 12 août 2013.

lutte contre la cybercriminalité[99].La république sénégalaise a institué une loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité[100]. Il en découle que la loi applicable aux infractions de la cybercriminalité commises sur le territoire de chaque Etat de l'espace de la CEDEAO est la loi de l'Etat du lieu de la perpétration de l'infraction liée à la cybercriminalité.

L'article 10 du Code pénal béninois dispose que « la loi pénale française est applicable aux infractions commises sur le territoire de la République. L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire ». La loi pénale béninoise est aussi applicable à quiconque s'est rendu coupable sur le territoire de la République, comme complice, d'un crime ou d'un délit commis à l'étranger si le crime ou le délit est puni à la fois par la loi béninoise et par la loi étrangère et s'il a été constaté par une décision définitive de la juridiction étrangère[101]. Il s'agit de la règle de la double incrimination[102].

2) La loi applicable aux cyber infractions commises hors du territoire

La république du Bénin considère que l'infraction a été commise sur internet sur le territoire de la République du Bénin dès lors que le contenu illicite est accessible depuis la République du Bénin[103]. Il en résulte que les juridictions béninoises sont même compétentes pour connaitre des infractions liées à la cybercriminalité commises hors du territoire. Dès lors qu'elles sont compétentes en raison de l'accessibilité du contenu illicite depuis la république du Bénin, le code du numérique en république du Bénin est applicable[104]. Les juridictions béninoises sont également compétentes lorsque l'auteur ou la victime est de nationalité béninoise si l'infraction liée à la cybercriminalité est commise hors du territoire béninois[105]. Alors le code numérique est applicable lorsque le présumé coupable ou la victime est béninoise

---

[99]Loi n°2018-026 sur la cybersécurité et la lutte contre la cybercriminalité de la république togolaise.
[100]Loi n°2008-11 du 25 janvier 2008 portant sur la Cybercriminalité de la république sénégalaise.
[101]Article 14 précité de la loi n° 2018-16 du 28 décembre 2018 portant code pénal en république du Bénin.
[102]C. CASTETS-RENARD, « *Droit de l'internet : Droit français et européen* », 2ème éd. 2012, n° 1013, p. 401.
[103]Article 597 alinéa 1 de la loi n° 2017-20 portant code du numérique en République du Bénin
[104]Loi n° 2017-20 portant code du numérique en République du Bénin
[105]Article 597 alinéa 4 de la loi n° 2017-20 portant code du numérique en République du Bénin

si l'infraction liée à la cybercriminalité est commise sur hors du territoire.

Le choix de la loi applicable aux infractions commises hors du territoire dans le monde matériel ne pose aucun problème. En effet, lorsque les infractions sont commises hors du territoire de la République, la loi béninoise est susceptible de s'appliquer lorsque l'auteur de l'infraction ou la victime est béninoise[106].

Dans le monde immatériel, il y a lieu d'admettre que les infractions liées à la cybercriminalité sont commises à la fois sur le territoire français et à l'étranger[107]. La loi pénale béninoise est applicable à quiconque s'est rendu coupable sur le territoire de la République, comme complice, d'un crime ou d'un délit commis à l'étranger si ce crime est puni par la loi béninoise et par la loi étrangère et s'il a été constaté par une décision définitive de la juridiction étrangère »[108]. Cette disposition vise les infractions liées à la cybercriminalité commises à la fois sur le territoire béninois et à l'étranger. Ainsi, « la loi pénale béninoise est applicable à tout crime commis par un béninois ». Elle est applicable aux délits commis par des béninois hors du territoire de la République si les faits sont punis par la législation du pays où ils ont été commis[109]. L'article 639 alinéa 5 du code béninois de procédure pénale que « La loi pénale béninoise est applicable à tout crime, ainsi qu'à tout délit puni d'emprisonnement, commis par un béninois ou par un étranger hors du territoire de la République lorsque la victime est de nationalité béninoise au moment de l'infraction ».

---

[106]Article 639 alinéa 5 de la loi n° 2012-15 du 18 mars 2013 portant code de procédure pénale en république du Bénin « La nationalité béninoise de la victime d'une infraction commise à l'étranger ou celle de ses ayants-droits attribue compétence aux lois et aux juridictions nationales ».

[107]M. QUEMENER Y. CHARPENEL, *op.cit.*, n° 705, p.158.

[108]L'article 640 de la loi n° 2012-15 du 18 mars 2013 portant code de procédure pénale en république du Bénin « Quiconque s'est, sur le territoire de la République rendu complice d'un crime ou d'un délit commis à l'étranger, peut être poursuivi et juge par les juridictions béninoises, si le fait est puni a la fois par la loi étrangère et par la loi béninoise, a la condition que le fait qualifie crime ou délit soit et constaté par une décision définitive de la juridiction étrangère ».

[109]Article 639 alinéa 5 de la loi n° 2012-15 du 18 mars 2013 portant code de procédure pénale en république du Bénin.

II) La recherche des preuves et la responsabilité pénale

La convention du Conseil de l'Europe sur la cybercriminalité, signée le 23 novembre 2001 à Budapest, reste à ce jour le seul instrument international contraignant en matière de lutte contre la cybercriminalité[110]. Un deuxième protocole additionnel à cette convention est en cours de rédaction depuis septembre 2017, et envisage de simplifier la coopération judiciaire entre les 63 pays adhérents à la convention et de faciliter la coopération directe avec les fournisseurs de services sur internet des autres pays membres[111]. Donc la lutte contre la cybercriminalité nécessite une coopération judiciaire internationale en vue de déroger au principe de la territorialité de la loi pénale. Cette coopération judiciaire internationale est justifiée par l'internationalité de la cybercriminalité, assurant la réunion des preuves dans l'espace immatériel[112]. En conséquence, elle permet déterminer de la responsabilité pénale des acteurs de la cybercriminalité. Il convient d'analyser les modalités et les caractéristiques des preuves numériques (A) et la responsabilité pénale internationale (B).

A) Les modalités et les caractéristiques des preuves numériques

Au niveau régional, la volonté de l'Union d'instaurer un espace de sécurité, de liberté et de justice l'a amené à créer une coopération policière et judiciaire en matière pénale[113]. Basée sur le principe fondamental de reconnaissance mutuelle des décisions et jugements entre les Etats membres, cette coopération assure la facilité entre les Etats la communication des éléments de preuve par dérogation à la souveraineté de chaque Etat. Il convient d'analyser la recherche preuves numériques dans le cyberspace (1) et les garanties de fiabilité des preuves numériques (2).

---

[110]H. SOLOMON « La convention de Budapest sur la cybercriminalité à 20 ans », le 11 novembre 2021, https://www.directioninformatique.com/la-convention-de-budapest-sur-la-cybercriminalite-a-20-ans/90060

[111]*Ibid*

[112]Article 32 de la directive C/DIR/1/08/11 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO, soixante sixième session ordinaire du conseil des ministres Abuja, 17-19 août 2011 stipule « L'écrit électronique est admis comme preuve en matière d'infraction à condition que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».

[113]Article 82-2-a du TFUE

1) La recherche des preuves numérique dans le cyberespace

Le critère de l'internationalité des infractions liées à la cybercriminalité implique que l'on déroge au principe de territorialité de la loi pénale dans la collecte des preuves numériques. Le critère *ratione loci*, permettant de rechercher et de saisir sur mandat[114] les données stockées sur le territoire béninois, et le critère *ratione personae*, permettant de faire de même pour toutes données détenues par une personne soumise à la loi béninoise du fait de sa nationalité, de sa résidence ou de son immatriculation au registre du commerce (donc indépendamment du lieu de résidence pour les personnes morales)[115]. Cette solution répondrait à la faiblesse de la compétence fondée sur la seule accessibilité aux données : le principe même d'internet permet à toute personne située à n'importe quel endroit du monde d'accéder à ses données. Ainsi, toutes les autorités judiciaires, de n'importe quel État, seraient compétentes pour accéder à toute donnée, peu importe son lieu de situation. Cette solution serait dangereuse pour les libertés individuelles. En revanche, la propriété des données a encore un sens en matière de technologie informatique, si bien que soumettre l'accès non consenti aux données par les enquêteurs à la loi à laquelle est soumise la personne les détenant semble malgré tout constituer un bon compromis, reste à voir comment une telle solution serait mise en œuvre[116]. Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire béninois, sont utiles à la manifestation de la vérité, le juge d'instruction peut opérer une perquisition ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique ou un support et aux données présentes dans ces derniers dès lors que ces données sont accessibles à partir du système initial ou disponible pour le système initial[117]. S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponible pour le système initial, sont stockées dans un autre système informatique situé à l'étranger, elles sont recueillies par le juge d'instruction, par voie de commission rogatoire internationale[118].

[114]Étant précisé qu'il n'existe pas de mandat de perquisition en droit français, la solution, si elle devait inspirer le droit français, s'appliquerait à l'ordonnance du juge des libertés et de la détention ou à la commission rogatoire du juge d'instruction. Il en est de même pour le droit béninois.

[115]A. ROUSSELET-MAGRI «Les perquisitions informatiques à l'épreuve du principe de souveraineté, dans un contexte de mondialisation du stockage de données », étude comparée en droit français et états-unien, in revue de science criminelle et de droit comparé 2017/4 p.675.

[116]*Ibid.*

[117]Article 587 al 1[er]de la loi n°2017-20 portant code du numérique en République du bénin

[118]Article 587 alinéa 2 de la loi n° 2017-20 portant code du numérique en république du bénin

2) Les garanties de fiabilité des preuves numériques

Pour avoir une valeur probante, l'information numérique doit présenter des garanties de fiabilité qui correspondent à deux groupes de conditions : les conditions générales et les conditions spécifiques. Les conditions générales incluent l'idée que l'information numérique, comme tout élément de preuve, soit recevable et en lien direct avec les faits en l'étude. Une information numérique est recevable devant une juridiction pénale lorsqu'elle a été recueillie dans les conditions de légalité, c'est-à-dire lorsque les principes de dignité, de loyauté, de proportionnalité et/ou de nécessité ont été rigoureusement observés par les enquêteurs. Pour rappel, le principe de dignité renvoie à l'absence d'emploi de la violence par les agents enquêteurs pendant de la collecte des éléments de preuve. La jurisprudence française est intransigeante sur cette question de dignité. Dans une décision de 2010 portant sur une question prioritaire de constitutionnalité, le Conseil constitutionnel a notamment rappelé cette valeur constitutionnelle. Il a précisé que « *la protection des droits et libertés constitutionnellement garantis, au nombre desquels figurent le respect de la vie privée, protégé par l'article 2 de la Déclaration de 1789, le respect de la présomption d'innocence, le principe de dignité de la personne humaine, ainsi que la liberté individuelle que l'article 66 place sous la protection de l'autorité judiciaire* »[119].

La loyauté, quant à elle, est la conformité aux règles de la procédure. Dans le cadre d'une enquête judiciaire, elle consiste pour les enquêteurs à ne pas provoquer à la commission de l'infraction. La doctrine la conçoit comme « une manière d'être de la recherche de la preuve conforme au respect des droits de l'individu et à la dignité de la justice »[120]. Ce principe de la sincérité de la preuve est valable tant pour les enquêteurs que pour les magistrats[121]. Il a été rappelé plusieurs fois par la Cour de cassation notamment dans l'arrêt Schuller en 1996, dans lequel elle a solennellement affirmé que n'était pas admissible une preuve procédant d'une "machination de nature à déterminer les agissements délictueux et que, par ce stratagème, qui a vicié la recherche et l'établissement de la vérité, il a été porté atteinte au principe de la loyauté des preuves"[122]. En effet, de nouvelles

[119]Conseil constitutionnel, 16 septembre 2010, QPC 2010-25

[120]P. Bouzat, «La loyauté dans la recherche des preuves», Mélanges Hugueney, 1964, p. 155.

[121]Cass. crim., 12 juin 1952, Bull. n° 153

[122]Cass. crim., 27 fév. 1996, bull. crim., n° 93 , Voir aussi Cass., crim., 4 juin 2008, Bull. crim. n°41 et Cass. crim., 11 juillet 2017, n° 17-80313

législations sont venues assouplies ce principe en instaurant des dispositions dérogatoires à l'égard de la criminalité transfrontalière dont les preuves sont souvent difficiles à collecter. C'est le cas de la loi dite Perben II du 09 mars 2004 qui a étendu le régime de l'infiltration d'agents dans les organisations afin d'inciter à la preuve. Il y a également la loi LOPPSI 2 qui intervient dans ce domaine. En revanche, à la faveur des particuliers ou les justiciables, contrairement à la jurisprudence de la chambre civile qui maintient une position constante sur le refus de productions des preuves recueillies illicitement, la déloyauté dans la collecte de la preuve en droit pénal est admise à la condition que ces preuves seront débattues et que l'exercice du droit de la défense sera pleinement respecté[123]. Le principe de proportionnalité implique que les moyens de preuve employés ne sont pas en disproportion avec l'infraction poursuivie, afin de protéger la vie privée des personnes. A défaut du respect de ces principes, les éléments de preuves recueillis seront frappés de nullité.

En outre, toujours au titre des conditions générales, il apparait également important que les indices de preuve recueillis soient en lien direct avec les faits sur lesquels porte une poursuite. Une telle évidence se justifie au regard notamment d'une bonne administration de la justice. Ce critère de lien direct est formulé de diverses manières tant en droit interne que dans la convention. La convention de Budapest parle de « données relatives au trafic[124] », qu'elle désigne par « toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ». A l'analyse, l'usage du terme « trafic » est embarrassant dans la proportion où il n'éclore pas précisément le lien direct avec une enquête de cybercriminalité. Littéralement, cette formule utilisée par les rédacteurs de la Convention met en lumière les informations relatives à une communication enregistrée lors de la surveillance électronique[125]. De plus, au Bénin l'information numérique pour avoir

[123]Cass. crim., 15 juin 1993, Bull. 210 : « ... la circonstance que des documents ou des enregistrements remis par une partie ou un témoin aient été obtenus par des procédés déloyaux ne permet pas au juge d'instruction de refuser de les joindre à la procédure, dès lors qu'ils ne constituent que des moyens de preuve qui peuvent être discutés contradictoirement ; que la transcription de ces enregistrements, qui a pour seul objet d'en matérialiser le contenu, ne peut davantage donner lieu à annulation ».

[124]Article 16 de la convention de Budapest

[125]Article 1 de la convention de Budapest. Le Bénin a signé cette convention.

une valeur probante, doit présenter des garanties spécifiques telles que l'intégrité[126], la traçabilité et l'authenticité. L'intégrité renferme l'hypothèse où le contenu de l'information n'a pas été modifié. L'authenticité tient à la fiabilité de l'origine de l'information, et la traçabilité met en exergue le fait que le procédé technique de la collecte des données doit permettre d'établir les différentes opérations techniques qui ont pu être réalisées jusqu'à la conservation des éléments de preuve. Certains auteurs ajoutent un autre critère qui est celui de la pérennité[127] de l'information, mettant ainsi en lumière la qualité de la preuve dans le temps.

B) La responsabilité pénale internationale

La responsabilité pénale d'un auteur présumé d'une infraction conditionne l'existence d'une faute pénale, l'imputation de cette faute pénale à une personne physique ou une personne morale[128]. La répression d'une infraction conditionne l'existence d'un élément légal, d'un élément matériel, et d'un élément moral. Le principe de territorialité de la loi pénale constitue un obstacle à la poursuite internationale des cybercriminels. Mais la détermination de la responsabilité pénale internationale des cybercriminels nécessite des mécanismes visant à faciliter la poursuite judiciaire et l'extradition des prévenus vers les Etats victimes. Il convient d'analyser la coopération internationale et l'entraide pénale (1) et l'extradition des prévenus vers les Etats victimes (2).

---

[126]Article 268 de la loi n° 2017-20 portant code du numérique en république du bénin « La preuve sous forme électronique a la même force probante et est admise au même titre que la preuve sous forme non-électronique, sous réserve que puisse être identifiée la personne dont elle émane, et qu'elle soit établie et conservée dans des conditions qui en garantissent l'intégrité et la pérennité ».

[127]Ibid

[128]Article 17 et suivants de la loi n° 2018-16 du 28 décembre 2018 portant code pénal en république du Bénin « Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement, selon l'un des modes de participation criminelle prévue par le présent code, des infractions commises pour leur compte, par leurs organes ou leurs représentants. Toutefois, les entités territoriales décentralisées ne sont responsables pénalement que des infractions commises dans l'exercice d'activités susceptibles de faire l'objet de conventions de délégation de service public. La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques, auteurs ou complices des mêmes faits, sous réserve des dispositions du quatrième alinéa de l'article 19. Sont pénalement responsables de l'infraction les seuls membres de la personne morale par la volonté et ou dans l'intérêt desquels les faits ont été commis. Lorsque la responsabilité de la personne morale est engagée exclusivement en raison de l'intervention des personnes physiques identifiées, seule la personne physique qui a commis la faute la plus grave peut être condamnée ». Voir également l'article 4 de la loi n° 2017-20 portant code du numérique en République du Bénin « Les personnes morales autres que l'Etat, les collectivités locales et les établissements publics sont responsables des infractions prévues par les dispositions du présent Livre

1) La coopération internationale et l'entraide pénale

Elle revêt en matière de cybercriminalité une importance cruciale parce que la lutte contre ce type de délinquance internationalisée répond à un besoin commun des Etats[129]. La nécessité de poursuivre les acteurs de la cybercriminalité dans le monde se heurte au principe de territorialité de la loi pénale. La solution pour assurer la répression des cyberdélinquants est d'assurer l'extension du principe de territorialité de la loi pénale. Cette extension ne peut se faire que lorsqu'il est mis en place une coopération internationale de lutte contre les infractions relatives à la cybercriminalité.

La dimension internationale est essentielle dans la lutte contre la cybercriminalité, compte tenu de l'extranéité des cyberattaques. En 2020, le parquet spécialisé en cybercriminalité de Paris a relevé une hausse très importante du nombre de demandes d'entraide internationale sortantes, attestant du caractère décisif de la coopération pénale internationale en matière de cybercriminalité. La lutte contre la cybercriminalité nécessite une coopération internationale efficace en vue d'assurer la préservation des données, la mise en place de techniques spéciales d'enquêtes comme l'interception ou la captation, le rapprochement *à partir d'indices de compromission ou encore l'échange de pratiques. Intensifier les compétences techniques et accompagner nos partenaires étrangers spécialisés en matière de cybercriminalité nous permet de contribuer à une plus grande efficacité dans l'exécution des demandes d'entraide pénale, qui sont essentielles au succès des enquêtes. Les échanges opérationnels jouent un rôle central dans la lutte contre la cybercriminalité, sur le plan national et international*[130].

La convention du Conseil de l'Europe de 2001 sur la cybercriminalité (la «convention de Budapest») est le premier traité international sur la question; elle définit des infractions liées à la cybercriminalité, prévoit une série de pouvoirs et de procédures pour enquêter sur les

---

lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé : 1- sur un pouvoir de représentation de la personne morale ; 2- sur une autorité pour prendre des décisions au nom de la personne morale ; 3- sur une autorité pour exercer un contrôle au sein de la personne morale».

[129]B. PEREIRA « *La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité* ». Revue internationale de droit économique, 2016/ 3 t. XXX, n°3 p.402

[130]https://www.enm.justice.fr/actu-31052021-cybercriminalite-l-enm-agit-pour-la-cooperation-internationale, consulté le 16/06/2022.

actes de cybercriminalité, comme la perquisition de réseaux informatiques et l'interception de données, et pour obtenir des preuves électroniques concernant toute forme de criminalité, et elle instaure un cadre de coopération internationale[131]. La directive C/DIR/1/08/11 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO prévoit des règles de procédure en matière de perquisition[132] et de mode de preuve[133]. Le Code numérique de la République du Bénin prévoit des perquisitions des données stockées dans un système informatique[134] et des modes des preuves des infractions liées à la cybercriminalité[135]. Les perquisitions ne peuvent avoir lieu qu'avec le consentement exprès de la personne chez qui l'opération a lieu[136]. Cependant, si l'enquête est relative à un crime ou un délit puni de plus de cinq ans de peine d'emprisonnement ou si la recherche de biens le justifie, le juge d'instruction peut, sur autorisation écrite, décider que la perquisition et la saisie seront effectuées sans l'assentiment de la personne[137].

La convention de Budapest étant ouverte aux États non-membres du Conseil de l'Europe, des pays de toutes les régions du globe y ont adhéré. Aujourd'hui 66 États y sont parties tandis que quatorze autres pays ont été invités à y adhérer. Cette convention sert de fondement à la législation de lutte contre la cybercriminalité dans 80 % des pays du monde. L'adoption, le 17 novembre 2021 par le Comité des Ministres du Conseil de l'Europe, d'un deuxième protocole additionnel

---

[131]L'Union a adopté des règles communes qui coïncident avec plusieurs éléments envisagés pour cette convention. Ces règles communes consistent en un ensemble complet d'instruments relatifs au droit pénal matériel, à la coopération policière et judiciaire en matière pénale, aux normes minimales en matière de droits procéduraux, et aux garanties en matière de protection des données et de la vie privée. Il conviendra de tenir également compte de futures règles communes.

[132]Article 33 de la directive C/DIR/1/08/11 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO, soixante sixième session ordinaire du conseil des ministres Abuja, 17-19 août 2011 stipule « Les autorités nationales compétentes peuvent opérer des perquisitions ou saisies ou accéder à tout système informatique pour la manifestation de la vérité Toutefois, lorsque la saisie du support électronique ne paraît pas souhaitable, les données, de même que celles qui sont nécessaires à la compréhension du système, font l'objet de copies sur des supports de stockage informatique et sont placés sous scellés ».

[133]Article 33 de la directive C/DIR/1/08/11 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO, soixante sixième session ordinaire du conseil des ministres Abuja, 17-19 août 2011 stipule « L'écrit électronique est admis comme preuve en matière d'infraction à condition que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».

[134]Article 587 du Code numérique de la République du Bénin

[135]Article 590 du code précité

[136]Article 589 alinéa 1er du code précité

[137]Article 589 alinéa 2 du code précité

à la convention de Budapest montre que cette convention conserve toute sa pertinence en tant que cadre de coopération internationale en matière de cybercriminalité[138]. Cette coopération permettra d'extrader les auteurs et complices des actes de cybercriminalité pour être jugé dans un Etat ayant formulé leur extradition. Les suspects accusés n'auront plus la possibilité d'opposer à l'Etat requérant le respect du principe de territorialité de la loi pénale et son incompétence juridictionnelle.

2) L'extradition des prévenus vers les Etats victimes

Le problème de la localisation de l'infraction pose indéniablement celui relatif à la compétence[139].Cette dernière soulève d'autres problèmes de coopération. Pour preuve, la comparution de l'auteur d'une infraction localisée à l'étranger est assez délicate dans la mesure où elle doit prendre la décision de l'extrader ; ce qui n'est pas toujours facile en raison de l'existence d'obstacles divers. En effet, la nationalité de l'auteur de l'infraction peut poser problème en ce sens qu'elle jouera beaucoup dans l'emploi de cette procédure. L'Etat requis refusera de s'exécuter surtout lorsque la demande d'extradition visera ses nationaux. Bon nombre de conventions d'extradition et de lois nationales admettent cette attitude comme règle[140]. La Convention[141] de la CEDEAO relative à l'extradition conditionne l'extradition d'un national de l'Etat requis à la discrétion de ce dernier. En cas de refus d'extrader, les juridictions de l'Etat requis peuvent être saisies pour ce faire à la demande de l'Etat requérant[142].

En plus de la nationalité, le lieu de perpétration de l'infraction peut constituer un empêchement à la poursuite. L'Etat requis peut refuser d'extrader l'individu réclamé lorsque l'infraction a été commise en tout ou partie de son territoire, même s'il n'est pas son national. L'Etat peut en outre refuser l'extradition si l'infraction servant la cause de

[138]Par conséquent, une nouvelle convention internationale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles est susceptible d'affecter des règles communes de l'Union ou d'en altérer la portée.

[139]La difficulté relative à la compétence concerne la juridiction habilitée à connaître de l'affaire. Le problème peut se poser quant à sa saisine aussi bien au plan interne qu'au niveau international.

[140]Pour éviter l'impunité, certaines conventions prévoient une parade en admettant la possibilité de soumission de l'affaire à l'Etat requis s'il s'agit de son national qui est visé. L'Etat requérant doit en faire la demande.

[141]La convention de la CEDEAO relative à l'extradition a été adoptée en juillet 1994.

[142]Voir article 10 de la Convention de la CEDEAO relative à l'extradition.

cette demande a été commise en dehors du territoire de l'Etat requérant, alors que la législation de l'Etat requis n'autorise pas la poursuite d'une infraction de la même nature commise en dehors de son territoire[143]. Cette dernière situation montre la difficulté d'implémentation de la compétence universelle pour les juridictions des Etats qui s'investissent de cette mission à l'égard des infractions classiques. Ce type de compétence est-il nécessaire et envisageable au niveau ouest-africain à l'égard des infractions de cybercriminalité ? Les infractions de cyber crimes se produisant sur le réseau Internet s'étendent fréquemment sur plus d'un pays et nécessitent le concours d'autres Etats pour leur poursuite. Les règles classiques de réalisation de l'extradition ne sont pas aptes à favoriser la poursuite des auteurs de ces infractions qui se distinguent par leur internationalité. Les normes anciennes concourent à l'entretien de cyberparadis et l'institution de l'impunité. Néanmoins, *le gouvernement américain a annoncé le 23 mai 2022, l'extradition d'un nigérian, Chibundu Anuebunwa, un suspect accusé d'une escroquerie de plusieurs millions de dollars par compromis de messagerie commerciale*[144]. M. Anuebunwa a été extradé du Royaume-Uni pour faire face à des accusations criminelles aux Etats-Unis. M. Anuebunwa y compris ses complices ont été accusés d'avoir commis le crime entre 2014 et 2016 ; en participant prétendument à des escroqueries par compromission des e-mails professionnels (« escroqueries BEC ») qui ont ciblé des milliers de victimes dans le monde, y compris aux Etats-Unis[145]. Dès lors que les auteurs et complices des infractions de cyber crimes sont connus, les Etats victimes peuvent demander leur extradition du pays de la perpétration des cybercrimes vers eux pour y être jugés. L'affaire d'extradition de M. Anuebunwa vers les Etats-Unis en est illustrative. Les auteurs et complices de la cybercriminalité n'échappent plus véritablement à des poursuites judiciaires grâce à la coopération internationale des Etats, aux traités multinationaux portant sur l'extradition. En effet, longtemps ignorée du fait de sa dimension immatérielle, la cybercriminalité a aussi souvent été considérée en Afrique de l'Ouest comme un fléau qui touchait d'abord les pays développés en raison de leur forte

[143]Voir art.11 de la Convention de la CEDEAO relative à l'extradition.
[144]https://www.justice.gov/usao-sdny/pr/nigerian-man-extradited-united-kingdom-participating-business-email-compromise-scams
[145] Idem

connectivité[146]. Mais le caractère souvent transfrontalier des cyber infractions rend ainsi obligatoire l'harmonisation des textes et la signature d'accord bilatéraux permettant l'extradition d'un pays à l'autre des cybercriminels[147].Certains pays de la CEDEAO ont se sont dotés d'une loi réprimant la cybercriminalité. En parallèle des travaux relatifs à ces conventions internationales, les Etats de la CEDEAO ont adopté, lors d'une session ordinaire les 17 et 18 août 2011 à Abuja au Nigéria, une directive sur la lutte contre la cybercriminalité dans l'espace de la CEDEAO[148]. Cette directive s'applique à toutes les infractions relatives à la cybercriminalité dans l'espace CEDEAO, ainsi qu'à toutes les infractions pénales dont la constatation requiert la collecte d'une preuve économique[149].

La mise en œuvre des règles de l'extradition nécessite également l'observation d'un principe fondamental qui revient couramment dans les conventions de coopérations pénales internationales. Il s'agit du principe de la double incrimination. Ce principe peut poser un problème dans la poursuite de l'infraction en cas de la localisation de son auteur à l'étranger. Ce principe impose que l'acte soit pénalement qualifié aussi bien par l'Etat requérant que par celui requis. Le texte communautaire ouest-africain relatif à l'extradition pose ce principe de double incrimination de l'acte à la base de la demande d'extradition. Il en ressort que la double incrimination suppose l'incrimination de l'acte par les deux Etats d'une part, et d'autre part, l'existence d'un minimum de peine privative de liberté de deux ans[150]. Le risque d'impunité de l'acte répréhensible est grand lorsqu'il n'est pas incriminé par l'Etat sollicité dans le cadre de la coopération[151]. Bon nombre d'Etats ouest-africains n'ont pas encore adopté une législation contre les cybercriminels[152]. Il est alors très difficile de poursuivre certains

[146]« L'Afrique et la cybercriminalité : le cas du Sénégal », http://www.dakaractu.com/L-Afrique-et-lacybercriminalite-Le-cas-du-Senegal_a115493.html, dakar actu, consulté le 17 août 2016.

[147]J. Dechanet, M. Ludmann, C. Rossi *« Afrique de l'ouest : le défi de la cybersécurité* », *op.cit*., p. 24.

[148]J. Dechanet, M. Ludmann, C. Rossi, *op.cit*., p. 26.

[149]« Lutte contre la cybercriminalité - 15 pays de l'Afrique de l'Ouest harmonisent leurs législations », http://www.balancingact-africa.com/news/fr/issue-no-177-23-f-vr/177/actualit-s-internet/lutte-contre-la-cybe/fr, Balancing Act, consulté le 20 mars 2016.

[150]Art. 3 de la Convention de la CEDEAO relative à l'extradition.

[151]Même le non-national de l'Etat requis bénéficie de cette protection qu'offre le principe de double incrimination de l'infraction.

[152]Jusqu'à présent, le Nigéria n'a pas encore transformé son projet de loi en loi. Le 25 mars 2022, la Cour régionale de l'Afrique de l'Ouest a rendu son arrêt stipulant que la loi nigériane portant sur la cybercriminalité devait être conforme à la Charte africaine des droits de l'homme et des peuples (CADHP) et au Pacte international relatif aux droits civils et politiques (PIDCP).

actes cybercriminels dans le cadre d'une coopération. Cette réalité est une grande tare des législations face à cette nouvelle forme de délinquance qui se produit dans un espace international. Par ailleurs, la flexibilité des peines privatives de liberté au sein de la législation du Ghana pour les infractions de cybercriminalité est-elle de nature à favoriser la poursuite internationale des infracteurs ? La faiblesse des peines privatives de liberté est incompatible avec la Convention de la CEDEAO qui conditionne l'extradition de personnes sollicitées à l'existence d'une peine d'un minimum de deux ans. Il est alors évident que cette convention ne sera pas opérationnelle à l'égard des infractions sanctionnées par une peine privative de liberté dont le minimum n'atteint pas les deux ans.

CONCLUSION

La cybercriminalité, mondiale par nature, Internet permet aux délinquants de se livrer à presque n'importe quelle activité illicite. Il est donc essentiel que toutes les infractions commises dans le cyberspace ne demeurent pas hors d'atteinte. Il existe une variété d'infractions de cybercriminalité. Mais les infractions liées à la cybercriminalité sont constituées des celles commises au moyen de réseau d'internet. La répression de ces infractions est conditionnée par l'existence d'éléments légal, matériel, et intentionnel. Dès lors que ces éléments sont réunis pour la commission d'une infraction de la cybercriminalité, la responsabilité pénale des auteurs et complices est engagée. Les auteurs et complices de la cybercriminalité n'échappent plus aux poursuites judiciaires. La coopération internationale et les conventions portant sur l'extradition favorisent les poursuites judiciaires. Il n'y a plus d'obstacle en matière des recherches de preuves établissant la responsabilité pénale internationale des auteurs et complices de la cybercriminalité. L'entraide judiciaire internationale contribue à la recherche des preuves. L'adresse IP permet finalement de retrouver l'auteur des infracteurs de la cybercriminalité. L'extension du principe de la loi pénale en matière de la cybercriminalité constitue une innovation du droit en matière des droits des nouvelles technologies et de l'informatique. Les infractions de cybercriminalité sont réprimées par loi de la République lorsque ces infractions sont commises à la fois sur le territoire et à l'étranger. Les juridictions sont compétentes lorsque les faits constitutifs des infractions sont commis à l'étranger ou ses faits de complicité sont commis sur le territoire. Les juridictions de la République sont aussi compétentes par la réciprocité d'incrimination.

RENSEIGNEMENTS

1 - REDACTION / ADMINISTRATION

Diffusion / Abonnements
S'adresser à Théodore HOLO
B.P. 990 COTONOU
(République du Bénin)

2 - CONDITIONS DE VENTE

Prix du numéro : 3 000 F CFA
Abonnement annuel : - Bénin : 6 000 F CFA
Etranger (AVION) :

- Afrique Noire : 12 000 F CFA
- France : 25 000 F CFA
- Europe : 30 000 F CFA
- Autres pays : 40 000 F CFA

3 - COMPTE BANCAIRE DE LA REVUE

BANK OF AFRICA
Compte : N° 015 11 72948
Cotonou (République du Bénin)

Directeur de la Publication : Théodore HOLO

Dépôt Légal N° 2831
4ème trimestre 2008