Brainae Journal of Business, Sciences and Technology
ISSN "2789-374X (print)" "2789-3758 (online)
Volume 26, Issue 6, Juin 2023
http://www. brainajournal.com info@brainae.org

CYBERCRIMINALITE : L'AFRIQUE EST-ELLE UN NO MAN'S LAND JURIDIQUE ?
Esquisse d'une Approche Holistique : cas du Gabon.

Par
Dr. Christ Hermann POUNAH
Doctorat/PHD en Droit, Maître Assistant
Mobile +241 77474400
E-mail : hermannchrist@gmail.com

A reçu : 09 Mai, 2023 ; **Accepté** : 29 Mai, 2023 ; **Publié :** 06 Juin 2023

Résumé

L'usage des Technologies de l'Information et de la Communication (TIC), particulièrement de l'Internet, s'est mué en question d'importance stratégique pour l'ensemble des pays du globe.

En effet, un Internet libre, dynamique, ouvert et sécurisé représente à n'en point douter, un moteur de croissance économique et de développement social à même de faciliter la communication, l'innovation, la recherche scientifique et la transformation de nombreux secteurs d'activité.

Cependant, la croissance exponentielle d'Internet a inévitablement conduit à de nouveaux défis pour la communauté mondiale. Tant que les sociétés s'interconnecteront, plus les vulnérabilités et les menaces cybernétiques émergeront avec leur lot d'activités et de menaces criminelles que sont la cybercriminalité et la criminalité informatique. S'il est plus que jamais nécessaire de veiller sur la sécurité des populations, il sied également de veiller à ce que la sécurité des infrastructures critiques soit régulièrement améliorée afin de maintenir leur intégrité et leur fiabilité ainsi que la confiance des utilisateurs.

Cela passe indubitablement par la mise à jour des arsenaux législatifs des Etats, afin de les adapter aux fluctuations incessantes du réseau Internet, mais également par l'élaboration de législations communes transnationales, « fer de lance » d'une coopération juridique internationale capable de véritablement juguler ce fléau.

Mots-clés : Technologie de l'information, Internet, cybercriminalité, criminalité informatique, arsenaux législatifs.

Abstract

The use of Information and Communication Technology (ICT), particularly the Internet, has become a matter of strategic importance for all countries of the world. Indeed, a free, dynamic, open and secure Internet undoubtedly represents an engine of economic growth and social development capable of facilitating communication, innovation, scientific research and the transformation of many sectors of the world's activity.

However, the exponential growth of the Internet has inevitably led to new challenges for the global community. As societies become more interconnected, more cyber vulnerabilities and threats will emerge with their share of criminal activity and threats such as cybercrime and computer crime. While it is more necessary than ever to ensure the safety of populations, it is also important to ensure that the security of critical infrastructures is regularly improved in order to maintain their integrity and reliability as well as user confidence.

This undoubtedly involves updating the legislative arsenals of the States, in order to adapt them to the incessant fluctuations of the Internet network, but also by drawing up common transnational legislation, the "spearhead" of international legal cooperation capable of truly curb this scourge.

Keywords : Information technology, Internet, cybercrime, computer crime, legislative arsenals.

1- De l'Internet

Internet[1] est le nom donné au réseau informatique mondial, qui repose sur le système d'adresses global des protocoles de communication "TCP/IP[2]". Ce système rend accessible au public des services comme le courrier électronique et le World Wide Web[3] (réseau mondial des serveurs multimédias), c'est-à-dire : un ensemble de réseaux de toutes tailles interconnectées via le protocole IP (Internet Protocol) en d'autres termes, le protocole standard qui régit les réseaux grâce à Internet.

Il faut dire qu'Internet est le plus grand réseau informatique du monde, un réseau sur lequel il est possible d'échanger des informations dans une liberté quasi absolue. Il associe ainsi des ressources de télécommunication et des ordinateurs destinés à l'échange de messages
Électroniques, d'informations multimédias et de fichiers de toutes sortes. De plus, Internet fonctionne de manière décentralisée. En effet, la gestion des différents sites se fait via des serveurs gérés par chaque Etat et selon les lois qu'il juge à même de protéger autant que possible ses concitoyens. Ainsi, la "toile" grâce à sa convivialité (utilisation de l'hypertexte) permet un usage facile, rapide, interactif et peu onéreux de l'Internet. Le Web est donc la partie la plus attractive de l'Internet et celle qui de loin l'a rendu populaire auprès des utilisateurs.

Si le Web est d'une part, un service, un moyen d'obtenir des informations en provenance de divers ordinateurs il permet également d'autre part, de commettre un certain nombre de délits et de méfaits en permettant la circulation de tout type de documents : textes, images, sons et vidéo. Le Web favorise donc à un certain degré, leur usage à des fins que le droit qualifie d'interlopes, d'illégales et contraires aux règles sensées régir nos sociétés.

Il existe de nombreux exemples de délits : diffusion auprès des enfants de photographies pornographiques ou violentes, fraude à la carte bleue, c'est-à-dire l'utilisation de votre carte par autrui sans votre consentement.

2- Criminalité tous azimuts

Aujourd'hui, la criminalité à travers les nouvelles technologies a pris un essor considérable et on ne compte plus les victimes d'actes de piratages commis tant au niveau des particuliers, des administrations publiques que des entreprises, à l'exemple de l'usage par certaines personnes mal intentionnées de logiciel pirates tels que les chevaux de Troie.

Il en va donc que contrairement à certaines idées reçues, Internet est loin d'être un univers exempt de toute application du droit même si sa spécificité est en fait, un environnement en perpétuel fluctuation, à l'intérieure duquel le droit peine à trouver ses repères. C'est d'ailleurs pour cette raison que les Etats manifestent aujourd'hui, plus que jamais, le souhait de créer un cyberespace judiciaire censé réprimer les abus de toute nature sur le Web.

Malheureusement pour ce qui est de la législation en la matière, le continent africain accuse encore au XIème siècle, un certain retard par rapport à l'occident ; la plupart des Etats africains optant pour un mimétisme législatif vis-à-vis de l'occident qui dans de nombreux domaines, bénéficie en la matière, d'une avance considérable.

Au reste, la volonté de réprimer tend à mettre en exergue les questions suivantes : quels seraient les mécanismes dont le droit plus particulièrement le droit pénal ferait usage sur la sphère Internet ? Plus encore, l'application du droit sur la cyberculture (ensemble des structures, de codes et de comportements relatifs à l'Internet) se fera-t-elle sans difficulté ?

L'amalgame de procédés et de techniques qui constituent Internet, pose de véritables problèmes quant à l'application du droit sur une culture ayant ses propres modes de fonctionnement. Il apparaît alors indispensable de décliner de façon pertinente la cybercriminalité et de faire ressortir ses multiples caractères, compte tenu du fait qu'elle peut revêtir de nombreux aspects allant des atteintes aux systèmes de traitement automatisé de données, à la possession de contenus illicites, à la diffamation et autres arnaques.

Par ailleurs, comment parler du pénal sans évoquer le côté répressif qu'il représente et la volonté qu'il nourrit de tracer un canevas d'usage du Web sans pratique répréhensible ? La tâche pourrait paraître au demeurant ardue dans la mesure où, les litiges sur Internet recouvrent un nombre conséquent d'aspects tous plus pernicieux les uns que les autres.

En outre, presque tous les litiges sur Internet peuvent prendre très vite et très facilement une dimension internationale du moins potentiellement d'où, la difficulté qu'éprouve le droit à s'appliquer comme il se doit.

[1] A l'origine, Internet fût développé par « le ministère de la Défense des Etats-Unis ce fût un projet du Pentagone qui avait pour ambition de créer un réseau devant relier entre elles toutes les entreprises travaillant pour l'armée américaine. Le concept a été inventé pendant la guerre froide, par l'agence américaine ARPA. Il permettait de sécuriser les transmissions informatiques contre les attaques nucléaires. Sa véritable naissance, date de 1974, quand Vint Cerf mit au point la norme IP. Cette norme permit de fédérer tous les ordinateurs, toutes plates-formes confondues. Ce réseau a servi par la suite d'ossature pour l'actuel réseau Internet, qui relie aujourd'hui près de 20000 réseaux locaux dispersés dans le monde avec plus de 20 millions d'utilisateurs potentiels ». www.dicodunet.com.

[2] Transmission control protocol / Internet protocol.

[3] La toile en langue anglaise.

Réseau ouvert, permettant de consulter une information de n'importe quelle région du monde, Internet ne connaît pas de frontières. La rapidité dans la circulation des données favorise cette internationalisation et partant, les difficultés inhérentes à la résolution des litiges par les Etats concernés. Il s'agit en l'espèce de sa spécificité. Le résultat est donc que chaque Etat cherche à faire prévaloir ses lois, sinon son système juridico-judicaire.

Il apparaît dès lors un fait non négligeable : la nécessité pour tous les Etats de regarder dans la même direction, afin d'éviter un amalgame au niveau de l'exercice des poursuites, de la détermination des coupables, des lieux d'infractions et même des problèmes de procédure et de territorialité.

En effet, les flux transfrontaliers de données confèrent aux infractions un caractère international. Il arrive par exemple et ceci de manière récurrente que la personne qui met en ligne l'information répréhensible reçue dans un pays donné, se trouve en fait dans un autre pays[4]. Il n'est donc pas fortuit de penser que face aux multiples dérives sur Internet, la mise en place de moyens coercitifs conséquents s'impose.

3- Observations

Le constat est malheureusement "amer". En effet, dans la plupart des législations africaines, les textes d'incrimination contenus dans les codes pénaux sont très souvent caractérisés par leur inadaptation aux spécificités de la cybercriminalité. Il arrive de manière fréquente et même, itérative que certains juges se trouvent "dépassés" par ce phénomène qu'est la cyberdélinquance dans la mesure où, il y a dans de nombreux cas une inadaptation[5] des incriminations classiques aux particularismes de la cybercriminalité.

La structure même du réseau entraîne des questions nouvelles auxquelles les réponses ont dû être ou restent à trouver. Si l'on compare les catégories classiques du droit et celles qu'il est possible de trouver à propos de l'Internet, on remarquera alors que les litiges sur Internet sont très souvent protéiformes, notamment : le non-respect du droit d'auteur (la reproduction sans autorisation du texte d'une chanson...) ; suivent les atteintes à la personnalité, telles que le non-respect de la vie privée, la diffamation, l'usage frauduleux des données à caractère personnel.

Internet peut encore être utilisé de diverses manières, par exemple pour exercer une concurrence déloyale ou attenter au droit des marques par l'entremise d'un site destiné à tromper les clients d'une entreprise. Enfin, la responsabilité contractuelle peut être mise en jeu lorsqu'il s'agit de contrats passés en ligne.

Au demeurant, il apert que l'inadaptation de certaines solutions traditionnelles élaborées pour un univers typiquement matériel à un environnement immatériel dans sa totalité, soit une constante dans le cadre des nouvelles technologies. Il y a ainsi, impossibilité de mener parfois à bien, certaines poursuites, à cause de la pluralité des intervenants et leurs complices sur ce type de plateforme mais aussi et surtout, il y a la dispersion des éléments de l'infraction qui les rendent quasiment impossible à rattacher à un territoire déterminé.

Qui plus est, la limite d'une véritable harmonisation des législations dans le cadre de la gestion du contentieux sur Internet restera un frein non négligeable, tant que les Etats n'auront pas pris leurs responsabilités à ce propos.[6] Au regard du caractère immatériel d'Internet, quelle est la réponse juridique des Etats ?

4- Arsenaux juridiques inadaptés

Il n'y a rien d'étonnant dans le fait que les Etats puissent se retrouver pris de cours par l'ascension de ce nouveau médium. Les retardataires sont nombreux, face aux menaces du cybermonde.

« Les Etats ont des arsenaux législatifs sous-développés », c'est déjà le constat que dressait déjà le rapport effectué en 2000 par le cabinet britannique Mc Connell International. Il faut relever que cette situation a très certainement évolué, mais pas sur l'intégralité du continent africain.

Sur les cinquante deux (**52**) pays étudiés à cette époque par Mc Connell, huit (**8**) avaient procédé à une révision de leurs textes. Derrière les Philippines, on trouvait les Etats-Unis et le Japon, puis l'Australie et l'Inde, car dans ce domaine, les lacunes juridiques ne trahissent pas forcément un manque de moyens et inversement.

L'intérêt de cette enquête réalisée en 2000 était de donner un aperçu global des mesures prises contre la cybercriminalité. Il faut préciser que des évolutions ont

[4] Deux affaires récentes en sont les parfaits exemples, largement diffusées par la presse généraliste, elles illustrent l'aspect du contentieux sur Internet : il s'agit des affaires Estelle Hallyday contre Valentin Lacambre, et l'affaire David Hirschman.

[5] Par exemple, le système juridique français donne entre autres la possibilité aux victimes d'actes de piratage informatique d'engager la responsabilité civile de l'auteur du piratage. Dans ce cas, il faudra impérativement démontrer une faute, un dommage et un lien de causalité, entre la faute et le dommage subi. Toutefois, la prudence s'impose dans la mesure où, une faute de la victime peut dans certaines circonstances être de nature à "édulcorer" la responsabilité du pirate en cas de sinistre informatique.

[6] S'il est par exemple possible en Belgique de poursuivre un intermédiaire qui a permis la mise en ligne et l'accès à des images à caractère pornographique, il semble malheureusement que ce ne soit pas le cas dans nombre de pays. Pr Ndiaw DIOUF : Infraction en relation avec les nouvelles technologies de l'information et de procédure pénale : l'inadaptation des réponses nationales face à un phénomène de dimension internationale, RSDA n° 2, 1998, p 67.

suivi notamment en ce qui concerne la prise de conscience sur la nécessité d'un consensus international, afin d'aboutir à une normalisation la plus étendue possible dans la façon de gérer ces affaires. Quid des législations africaines, au sein desquelles la question des moyens et mécanismes utilisés dans le cadre de la répression de la cybercriminalité se pose avec acuité ?

5- L'arrimage du continent africain

À la vue de l'ampleur prise par les TIC, notamment de l'Internet avec comme corollaire la cybercriminalité, les gouvernements africains se voient contraints aujourd'hui de n'être pas en reste de la communauté internationale, dans la répression du cybercrime.

Selon l'Union Internationale des Télécommunication (UIT), la cybersécurité est l'une des clés de la transformation numérique fiable et durable. Toutefois, il reste encore beaucoup à faire en Afrique relativement à ce segment. En effet en 2020, seuls quelques rares pays s'étaient déjà dotés d'une législation en matière de cybersécurité et seuls 19 pays disposaient déjà d'un Centre National d'Alertes Informatiques (CERT) : Afrique du Sud, Bénin, Botswana, Burkina Faso, Côte d'Ivoire, Egypte, Ethiopie, Ghana, Gambie, Kenya, Cameroun, Maroc, Maurice, Nigéria, Ouganda, Rwanda, Tanzanie, Tunisie et Zambie.

Si l'on se réfère auparavant, c'est-à-dire à l'année 2018, 13 pays seulement étaient dotés d'un CERT et l'UIT le relève dans son Global Cyber Security Index 2020. Elle explique par ailleurs, que ce type d'infrastructures « *sont nécessaires pour faire face de manière fiable aux incidents. L'absence de telles institutions et le manque de capacités nationales posent un réel problème pour répondre de manière adéquate et efficace aux cyberattaques. Les équipes nationales de réponse aux incidents informatiques jouent un rôle important dans la solution* ».

Certains pays[7] à l'instar du Sénégal adaptent leur législation au contexte actuel par la mise en place d'arsenaux juridiques à même de lutter contre la cybercriminalité. La survie de toute société dépend de sa capacité d'adaptation à son environnement, notamment sur le plan juridique ; c'est dans cette optique que s'inscrit le Gouvernement du Sénégal en allant dans le sens d'une réelle protection du cybercitoyen.

Ainsi, sous l'égide de Sénégal Numérique S.A (ancienne Agence De l'Informatique de l'Etat), une loi cadre concernant l'informatique et libertés, des textes sur la protection des données personnelles, le commerce, la signature électronique et enfin la cybercriminalité avaient été pris dès 2006. Il faut relever le fait que ce pays est depuis longtemps, à la pointe de ce qui se fait le mieux en matière de digitalisation, dans un contexte d'intensification des moyens que propose l'outil informatique et l'ensemble de ses corolaires.

Nous retiendrons par ailleurs, que sur le continent africain, le fait de ne pas mettre en place des mesures législatives de protection suffisamment coercitives pourrait constituer une faute susceptible d'atténuer ou plus grave encore, de mettre en échec une éventuelle action judiciaire à l'encontre des pirates. Le choix de l'action à entreprendre est donc avant tout une question d'appréciation.

Au regard de l'avancée fulgurante des réseaux informatiques et de l'Internet, il est impératif que le juridique suive la progression de la technique au risque de voir les Etats définitivement désarmés. Bien entendu, cette révolution ne peut être possible que par l'élaboration d'une "symbiose" réelle entre l'élément juridique et l'élément technique.

6- Perspectives

Il est possible pour chaque gouvernement, nonobstant les entraves et les insuffisances législatives, de combler le vide concédé qui, le temps passant, risque de devenir une sorte de gouffre difficile à combler. La Convention sur la cybercriminalité du 23 novembre 2001 à Budapest est un outil édifiant à cet égard. En effet, elle propose un nombre important de mécanismes et de mesures à même de juguler le phénomène. Il serait donc judicieux, voire même impérieux pour nos gouvernements de s'en inspirer.

Concernant le Gabon, il pourrait tout d'abord être question de légiférer abondamment en la matière compte tenu du retard accusé dans ce domaine. Il va sans dire qu'il ne s'agit nullement de "légiférer pour légiférer".

Bien au contraire, il conviendrait d'appliquer les mesures énoncées par la Convention sus-évoquée en ayant au préalable mis en lumière les différents écueils, compte tenu de l'élément d'étude (mutations incessantes de l'Internet et des supports électroniques), qui rend nos différents codes fussent-ils civils et pénaux parfois surannés.

Au titre des **infractions informatiques**, il s'agit de prendre en considération dans l'arsenal juridique gabonais, le concept de falsification c'est-à-dire :

[7] Au Gabon, à travers la loi n° 1/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel, le législateur gabonais ne se départit pas et à raison, de ce qui se fait partout ailleurs. Il a établi un certain nombre de règles et de directives en mesure d'encadrer les technologies de l'information et de la communication eu égard à la collecte et au traitement des DCP.

Il en est de même pour la loi n° 006/2020 du 30 juin 2020 portant modification de la loi n°042/2018 du 05 juillet 2019 portant Code pénal de la République Gabonaise.

- Eriger en infraction pénale, conformément au droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnelle et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles (falsification informatique) ;

- Eriger en infraction pénale, conformément au droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui :
  a) en introduisant, altérant, effaçant ou supprimant des données informatiques ;
  b) d'altérer le fonctionnement d'un système informatique, dans l'intention frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui (fraude informatique).

Concernant les **infractions se rapportant au contenu** il faudra absolument distinguer les infractions ayant trait à la pornographie enfantine (phénomène désormais récurrent) de celles liées aux atteintes à la propriété intellectuelle et aux droits connexes.

Le législateur gabonais devra légiférer *boni et aequi*[8], en tenant compte des spécificités gabonaises mais également de l'évolution du cyberdroit dans le monde, eu égard à la prolifération des infractions dans ce domaine.
Mutatis mutandis, il s'agira également d'étendre le champ d'action de l'Agence Nationale des Infrastructures Numériques et des Fréquences (ANINF) et de revisiter ses missions, ses prérogatives et son fonctionnement. Bien évidemment, un travail en osmose[9] entre l'Agence de Régulation des Télécommunications (ARTEL), la Commission Nationale pour la Protection des Données Personnelles (CNPDCP) et l'ANINF serait un avantage certain et de bon aloi.

Cette énumération de recommandations non exhaustive, n'a pas pour prétention de faire le tour de la question. Au contraire, tend-t-elle modestement, à mettre en exergue un nombre conséquent d'informations qui sont autant de pistes de résolution que d'espoirs d'une sortie de l'ornière. Subséquemment à ce qui précède, la doctrine à travers sa constellation de juristes, de chercheurs et même de non juristes serait d'un apport plus que considérable à la tâche qui consiste désormais à endiguer la « spirale infernale ».

Il faut retenir que l'adoption d'un cadre juridique efficient doit prendre en compte la diversité des informations qui procèdent des enceintes internationales, notamment communautaires dans lesquelles sont débattues de nouvelles normes applicables à l'Internet.

7- Implications multipartites

Le caractère mondial des réseaux implique une approche juridique adaptée d'où, il importe de traiter les services Internet dans leur diversité, afin de ne pas bâtir un droit spécifique pour l'ensemble de ses déclinaisons. Cela ne peut être possible que par une réelle volonté de la part des Etats d'opter pour une entraide internationale véritable, mais aussi et surtout en assurant la liberté des communications en ligne, et en clarifiant les droits et les responsabilités de chacun.

Le droit, loin s'en faut ne doit nullement apparaître comme le seul rempart face aux dérives de cet immense outil collectif que constitue le Web. Bien au contraire, les utilisateurs, c'est-à-dire les acteurs à tous les niveaux se doivent d'apporter leur pierre à l'élaboration laborieuse de cet immense édifice. D'où, l'obligation d'une conscientisation de tous. La nécessité d'agir à l'échelle internationale n'est plus à démontrer tant il est vrai qu'en matière de nouvelles technologies et notamment de l'Internet, les agissements solitaires des différents Etats ont prouvé leurs limites.

Il importe donc dans ce cas, de mettre en place des réseaux de lutte contre les infractions sur Internet dans lesquels les arsenaux juridiques répressifs et judiciaires de tous les pays se retrouveraient en accord, aussi bien sur le plan des sanctions que sur celui des moyens utilisés. Selon M. Erkki Liikanen[10] :
« *La liberté de l'Internet, qui est la source même de son succès, doit être préservée. Le fait est là : sans sécurité, pas de confiance, pas de transactions. Toutes les prévisions remarquables qui ont été faites sur la croissance du commerce électronique resteront des vœux pieux, si l'on ne peut avoir confiance dans les transactions électroniques* ».

Au delà de la coopération entre les Etats, apparaît la nécessité impérieuse pour les individus de connaître les droits et les responsabilités leur incombant. De quelle

[8] Définition que donnaient les Romains au droit et qui signifie littéralement : « l'art du bien et du juste ». L'expression est composée des substantifs *ars* = le talent, le savoir-faire, l'habileté, l'art ; *bonum* = bien et *aequun* = l'équité, le juste.

[9] Ce cadre est très favorable pour le développement de l'ANINF, en l'occurrence en ce qui concerne la mise en place d'un *Cyber Incident Response Team* (CIRT) au Gabon. Il peut lui permettre d'occuper efficacement une position clé au niveau national pour le renforcement de la coordination avec toutes les parties prenantes, le développement des politiques de cybersécurité et l'exécution de tous les services.

[10] Ministre des Finances pendant trois ans à la fin des années 80, il a été le premier commissaire européen finlandais entre 1995 et 2004, successivement en charge du Budget et de l'Administration, puis des entreprises et de la société de l'information. Il est aujourd'hui Gouverneur de la Banque de Finlande.

façon cette sécurisation peut elle être acquise si ce n'est par l'action commune de tous les pays concernés ?

Il est donc plus qu'important sinon nécessaire, de mêler tous les acteurs du « Net » à cette bataille que le droit entend mener et gagner face à la criminalité sur le Web, au risque de voir des efforts considérables sans cesse annihilés et, le juridique, rester toujours en marge de la technologie dont l'avancée est inexorable.

Dans cette lutte contre la cybercriminalité, les Etats ne sont pas les seuls. En effet, des organisations telles que les Nations Unies proposent à leur tour des solutions permettant d'ériger un véritable cadre juridique (par les gouvernements) afin de juguler la criminalité via Internet.

Les Nations Unies ont joué et continuent à jouer un rôle important dans le cadre de cette action notamment en faveur de la création d'un cadre juridique normalisé en matière de lutte contre la cybercriminalité. Les premières résolutions mettant la criminalité informatique au centre de ses préoccupations remontent à 1990 (résolution 45/.109 du 14 décembre 1990).

Depuis, l'intérêt de l'Organisation pour ces questions est allé crescendo. Elle a clairement rappelé le rôle qu'elle entend jouer dans le paragraphe b- des recommandations du 11ème congrès des Nations Unies pour la prévention du crime et la justice pénale qui s'est tenu à Bangkok du 18 au 25 avril 2005 :

« *Du fait de son universalité, le système des Nations Unies s'est doté de mécanismes renforcés de coordination interne demandés par l'Assemblée Générale, il devrait jouer un rôle de premier plan dans les activités entreprises au plan intergouvernemental pour garantir le bon fonctionnement et la protection du cyberespace de sorte que celui-ci ne fasse pas l'objet d'abus et ne soit exploité par des criminels ou des terroristes* ».

Plus particulièrement, le système des Nations Unies devrait continuer à promouvoir l'application d'approches mondiales dans la lutte contre la cybercriminalité et la coopération internationale en vue d'atténuer l'impact négatif de la criminalité liée à l'informatique sur le développement durable, la protection des personnes, le commerce électronique, les opérations bancaires et de commerce.

Les Communautés Economiques Régionales (C.E.R) et même l'Union Africaine ne devrait pas être en reste dans la mesure où, elles aussi doivent jouer un rôle majeur. Cette initiative paraîtrait louable pour les gouvernements ; elle permettrait d'abord aux Etats africains de renforcer leur coopération sur le plan de la lutte contre la cybercriminalité, mais aussi d'harmoniser leurs législations à de nombreux niveaux.

En effet, de telles mesures tendraient à faciliter le positionnement du continent africain en tant qu'interlocuteur "valable" sur l'échiquier mondial par le truchement de l'Union Africaine. Le fait que l'Afrique du Sud ait été le seul Etat africain partie à la Convention de Budapest du 23 novembre 2001 ne doit pas pour autant battre en brèche la volonté affichée depuis lors par certains Etats, afin d'évoluer dans le sens des efforts fournis au niveau du NEPAD par le plus grand nombre. La mise en place d'un environnement régional sécurisé passe par le souci qu'a chaque gouvernement d'harmoniser et d'opter pour une vision d'ensemble, sans laquelle aucune véritable avancée dans l'éradication de la cybercriminalité ne serrait possible.

Quant au Nouveau Partenariat pour le Développement en Afrique (NEPAD), il se doit d'être l'instrument par lequel les Etats parviendront à mettre sur pied les mesures adéquates avec le soutien de la communauté internationale car le cybercrime vu son caractère extrêmement volatil, ne saurait demeurer le problème d'une poignée d'Etats mais au contraire, le problème de tout un chacun impliquant à la fois les gouvernements et leurs arsenaux juridiques, que les cyberconsommateurs.

8- Finalité

Nous dirons en définitive, que le formidable outil qu'Internet représente aujourd'hui est sans conteste une avancée majeure pour la civilisation humaine. Grâce aux autoroutes de l'information et particulièrement de l'Internet, les cyberconsommateurs ont à leur disposition de nombreux moyens qui permettent d'étendre un peu plus le cyberespace. Pourtant, cet extraordinaire outil traîne avec lui son aspect négatif représenté par l'utilisation abusive et criminelle des réseaux informatiques, c'est-à-dire la cybercriminalité.

Ce phénomène criminel polymorphe et sans précédent « déstabilise les outils traditionnels d'appréhension de la criminalité et impose de nouvelles approches »[11] Il convient dès lors de mettre en exergue les difficultés rencontrées par la plupart des Etats africains quant à l'application du droit sur ce qui peut être qualifié aujourd'hui sans exagération de "cyberculture".

Il revient impérativement aux autorités africaines de prendre la mesure des choses, par la mise en place d'une politique criminelle adéquate répondant aux enjeux majeurs de la dématérialisation des instruments répressifs, de la recherche de la preuve et de la détermination et de l'identification des personnes responsables dans l'univers numérique.

[11] Séminaire de l'A.D.I.E-Coopération « Informatique et libertés, quel cadre juridique pour le Sénégal ? » www.adie.sn.

Nous avons relevé la nécessité de concevoir une réelle politique inter-Etats de lutte contre les cyberinfractions. En effet, étant donné qu'il n'est pas nécessaire que les auteurs d'infractions soient présents sur le lieu où se trouve la victime ou même sur le lieu de la commission de leur forfait, cette coopération s'impose inexorablement comme *modus operandi*.

Cette réalité est d'autant plus perceptible, que les enquêtes en matière de cybercriminalité vont de pair avec le besoin d'une coopération internationale. C'est d'ailleurs, de façon occurrente, l'une des principales demandes formulées par les enquêteurs lors des enquêtes transnationales : une réaction immédiate de la part de leurs homologues au sein du pays où se trouve l'auteur de l'infraction, voilà ce qui pourrait fondamentalement faire avancer l'action coercitive.

Bibliographie

ABLAIN, E. (2002). *La cybercriminalité en Afrique de l'Ouest : entre cyberinfluences et cybercriminalité endogène*. Paris : Cygne, 122 p.

BISMUTH, Y. (2017). *Le droit de l'informatique*. (4ème Ed). Paris : le Harmattan, 438 p.

DAVID, E. (2018). *Éléments de droit pénal international et européen*. (2nd Ed). Bruxelles : Bruylant, 1862 p.

DIOUF, N. (1998). Infraction en relation avec les nouvelles technologies de l'information et de procédure pénale : l'inadaptation des réponses nationales face à un phénomène de dimension internationale, *RSDA*, 2, 67.

FERAL-SCHULHL, C. (2020). *Cyberdroit : le droit à l'épreuve de l'Internet*. (8ème Ed). Paris : Dalloz, 1890 p.

ITEAUNU, O. (2016). *Quand le digital défie l'Etat de droit*. Paris : Eyrolles, 190 p.

JABER, A. (2009). *Les infractions commises sur Internet*. Paris : l'Harmattan, 318 p.

LARRIEU, J. (2010). *Droit de l'Internet*. 2nd Ed. Paris : Ellipses, 220 p.

QUÉMÉNER, M. (2018). *Le droit face à la disruption numérique*. Paris : Gualino, 360 p.

QUÉMÉNER, M. ; DALLE, F. et WIERRE, C. (2020). *Quels droits face aux innovations numériques ?* Paris : Gualino, 232 p.

TEPI, S. (2020). *La cybercriminalité au Cameroun enjeux d'une législation en quête d'efficacité*. Paris: l'Harmattan, 273 p.

THOMAS, D. et LOADER, B. (2000). *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. New York : Routledge, 300 p.

TOURÉ, P.-A. (2014). *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal*. Paris : l'Harmattan, 620 p.

Webographie

DEPRAU, A. (2018). Les réponses judiciaires face à la cybercriminalité. *Village de la Justice.* Repéré à https://www.village-justice.com/

UIT. (2012). *Comprendre la cybercriminalité : Phénomène, difficultés et Réponses juridiques*. Repéré à www.itu.int

UIT. (2009). *Comprendre la cybercriminalité : guide pour les pays en développement*. Repéré à cybmail@itu.int

UIT. (2020). Global Cybersecurity Index. Repéré à www.itu.int

Textes législatifs

Loi n° 1/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel (J.O. 25 septembre 2011)

Code pénal loi n° 006/2020 du 30 juin 2020 portant modification de la loi n°042/2018 du 05 juillet 2019 portant Code pénal de la République Gabonaise, Publications Officielles, (2020)

Décret n° 000205/PR du 30 juin 2020 portant promulgation de la loi n° 006/2020 portant modification de la loi n° 042/2018 du 05 juillet 2019 portant Code pénal de la République Gabonaise, (2020)