Territorialité du droit pénal et cybercriminalité
The territorial Principe of penal law and cybercrime

Maitre Titouche Radia
Faculté de droit et des sciences politiques
Université Mouloud Mammeri, Tizi Ouzou .

تاريخ الإرسال :2018/06/03 تاريخ القبول : 2018/06/19 تاريخ النشر :2018/10/12

Résumé :

La cybercriminalité est l'un des plus grands fléaux de ce siècle, une criminalité en perpétuelle évolution assistée par la plus grande invention du monde moderne. Des milliers de criminels cachés derrière leurs écrans, se connectant depuis les quatre coins de la planète, un anonymat qui leur permet de sévir à l'abri de toutes poursuites judiciaires. La lutte contre la cybercriminalité est confrontée à plusieurs obstacles au vue du caractère virtuelle de celle-ci ; un espace immatériel auquel les normes traditionnelles de droit pénal peinent à s'appliquer. Une réalité qui nécessite une approche plus à même d'englober les aspects techniques de la criminalité numérique.

Mots-clés : *Cybercriminalité , droit pénal , pornographie enfantine , jurisprudence .*

***Abstract** :*

Cyber criminality is one of the most acute problems facing the world nowadays .this genuine plague is continuously evolving thanks to the biggest modern times invention.

Thousands of criminals well ambushed behind their computers, and connecting from everywhere and nowhere at the same time, given the anonymity they enjoy and which protects them from any possible tracking. Fight against cyber criminality is indeed immaterial, and the traditional, or conventional weapons of penal laws fail to cute .Such as situation requires an approach more likely to include technical aspects of the cyber criminality scourge.

***Keywords:** Cybercrime , criminals , penal law ; child pornography .*

***Introduction** :*

En se connectant aux services de communication et d'information, les usagers créent une sorte d'espace commun, dit « cyberespace »[1], qui sert à des fins légitimes, mais peut aussi donner lieu à des abus. Les infractions commises dans le cyberespace le sont contre l'intégrité, la disponibilité et la confidentialité des systèmes informatiques et des réseaux de télécommunication, à moins qu'elles ne consistent en l'utilisation de ces réseaux ou de leurs services dans le but de commettre des infractions classiques[2].

Le caractère international des infractions commises au moyen de l'internet se heurte à la territorialité des institutions nationales de répression[3]. En effet ; les actes de cybercriminalité ont une dimension transnationale, qui

implique des enquêtes transnationales, et qui soulève des questions ayant trait à la souveraineté[4]*, à la compétence et aux preuves extraterritoriales, et nécessite une coopération internationale.*[5]

Le principe de souveraineté implique que chaque infraction commise sur le territoire d'un Etat doit être poursuivie selon les lois de celui-ci et par les autorités qui le représentent. Une règle que tout pays se doit de respecter. Cependant, si les limites géographiques du monde réel sont faciles à déterminer, celles du monde virtuel sont loin d'être évidentes. En effet ,l'infraction dite traditionnelle aussi complexe qu'elle puisse être est toujours commise dans un environnement palpable, terrestre, marin ou aérien ; aussi l'on peut toujours la relier à un Etat bien précis. Alors que celles reliées au réseau mondial de l'internet sont commises partout et nulle part à la fois, dans un monde sans limites, en dehors de toute notion de territorialité[6]*.*

Ce qui implique que techniquement ces infractions ne sont commises nulle part et donc ne tombent sous la coupe d'aucune législation, ou bien l'inverse ; ces infractions sont commises dans tous les pays à la fois, ce qui soulève un problème immense qui est la compétence potentielle de plusieurs législations toutes aussi différentes les unes des autres en matière de poursuite et répression de l'infraction.

L'irruption de ce nouveau phénomène criminel dénommé cybercriminalité caractérisé par sa transnationalité, son immatérialité, sa volatilité et l'anonymat de ses acteurs a contribué à brouiller les repères du système pénal auquel il

lance un véritable défis. Celui de savoir si les réponses traditionnelles et permanentes, conçues et élaborées pour un environnement matérialisé et national, sont aptes à saisir cette nouvelle réalité de l'ère numérique.[7]

Le droit pénal est confronté à cette sphère innovante qui désarçonne quelque peu les juristes ; et il ***importe désormais de savoir si les règles juridiques traditionnelles de compétence territoriale du droit pénal sont adaptées en matière de cybercriminalité.***

L'approche du principe de territorialité du droit pénal en sollicitant les normes traditionnelles de compétence a vite démontré son inefficacité sur le terrain (partie 1) . aussi cette dernière se devait d'évoluer avec la technologie et trouver de nouvelles alternatives à même d'englober toutes les spécificités de la cybercriminalité (partie 2).

Partie 1 : Des limites des normes traditionnelles de compétence territoriale du droit pénal.

La norme juridique est d'inspiration sociale, elle vient répondre à une nécessité bien précise et la norme pénale ne déroge pas à cette règle. Les changements que subit une société fait qu'aucune loi n'est figée dans le temps et l'espace et une constante mise à jour est cruciale au maintien de l'ordre et au bon fonctionnement des institutions. Aussi, le changement est l'apanage du droit positif.

Les bouleversements technologiques font partie des moteurs de changement des normes juridiques[8] *abolissant toute notion de frontières* ***(section 1)***

internet a beaucoup influencé le paysage juridique du 21 éme siècle, démontrant l'incapacité des normes existantes à déterminer la compétence territoriale du droit pénal en matière de cybercriminalité ***(section 2).***

Section** 1 : **De l'aspect international de la cybercriminalité

La cybercriminalité constitue l'un des plus grands fléaux du monde moderne, une révolution dans le domaine du crime, des infractions à la pointe de la technologie, assistées par la plus grande invention de cette ère.

L'ère du numérique, formée de deux chiffres combinés à l'infinie créant un monde parallèle ou prospère une nouvelle forme de criminalité complexe qui échappe aux notions juridiques classiques.

1. La cybercriminalité : une réalité protéiforme mal cernée et non définie.

Trouvant son origine dans le droit anglo-saxon et légitimée par la norme européenne, la cybercriminalité ne renvoie pas à une liste d'infractions bien déterminées, puisqu'elle couvre quasiment l'ensemble du champ infractionnel.[9] *Il s'agit davantage d'une manière d'opérer particulière qui, utilise ou cible un système d'information.*

En effet ; la technologie facilite la commission de l'infraction, puisqu'un simple clic informatique suffit pour passer à l'acte ou atteindre à distance la victime potentielle, même si la mise en scène et les techniques utilisées sont souvent très élaborées.

Seulement de nos jours, ces dernières tendent à être maitrisées de plus en plus grâce à la démocratisation

d'internet et l'accessibilité des supports informatiques. De nos jours même une personne avec un niveau intellectuel limité peut utiliser les nouvelles technologies, car celles-ci sont conçues pour viser le plus grand nombre de consommateurs.

La technologie démultiplie les effets de la criminalité, en permettant, simultanément, d'attaquer de nombreuses cibles et en bénéficiant de la rapidité de propagation que permet l'outil informatique quelque soit son support, que ce soit un ordinateur, une tablette ou encore un téléphone.

Ajoutant à cela l'impunité dont bénéficie son auteur, qui jouit le plus souvent d'un anonymat fortement protégé, et de l'extranéité[10] *qui résulte de la localisation des serveurs et du lieu de stockage des données des principaux prestataires d'Internet.*

Par voie de conséquence, la cybercriminalité se prête mal à une définition celles-ci sont en fait légion mais aucune ne s'est véritablement imposée ce qui contribue au sentiment de flou que suscite ce concept et donc à la difficulté de son appréhension.

La cybercriminalité demeure encore pour les juristes une notion abstraite et la convention sur la cybercriminalité du conseil de l'Europe[11] *ne la définit pas, de même que le législateur algérien , qui à travers les réformes successives du volet pénal en matière de cybercriminalité utilise plusieurs termes sans pour autant la définir ; à savoir infractions portant atteinte aux systèmes d'analyses*

automatiques des données [12] *et infractions en relation avec la technologie de l'information et de la communication*[13] .

Aucun texte ne précise la notion de cybercriminalité, ce qui se comprend parfaitement vue la complexité de ce phénomène en perpétuel évolution ; aussi il est important néanmoins d'essayer de cerner la notion de cybercriminalité pour pouvoir déterminer quels types d'infractions sont concernés par ce phénomène.

2. Appréhension de la cybercriminalité en droit algérien.

La cybercriminalité n'est pas saisie par le droit interne algérien, même s'il y est fait référence sous d'autres appellations. comme mentionnée ci-dessus, essayer de donner une définition absolue à la cybercriminalité serait peine perdue car celle-ci englobe en son sein des centaines de possibilités que l'on saurait cerner ; si ce n'est en incriminant ces facettes au fur et à mesure de leurs apparitions en consacrant des textes propres à chacune d'entre elles.

Une ligne de conduite qu'a suivie le législateur algérien en commençant par la forme basique et purement informatique de la cybercriminalité en incriminant ***les atteintes aux systèmes d'analyses automatiques des données*** . [14]

Puis il s'est rendu compte que le système informatique pouvait ne pas être l'objet de l'atteinte mais un moyen de commission de celle-ci tout comme il pouvait constituer un environnement pour l'infraction plus communément connue sous l'appellation d'infraction de contenus. Aussi, il adopta

un autre terme plus large et surtout plus en phase avec la nature complexe de la cybercriminalité qui est : ***infractions liées à la technologie de l'information et de la communication.***[15]

Ainsi, le droit pénal algérien envisage enfin la cybercriminalité sous toutes ses formes, prenant en compte le facteur internet dans ses incriminations et la dimension internationale de ce phénomène. Un progrès qui permet enfin la mise en place d'un arsenal juridique à même de combattre la cybercriminalité. Même si la tâche s'annonce rude il n'en demeure pas moins que le droit pénal algérien est mieux armé qu'avant pour y faire face .

Section 2 : Territorialité du droit pénal ; une notion qui peine à s'appliquer à la cybercriminalité.

Le progrès des techniques de l'information a des répercussions directes sur tous les secteurs de la société moderne. L'intégration des systèmes de télécommunication et d'information, en permettant le stockage et la transmission quelle que soit la distance de toutes sortes de données, ouvre un immense champ de possibilités nouvelles.

Ces progrès ont été favorisés par l'apparition des réseaux informatiques et des autoroutes de l'information, notamment l'Internet, grâce auxquels toute personne ou presque peut avoir accès à la totalité des services d'information électronique, où qu'elle se trouve sur la planète.

1) ***De la Notion de territorialité du droit pénal*** *:*

La territorialité de la loi pénale est un principe qui veut que la loi pénale d'un pays déterminé s'applique et de ce fait, ses

juridictions sont compétentes en matière de poursuite et répression des infractions commises sur le territoire quelle que soit la nationalité de l'auteur et celle de la victime. C'est-à-dire, la loi pénale applicable sera celle du lieu de commission de l'infraction, peu importe la nationalité de l'auteur des faits[16]

L'article 3 [17]*du code pénal algérien stipule que la loi pénale algérienne s'applique à toutes les infractions commises sur le territoire de la république. Et l'article 586 du code de procédure pénale*[18] *précise* ***: « est réputée commise sur le territoire de la république toute infraction dont un acte caractérisant un de ses éléments constitutifs***[19] ***a été accompli en Algérie. »***

Il est clair que le législateur algérien tout comme son homologue français[20]*a adopté la théorie dite de* ***l'ubiquité*** [21] *selon laquelle il y a rattachement au territoire national et au droit pénal de ce dernier dès lors qu'une partie de l'infraction est commise sur ce territoire. En effet, par application de la théorie de l'ubiquité, il suffit, dans ce dernier cas qu'un fait constitutif soit localisé sur le territoire algérien.*

Cette théorie conduit à élargir la compétence territoriale de chaque État en permettant de localiser une infraction indifféremment du lieu de manifestation de l'action et de survenance de son résultat. Selon cette théorie, il est alors possible de localiser une infraction au lieu de la survenance de son fait générateur ou au lieu de la production de son résultat. Si ces règles s'appliquent aisément à l'infraction

dite traditionnelle ; elles peinent à l'être sur la cybercriminalité où la grande question qui reste souvent en suspens est ***le lieu de la commission de l'infraction****.*
En effet, la cybercriminalité évolue dans un milieu virtuel étranger à la notion traditionnelle de territorialité telle qu'énoncée dans les lois. Aussi, essayer d'appliquer celle-ci sans prendre en compte la spécificité et le volet technique de cette infraction serait totalement obsolète.

2) Difficultés d'application de la notion sur la cybercriminalité

a) Caractère planétaire et virtuel de la cybercriminalité :

Mondial par nature, 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 cyberespace ne demeurent pas hors d'atteinte. En effet, des terroristes utilisent l'anonymat qu'offre internet pour recruter et endoctriner des milliers de personnes et s'offrent ainsi le luxe de mener leur guerre sainte à travers des milliers de sites de propagande bien cachés dans les profondeurs abyssales de la toile.

De même pour les délinquants sexuels qui profitent des méandres du web pour s'adonner à leurs pratiques et laisser libre court à leurs vils instincts. Des milliers de criminels surfent ainsi dans un espace qui ne connait pas de frontières, un monde virtuel qui a toujours une cachette à leur offrir.

Une particularité qui donne toujours aux criminels une longueur d'avance si ce n'est plus ; d'autant plus que les infractions commises via internet ont lieux partout et nul part ; même si il est toujours possible de les relier à un endroit bien précis ; cela demande des moyens juridiques et logistiques colossaux, en plus d'une coopération sans faille entre les Etats sans laquelle tous les efforts fournis seront réduits à néant.

b) ***Une scène de crime virtuelle : Où sont commises les infractions ?***

Au vue du caractère transfrontalier de la cybercriminalité, il est plus que crucial de la relier à un territoire bien précis du monde réel ; car c'est de cela que dépondra la compétence d'un Etat bien précis à poursuivre ladite infraction selon ses lois et par ses propres autorités judiciaires. Pour se faire, il faudrait déterminer le lieu de commission de l'infraction comme stipulé dans le code pénal ainsi que dans la constitution.

Hors cela s'avère compliqué quand on sait que la cybercriminalité a pour cible ou domaine un territoire virtuel où les frontières telles que nous les connaissons n'existent pas, car le cyberespace est un monde parallèle au monde matériel.

En effet, un cyber délinquant pourrait élaborer un virus informatique en Algérie, puis infecter un ordinateur zombie localisé en Lybie et en prendre possession , puis lancer une attaque contre les serveurs d'une société basée en France .

La manœuvre aurait pour but le piratage de données privées .

En nous référant aux normes traditionnelles de territorialité du droit pénal plusieurs lois sont compétentes :

- *Selon la théorie de l'action ; la loi algérienne est compétente dès lors que l'un des éléments constitutifs de l'infraction est commis en Algérie. Et dans ce cas de figure l'attaque a été lancée depuis un ordinateur se trouvant sur le territoire algérien. ce qui localise l'infraction en Algérie d'où la compétence territoriale du droit pénal algérien. De même que la loi libyenne serait compétente du fait que l'ordinateur détourné et auteur de l'attaque se trouverait sur son territoire[22]. Ce qui engendrerait inévitablement un conflit de compétence.*
- *Selon celle du résultat : le droit français serait compétent du fait que le résultat de l'attaque se serait concrétisé sur le territoire français[23]..*

artie 2 : De l'adaptabilité des normes traditionnelles de compétence territoriale du droit pénal.

Section 1 : Des alternatives pour relier la cybercriminalité à un territoire bien précis.

Si la technologie permet aux criminels de commettre leurs activités en toute impunité ; celle-ci peut aussi être utilisée par les autorités pour les traquer et les localiser ; car la cybercriminalité a beau avoir pour domaine le monde virtuel, il n'en demeure pas moins qu'elle est commise par des êtres de chair et de sang qui se trouvent quelque part dans un Etat bien réel régi par le droit.

Aussi, les juristes à défaut de localiser l'infraction dans un univers non palpable ont eu une approche différente qui consiste à relier les auteurs et les données à un lieu bien physique. En effet; l'infraction de cybercriminalité peu importe sa facette est commise soit dans l'Etat où le délinquant s'est connecté à internet pour commettre l'infraction ; soit dans le pays où se trouve le serveur qui héberge les données, soit dans le pays ou les contenus sont accessibles.

1) Lieu de connexion et régime de l'adresse IP.

Même s'il est impossible de localiser une infraction commise dans un environnement immatériel, on peut toujours la relier à un point bien précis de notre réalité, aussi quand un individu se connecte pour télécharger ou visionner des contenus pédopornographique ou tout autre contenu illicite, il le fait à partir d'un point géographique bien précis qui pourrait être considéré comme le lieu de commission de l'infraction .

Ce critère représente l'alternative qui viendrait transposer les normes traditionnelles de compétence territoriale du droit pénal à la cybercriminalité, Et pour remonter au lieu de connexion et de ce fait à l'auteur, l'adresse IP[24]*apparait comme étant la solution la plus efficace.*

Ce sont les fournisseurs d'accès qui attribuent une adresse IP à leurs clients lorsque ces derniers se connectent à internet ; il est donc parfaitement possible de remonter par ce biais, à un abonné.[25]

L'adresse internet protocole ou adresse IP apparait comme une notion d'avantage technique que juridique, mais elle revêt une importance capitale pour remonter jusqu'à l'utilisateur voir l'auteur d'une infraction.[26]*C'est pour cela que le législateur algérien oblige désormais les fournisseurs de services internet à conserver les données relatives au trafic de leurs clients, notamment celles concernant les données permettant l'identification des utilisateurs du service en plus de l'obligation de les communiquer aux autorités compétentes.*[27]

Par exemple, le lieu d'émission des sites litigieux qui peut correspondre au domicile de l'internaute signalant est un critère qui peut être retenu, de même que le lieu de localisation du serveur véhiculant le site litigieux .Les règles de compétence édictées notamment par l'article 586 du Code de procédure pénale algérien s'appliquent en la matière , seulement les investigations sont vite bloquées en raison de la localisation des données indispensables au bon déroulement de l'enquête hors du territoire algérien car les sites sont souvent hébergés à l'étranger comme les sites et réseaux sociaux les plus connus tels que facebook , Yahoo et des milliers d'autres .

2) ***L'émergence de la théorie de l'accessibilité au site ou contenu.***

Selon cette théorie l'accessibilité du contenu illicite depuis le territoire algérien constitue un élément constitutif de l'infraction, ce qui induit la compétence du droit pénal algérien. Une position adoptée par la jurisprudence

*française qui considère qu'un élément constitutif de l'infraction est commis sur le territoire français lors de la connexion à des informations illicites se situe en France. A cet égard, par jugement en date du 26 février 2002, le tribunal de grande instance de Paris (17e chambre) a rappelé que "**le juge français est compétent dans la mesure où les messages ou le contenu du site sont rendus accessibles, par l'Internet, sur le territoire français"**[28].*

Comme l'a rappelé le rapport du Conseil d'Etat "l'Internet et les réseaux numériques,[29] il résulte de ces dispositions que la loi pénale française s'appliquera clairement dans le cas d'un message litigieux disponible sur le réseau Internet, quelque soit sa source dans le monde, et accessible de France, dès lors que la réception par l'utilisateur sur le territoire français est bien un élément constitutif de l'infraction en application de l'article 113-2 du Code Pénal. Une célèbre affaire de justice confirme la position de la jurisprudence française en matière de contenus illicites émanant de l'étranger et accessible en France ;celle de la Licra[30] contre le géant américain Yahoo.

L'affaire de la Licra contre Yahoo a abouti à une décision de justice qui aborde la question de la territorialité des lois françaises et leur application à un site internet. La Ligue internationale contre le racisme et l'antisémitisme et l'union des étudiants juifs de France constatent qu'il est possible d'acheter des objets nazis aux enchères en se connectant au site web de Yahoo!, en violation de l'article R.645-1 du

Code Pénal français et entreprennent des poursuites judiciaires à l'encontre du site .

Il est notamment rapporté qu'une boîte de Zyklon B, un gaz utilisé dans les camps de la mort, est vendue 50 dollars sur le site. Les associations décident de porter plainte contre Yahoo! en mai 2000 et l'assignent en référé le 15 mai 2000 devant le Tribunal de grande instance de Paris.[31]

Par ordonnance en novembre 2000, le Président Gomez du tribunal de grande instance de Paris condamne Yahoo! à prendre toutes mesures de nature à dissuader et à rendre impossible toute consultation sur yahoo.com du service de vente aux enchères d'objets nazis et de tout autre site ou service qui constitue une apologie du nazisme ou une contestation de crimes nazis , sur le fondement de l'article R.645-1 du Code pénal[32]*, sous astreinte de 100 000 francs par jour de retard.*[33]

Le tribunal a considéré que la loi pénale française était compétente : dès lors que Yahoo sait qu'elle s'adresse à des Français puisque, à une connexion à son site d'enchères réalisée à partir d'un poste situé en France, elle répond par l'envoi de bandeaux publicitaires rédigés en langue française ; Qu'est ainsi suffisamment caractérisé en l'espèce le lien de rattachement avec la France, ce qui rend la juridiction français parfaitement compétente .

3) L'évolution jurisprudentielle en faveur de la théorie de la focalisation :

Si on a pu constater que la jurisprudence s'est d'abord naturellement tournée vers le critère de l'accessibilité pour

fonder sa compétence, nous avons pu remarquer que cette théorie souffrait de terribles lacunes du fait que plusieurs pays pourraient se disputer la compétence du fait que les contenus sont dans la plupart des cas disponibles un peu partout dans le monde. Ce qui motive la recherche de nouveaux critères permettant de limiter de manière raisonnable la compétence territoriale d'un État, face à une situation où tous peuvent revendiquer leur compétence de manière égale.

En effet ; la conception extensive de la théorie de l'ubiquité amène à rendre disponibles les sites Internet dans le monde entier, partout où une connexion Internet existe. A cette fin, la jurisprudence [34] doit nécessairement chercher à adapter le caractère national de sa législation à la portée universelle du réseau Internet[35].

Pour ce faire, une évolution des critères de rattachement est indispensable et c'est ce vers quoi la jurisprudence française, s'est tournée en décidant de restreindre son champ de compétence en adoptant la théorie de la focalisation.[36]Ainsi, la jurisprudence française a exigé du juge français un lien suffisant, substantiel ou significatif entre les faits allégués et le territoire français.

En effet ,Un arrêt de la chambre criminelle de septembre 2008[37]a posé une condition supplémentaire à l'accessibilité pour rattacher au territoire français une infraction commise via le réseau Internet depuis un site étranger. En l'espèce, il s'agissait d'un site italien ayant mis en ligne un article sans l'accord des ayants droit français.

La contrefaçon ayant pour élément constitutif sa perpétration un autre territoire que la France à savoir l'Italie, il fallait donc prouver la possibilité pour le public français d'accéder à cet article. La Cour d'appel[38]*, se basant sur la jurisprudence antérieure, avait estimé que l'accessibilité du site suffisait pour caractériser la perpétration de l'infraction sur le territoire français.*

La Cour de cassation va censurer ce raisonnement et va estimer que l'article, accessible uniquement via un site italien et rédigé en langue italienne, n'était pas à destination du public français. De ce fait, les juges du fond n'ont pas suffisamment rattaché la contrefaçon avec le territoire français. Ainsi, les juges de cassation posent comme critère la nécessité de s'adresser effectivement au public français et pour ce faire, l'emploi de la langue française semble être un impératif[39]*.*

Section 2 : Nécessité d'une approche globale de la cybercriminalité.

Déterminer le lieu de commission de la cybercriminalité tel qu'envisagé dans cet article requiert une pléthore de mesures tant sur le volet matériel que processuel du droit pénal au niveau national et international.

1. Mise en œuvre de moyens techniques

Le principe de souveraineté interdit par principe à la juridiction saisie du procès pénal d'exercer ses attributions en dehors de ses frontières et de recueillir elle-même dans un État étranger les preuves [40]*. En ce sens, la recherche de la*

preuve dans l'État du lieu de commission de l'infraction peut poser de sérieuses difficultés.

En effet, une infraction pénale n'a de réalité juridique que si elle peut être prouvée de manière certaine et sans équivoque. Si la preuve pénale est impossible à établir, tout notre droit pénal est alors voué à rester à l'état d'ébauche[41]*. De fait, il est primordial que le droit pénal et la procédure pénale s'adaptent à la spécificité et au caractère volatil et planétaire de la cybercriminalité. De nouveaux moyens juridiques d'investigations doivent être créés afin de recueillir les preuves numériques dans des conditions incontestables sur le plan juridique.*

En ce qui concerne l'organisation des services d'enquête, les Etats hésitent entre le recours à des enquêteurs spécialisés et la création de véritables services dédiés à la lutte contre la cybercriminalité ; toutefois, la croissance de cette délinquance les incite actuellement à privilégier la seconde solution, quitte à créer, dans le cadre de tels services, des groupes plus spécialement assignés à lutter contre telle ou telle forme de cyber délinquance.

L'Algérie s'est doté d'un organe national entièrement dédié à la lutte contre la cybercriminalité composée de juges et d'officiers de police judiciaire. Une compétence technique inédite mise à la disponibilité des forces de police judiciaire sur tout le territoire. Un prélude nous l'espérons à la création d'unités locales spécialisées dans la lutte contre la cybercriminalité à long terme.

Un organe national de prévention et de lutte contre la criminalité liée aux technologies de l'information et de la communication[42]*. Dont la mission serait :*

- *la dynamisation et la coordination des opérations de prévention et de lutte contre la criminalité liée aux technologies de l'information et de la communication.*
- *l'assistance des autorités judiciaires et des services de police judiciaire en matière de lutte contre la criminalité liée aux technologies de l'information et de la communication, y compris à travers la collecte de l'information et les expertises judiciaires.*
- *l'échange d'informations avec ses interfaces à l'étranger aux fins de réunir toutes données utiles à la localisation et à l'identification des auteurs des infractions liées aux technologies de l'information et de la communication.*

En effet, Un décret[43] *adopté plus de 5 ans après la loi 09-04 crée l'organe national de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication, Une autorité administrative Indépendante jouissant de la personnalité morale et de l'autonomie financière, placée auprès du ministre chargé de la justice.*
Un grand pas pour le droit processuel algérien, car en plus d'assister les différentes entités judiciaires dans leur travail ; cet organe veille à développer une solide coopération tant au niveau national qu'international en mettant à contributions toutes les institutions publiques et privées concernées par la lutte contre la cybercriminalité.

2. .*Coopération judiciaire internationale.*

*L'efficacité de la lutte contre la cybercriminalité repose, en grande partie, sur une véritable coopération internationale, élément incontournable qui doit s'inscrire dans le prolongement de l'activité opérationnelle des services d'enquête et des autorités judiciaires***.**

Dans ce contexte, l'Algérie a vu ,depuis 2009, le lancement progressif d'initiatives, institutionnelles et juridiques qui ont permis de premières avancées concrètes au niveau international en matière de coopération contre la cybercriminalité. Le législateur a abordé la question de la coopération internationale dans le cadre des investigations sur la cybercriminalité, surtout en matière de perquisition informatique.

En effet, Dans le cadre des investigations ou des informations judiciaires menées pour la constatation des infractions comprises dans le champ d'application de la loi et la recherche de leurs auteurs, les autorités compétentes peuvent recourir à l'entraide judiciaire Internationale pour recueillir des preuves sous forme électronique.[44]

La nécessité de la mise en application de mesures de coopération internationale n'est plus à prouver, et le législateur algérien se devait de traiter la question de l'éventualité de devoir recourir aux autorités étrangères dans le cadre des investigations et informations en matière de cybercriminalité. Sans quoi tous les efforts fournis pour la combattre serait vains, car comme citée plus haut les données visées par les enquêteurs peuvent ne pas être

stockées sur des serveurs se trouvant physiquement sur le territoire algérien aussi les autorités n'ont aucun droit d'y accéder sans l'aval du pays qui les abrite.

Aussi l'article 5 de la loi 09-04 précédemment citée traite ce point comme il suit : S'il est préalablement avéré que les données recherchées, accessibles au moyen du premier système, sont stockées dans un autre système informatique situé en dehors du territoire national, leur obtention se fait avec le concours des autorités étrangères compétentes Conformément aux accords internationaux pertinents et suivant le principe de la réciprocité.

Supposons que des enquêteurs algériens repèrent un délinquant sexuel proposons des relations sexuelles à des enfants via les réseaux sociaux, et qui d'après le signal émis par son ordinateur serait connecté depuis le territoire algérien. ce qui justifie la compétence territoriale du droit pénal algérien.

Seulement pour constater l'infraction et prouver la culpabilité de son auteur, les enquêteurs devront accéder aux données du site, ce qui poserait un réel problème dans l'éventualité ou celui-ci serait hébergé en dehors du territoire. .

Les services concernés n'auront d'autres solutions que celle de demander aux autorités étrangères de contacter le fournisseur d'hébergement concerné afin qu'il communique les informations relatives à la personne suspectée de partager des contenus à caractères pédopornographiques.

Une procédure lente et laborieuse qui peinerait à aboutir dans le cas de pays comme la Russie ou l'Ukraine qui ne luttent pas contre la pornographie enfantine et où prospèrent les hébergeurs de sites à caractère pédopornographique[45].

Conclusion :

Le secteur des technologies de l'information et de la communication encore souvent qualifiées de nouvelles technologies démontrent aussi par cet adjectif que le droit ne les a pas encore complètement appréhendées ; car elles sont en constante évolution.[46]

La question de la compétence territoriale est fondamentale dans le traitement judiciaire de la 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.

La théorie de l'ubiquité, découlant de la mise à disposition d'informations et de données dans le monde entier de manière simultanée, engendre diverses conséquences, puisque sur ce fondement, tous les pays du monde seraient en effet susceptibles de se déclarer compétents.[47]*En plus des preuves qui se trouvent le plus souvent à des milliers de kilomètres des enquêteurs.*

L'incohérence est d'autant plus manifeste que l'harmonisation des législations internationales est encore insuffisante[48] *et bon nombres d'États, au nom du principe de souveraineté, restent encore peu enclin à participer*

pleinement à cet effort de coopération[49]*. Par ailleurs, les condamnations pénales prononcées à l'étranger, quand elles le sont effectivement, ne peuvent en principe recevoir exécution dans le pays le plus intéressé par la répression du fait de l'absence d'exequatur en matière pénale.*[50]

Le droit pénal doit donc suivre le rythme de ces évolutions techniques, qui offrent des moyens extrêmement perfectionnés d'employer à mauvais escient les services du cyberespace et de porter ainsi atteinte à des intérêts légitimes. Étant donné que les réseaux informatiques ignorent les frontières, un effort international concerté s'impose pour faire face à de tels abus.

La lutte des services de polices contre les cybercriminels et le combat de David contre Goliath, une disparité énorme en matière de moyens et de compétences technologiques. Un grand faussé auquel il est urgent de remédier. L'arsenal juridique algérien en matière de cybercriminalité en est encore au stade embryonnaire. Encore loin d'égaler ceux des autres pays comme la France, un des Etats précurseurs dans le domaine du droit numérique.

Le législateur algérien devrait donc continuer sur sa lancée et se pencher plus en détails sur les aspects techniques de la cybercriminalité et prévoir des réponses en conséquence à savoir :

- ✓ *Créer plus d'organes spécialisés dédiés à la lutte contre la cybercriminalité mais surtout des moyens techniques permettant la localisation des auteurs.*

✓ *adopter une approche globale mêlant tous les acteurs privés et publics à la répression de cette criminalité.*

✓ *Former les membres du circuit judiciaire aux aspects technologiques et techniques de la cybercriminalité.*

✓ *Signer des conventions internationales en matière de coopérations juridiques et judiciaires avec le plus de pays possibles.*

Au vue de la démocratisation de l'utilisation du réseau internet en Algérie et toutes les infractions qui en résultent, il serait judicieux que la jurisprudence algérienne se penche sur la question de la territorialité du droit pénal en matière de cybercriminalité ; en définissant les critères requis au rattachement d'une infraction commise via le réseau internet au territoire algérien.

Références

[1]*Appelé aussi « infosphère »., il est à noter que le préfixe « cyber » que l'on ajoute à un mot existant pour en transposer la réalité dans le cyberespace vient du mot grec « kubernan» signifiant « gouverner », mais son sens actuel tire son origine du nom cyberspace, inventé en 1984 par l'auteur américain de science-fiction William GIBSON, dans son livre intitulé « Neuromancer» . Voir : Mohamed CHAWKI, Essai sur la notion de cybercriminalité, IEHEI, juillet 2006, p 10. Disponible sur www. iehei.org.*

[2] *Jean François Tyrode, éléments de procédure pénale dans le cadre de l'atteinte aux personnes par la cybercriminalité en droit européen », mémoire de master Droit de l'Internet Public - Administration – Entreprises, université paris 1,2007, page 05. Voir aussi : Chilstein David. Législation sur la cybercriminalité en France, Revue internationale de droit comparé. Vol. 62 N°2,2010. pp. 553-606. p 253 disponible sur www.persee.fr .*

[3] *Rapport explicatif de la Convention sur la cybercriminalité Budapest, 23.XI.2001, conseil de l'Europe, Série des traités européens - n° 185 ; pp 02.03, Disponible sur www.coe.int .*

[4] *Article 13 de la constitution algérienne : « La* ***souveraineté de l'Etat s'exerce sur son espace terrestre, son espace aérien et ses eaux. L'Etat exerce également son droit souverain établi par le droit international sur chacune des différentes zones de l'espace maritime qui lui reviennent ».*** *Loi 16-01 du 6 mars 2016 portant révision constitutionnelle. JO numéro 14, paru le 07 mars 2016.*

[5] *Étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face, UNODC/CCPCJ/EG.4/2013/2. P11.*

[6] *, Myriam Quéméner , Yves Charpenel , cybercriminalité droit pénal appliqué , Economica , France , 2010 , p 26.*

[7] *Cartier-Bresson Jean, « Comptes et mécomptes de la mondialisation du crime », L'Économie politique, 2002/3 no 15, p. 22-37. Page 35, 36 ARTICLE DISPONIBLE SUR : http/www .cairn.info / revue-l-économie-politique-2002-3-page-22-htm. Consulté le 25 décembre 2018.*

[8] *Eirick prairat , considération sur l'idée de norme , les sciences de l'éducation – pour l'ère nouvelle , vol 45 ; 2012/1 , pp1- 168 ; p 09 .*

[9] *Groupe de travail interministériel sur la lutte contre la cybercriminalité, Protéger les internautes, Rapport sur la cybercriminalité, France, 2014, p10.*

[10] *La plupart des sites abritant des contenus illicites sont hébergés dans des pays étrangers ; comme les sites de pornographie enfantine qui sont souvent hébergés en Russie ou en Ukraine, des pays ou les fournisseurs d'hébergements ne sont pas inquiétés par les autorités. Voir : collectif d'auteurs, confession d'un pédophile, l'impossible filtrage du web, in libro Veritas, 2009, France, p 19.*

[11] *Convention sur la cybercriminalité, conseil de l'Europe, Budapest le 23 novembre 2001, disponible sur www.europarl.europa.eu.*

[12] Loi n° 04-15 du 27 Ramadhan 1425 correspondant au 10 novembre 2004 modifiant et complétant l'ordonnance n° 66-156 du 8 juin 1966 portant code pénal , JO numéro 71 paru le 10 novembre 2004 .

[13]Loi n° 09-04 du 14 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. JO numéro 47, paru le 16 aout 2009.
[14] Loi n° 04-15, précédemment citée.

[15] Loi n° 09-04, précédemment citée.
[16]Edmond Mbokolo Elima , l'étude comparative de la répression de la cybercriminalité en droits congolais et français, mémoire de licence en cybercriminalité , université Mbandaka , faculté de droit , 2014 , p 10 .
[17] Ordonnance n 66-156 du 8 juin 1966, modifiée et complétée, portant code pénal ;
[18] Ordonnance n° 66-155 du 8 juin 1966, modifiée et complétée, portant code de procédure pénale.

[19]L'élément matériel de toute infraction peut être scindé en deux parties : l'une stricto sensu, l'action, qui exprime le dynamisme de la conduite délictueuse ; l'autre le résultat de l'acte, qui constitue la traduction matérielle d'un état subi ; autrement dit l'acte implique « un comportement volontariste indissociable de la personne de l'auteur, tandis que le résultat désigne un état, plus ou moins voulu par l'agent, toujours supporté par la victime à laquelle il renvoie directement ».

Voir : Romain BOOS, la lutte contre la cybercriminalité au regard de l'action des états, Thèse de doctorat, faculté de droit, sciences économiques et gestions de Nancy, Université de Lorraine, 2017. p 158.
[20] L'article 113-2 du Code pénal français précise que « ***la loi pénale française est applicable et que l'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a lieu sur le territoire français****. Disponible sur : www.legifrance.gouv.fr.*
[21] Romain BOOS, opus cité ,.p 147,148.

[22] Article 4 du code pénal libyen, disponible sur le site du ministère de la justice libyen http://aladel.gov.ly/home/ consulté le 3 juin 2018.

[23] L'article 113-2 du code pénal français dispose : « 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. » disponible sur www.legifrance.gouv.fr .

[24]Numéro unique d'identification donné à chaque ordinateur connecté à Internet. Un numéro IP est un groupe de 4 nombres (de 0 à 255) séparés par des points. Cette adresse peut être fixe (pour les connexions par ADSL ou câble) ou dynamique (elle change à chaque connexion en cas d'utilisation d'un modem téléphonique). Chaque fois qu'un ordinateur se connecte à Internet, il est repéré par l'adresse IP d'origine qui indique son emplacement sur le réseau. A une demande d'identification, peuvent correspondre plusieurs adresses IP. L'adresse IP destinataire correspond à la machine sur laquelle l'Internaute désire se connecter. Voir : Le traitement judiciaire de la cybercriminalité, guide méthodologique, ministère de la justice, direction des affaires criminelles et des grâces, France, mai 2002. p39.

[25] Myriam Quemener , Yves Charpenel , opus cité 60 .

[26] Ibid , p 59 .

[27] Article 11 de la loi 09-04 précédemment citée.

[28] Le traitement judiciaire de la cybercriminalité, guide méthodologique, opus cité, p 23.

[29]Internet et les réseaux numériques : étude adoptée par l'Assemblée générale du Conseil d'Etat le 2 juillet 1998, disponible sur www.ladocumentationfrancaise.fr .

[30] Ligue internationale contre le racisme et l'antisémitisme, informations disponible sur www.licra.org .

[31] Jérôme Thorel ; Affaire Licra contre Yahoo : jugement inapplicable aux États-Unis ; www.zdnet.fr Consulté le 17 octobre 2017.

[32]« Est puni de l'amende prévue pour les contraventions de la 5e classe le fait, sauf pour les besoins d'un film, d'un spectacle ou d'une exposition comportant une évocation historique, de porter ou d'exhiber en public un uniforme, un insigne ou un emblème rappelant les uniformes, les insignes ou les emblèmes

qui ont été portés ou exhibés soit par les membres d'une organisation déclarée criminelle en application de l'article 9 du statut du tribunal militaire international annexé à l'accord de Londres du 8 août 1945, soit par une personne reconnue coupable par une juridiction française ou internationale d'un ou plusieurs crimes contre l'humanité prévus par les articles 211-1 à 212-3 ou mentionnés par la loi n° 64-1326 du 26 décembre 1964. » Disponible sur www.legifrance. Gouv .Fr.

[33] Tribunal de Grande Instance de Paris Ordonnance de référé du 20 novembre 2000 disponible sur le site www.legalis .net . Consulté le 17 octobre 2017.

[34] Dans cette étude nous nous sommes basés sur la jurisprudence française en matière de compétence territoriale, plus riche et plus avancée que la jurisprudence algérienne qui reste encore au stade embryonnaire.

[35] LARDEUX (G.), « Les cyber-délits », Revue Lamy, droit de l'Immatériel, [2012], pp. 1-2.

[36] Romain BOOS , opus cité . p175.

[37]Cass .Crim., 9 septembre 2008, n° 07-87.281.disponible sur www.legifrance.gouv.fr

[38] 'arrêt de la cour d'appel de Paris , 13e chambre, 25 septembre 2007 . Disponible sur www.legifrance.gouv.fr

[39] Jean François Tyrode , opus cité , p 56 .

[40] UNODC, « La coopération internationale en matière pénale contre le terrorisme », programme de formation juridique contre le terrorisme, [2011], p. 87.

[41] Romain BOOS , opus cité , 183 .

[42] Article 13 de la Loi n° 09-04, précédemment citée.

[43] Décret présidentiel n° 15-261 du 24 du 8 octobre 2015 fixant la composition, l'organisation et les modalités de fonctionnement de l'organe national de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication ; JO numéro 53 paru le 08 octobre 2015 .

44 Article 16 de la Loi n□□09-04, précédemment citée.

[45] *ECPAT international , child pornography and sexual exploitation of children online , the world congress 3 against sexual exploitation of children and adolescents , Rio de Janeiro , Brazil , 25-28 November 2008 . p 31 .*

[46] *Myriam Quéméner , Yves Charpenel , opus cité , p 26.*

[47] *Francillon (J.), Cybercriminalité aspects de droit pénal international », Rapport au nom de l'Association internationale de Droit pénal, XIXe Congrès international de Droit pénal, [2013], p. 1. Disponible sur www.penal.org , consulté le 18 octobre 2017.*

[48] *En matière de protection de l'enfant contre l'exploitation sexuelle, bon nombre de gouvernements sont à la traine en matière de lutte contre certains aspects de la cybercriminalité telle que la pornographie enfantine, aussi coopérer avec ces états dans le cadre d'enquêtes et informations serait totalement inutile, voir : pornographie enfantine , examen de la législation type à l'échelle mondiale , centre international pour les enfants disparus et exploités , septième édition 2012 ; pp. 14-39 .*

[49] *Cette réticence est plus manifeste dans le cadre d'enquêtes ayant trait au terrorisme, un sujet délicat dont la portée dépasse souvent la simple infraction.*

[50] *Francillon (J.), « Le droit pénal face à la cyber délinquance et à la cybercriminalité », RLDI, [2012], p3.*