Revue Internationale du Chercheur
ISSN: 2726-5889
Volume 5 : Numéro 1

L'enquête pénale à l'épreuve de l'internet

Criminal investigation to the test of internet

Enyegue Caroline Patricia

PhD en droit privé

Enseignante à l'université de Yaounde II-Soa

Cameroun

Date de soumission : 03/02/2024

Date d'acceptation : 16/03/2024

Pour citer cet article :

Enyegue. C. P. (2024) « L'enquête pénale à l'épreuve de l'internet», Revue Internationale du chercheur «Volume 5 : Numéro 1» pp : 925-948

Résumé

L'avènement de l'internet a bouleversé toute la société. En effet les Tics sont au cœur de tout développement mais elles sont aussi devenues les cibles de la malveillance. De nouveaux types d'infractions ont vu le jour connus sous le nom de la cybercriminalité facilités par de nombreux avantages qu'offre l'internet à ses utilisateurs. Il était donc impératif de barrer la voie à cette nouvelle forme de criminalité en instituant une loi visant à lutter contre ce phénomène qui bouscule tous les canons de la recherche de la preuve en matière d'enquête pénale. Ainsi les méthodes d'investigation probatoires classiques sont en déphasage avec l'environnement numérique qui se particularise par son caractère atteritorial, dématérialisé de l'enquête et volatil des données. Ces spécificités de l'environnement numérique obligent le législateur a revisité ces méthodes d'investigation probatoires classiques ou du moins à créer de nouvelles. Néanmoins il faut le souligner ces nouvelles méthodes d'investigation numériques connaissent de limites voire d'insuffisances dans leur déploiement, bafouant ainsi les droits et libertés des personnes poursuivies.

Mots clés : cybercriminalité ; perquisition ; méthode investigation ; anonymat ; coopération internationale.

Abstract

The advent of the internet has shaken up soceity. In fact, ICTs are at the heart of all development. However, ICTs have become the target of malicious intent. New types of offenses are emerging know as cybercrime with the internet tool thanks to the numerous advantages it offers to its users. To block the way for this new form of crime, the legislator has established a law aimed at combating this phenomenon which shakes up all the canons of the search for proof in matters of criminal investigations thus creating new digital investigations methods. However, these new digital investigation methods have limits and sometimes violate the rights and freedoms of those being prosecuted.

Keywords : cybercrime ; search ; judicial requisition ; anonymity ; international cooperation.

Introduction

L'internet est au cœur de tout développement de la société. En effet l'utilisation des technologies de l'information et de la communication est désormais incontournable. Les bienfaits qu'elles prodiguent, constituent des supports et des facilitateurs de tout développement (Myriam Quemener, Yves Charpenel, 2010 ; Gouanlong Kamgang,N ; Adam Boukar, T ; 2023). Cependant comme l'enseignait si bien le Doyen Carbonnier « l'évolution des mœurs et des techniques donne naissance à des nouvelles formes de délinquance » (Papa Assane Touré, 2014). Effectivement la plupart des grandes découvertes technologiques ont engendré presque toujours à côté des progrès économiques qu'elles procurent à l'humanité des retombées négatives parmi lesquelles figurent en bonne place l'avènement de nouvelles formes de criminalité. Les TIC n'échappent pas à cette règle et sont devenues les cibles de la malveillance. Ainsi de nouveaux types d'infractions ont vu le jour connus sous le générique de cybercriminalité[1]. Face à ce constat plus ou moins alarmant, il était donc impérieux que le législateur réagisse en mettant sur pied une loi tendant à incriminer ces types de comportements et à punir tout contrevenant d'où l'avènement de la loi de 2010 relative à la cybersécurité et la cybercriminalité.

En effet la singularité des comportements cybercriminels visant les valeurs du cyberespace et réalisés au moyen des procédés nouveaux justifie leur basculement dans des catégories pénales autonomes (Judith Rochfed , Martial Braz, 2019). La loi de 2010 incrimine deux types d'infractions à savoir les comportements classiques[2] ayant utilisé comme moyen de commission de l'infraction le réseau internet d'une part et d'autre part les comportements spécifiques aux technologies de l'information et de la communication qui sont nés avec l'outil internet[3]. Il revient donc aux autorités policières et judiciaires de constater les infractions, d'en rassembler les preuves et de rechercher les auteurs. Il s'ouvre donc le procès pénal qui commence indubitablement par l'enquête pénale qui est la phase de la procédure pénale durant laquelle les autorités policières recherchent et rassemblent les preuves en vue de la manifestation de la vérité. L'enquête pénale se caractérise par un déploiement des techniques d'investigation de

[1] [1] On définit la cybercriminalité comme l'ensemble des infractions s'effectuant à travers le cyberespace par des moyens autres que ceux habituellement mis en œuvre et de manière complémentaire à la criminalité classique.

[2] On peut citer comme exemple le vol, le terrorisme, l'escroquerie, la diffamation, les injures etc.

[3] Comme infractions on peut citer les atteintes à la confidentialité des données, à l'intégrité des données, à la disponibilité des données etc.

recherche probatoire qui débute à la phase policière soit par l'enquête préliminaire ou l'enquête de flagrance d'une part. Nous pouvons citer comme techniques d'investigation de recherche probatoire la perquisition, les visites domiciliaires, les saisies, l'audition des témoins etc. D'autre part ces actes d'investigation de recherche de preuve ne se limitent pas uniquement à la phase policière, ils se déploient et s'étendent à la phase d'instruction par le juge d'instruction (Spener Yawaga , 2007) qui peut effectuer lui aussi des perquisitions , des saisies, des interrogatoires, des expertises etc et à la phase de jugement. Assurément le juge de jugement est aussi appelé à la recherche de la manifestation de la vérité et par conséquent procède à une instruction définitive (Djorbele Bambe ,2020) en interrogeant d'éventuels témoins, en requérant des expertises, en effectuant des descentes sur le terrain etc.

Ainsi présenté l'enquête pénale dans sa globalité substantielle, il revient de se demander si ces méthodes d'investigation classiques peuvent se déployer dans le cyber espace qui est synonyme de monde virtuel, étant entendu que le réseau internet se singularise par plusieurs aspects à savoir le caractère atérritorial, dématérialisé, et volatil des données. Cette étude est fort intéressante car elle nous permet d'apprécier le déploiement des techniques d'investigation classiques dans le cyberespace et par conséquent nous oriente vers le choix d'une politique criminelle adaptée au contexte cybernétique. Bref il revient de se poser la question de savoir comment le réseau internet influence-t-il l'enquête pénale ? La réponse à cette question est tributaire de la méthode adoptée. En effet la méthode est au cœur de toute recherche juridique. Ainsi il nous échoit d'utiliser comme démarche juridique la méthode exégétique qui nous permettra d'interpréter les textes de loi et notamment le code de procédure pénale et la loi de 2010 relative à la cybersecurité et la cybercriminalité et la méthode de la libre recherche scientifique qui consiste à s'intéresser à certaines décisions de justice qui font office en matière de cybercriminalité. Fort de cette analyse, on constate effectivement que ces méthodes d'investigation classiques de recherche de preuve sont inappropriées à se déployer dans le cyberespace d'où l'inadaptation des techniques d'investigations classiques de recherche probatoire (1) et la nécessité d'instituer de nouvelles techniques d'investigation numériques (2) afin de contrecarrer la montée exponentielle de la cybercriminalité.

1- L'inadaptation des méthodes d'investigation classiques

Les méthodes d'investigation classiques se révèlent inappropriées dans le cyber espace (Halimi, D, 2023). Ceci apparait à travers le particularisme de l'environnement numérique(A) et à travers les insuffisances des méthodes de recherche de preuve classiques face à l'outil internet (B).

1.1- Le particularisme de l'environnement numérique

Le cyberespace s'identifie par plusieurs aspects qui contribuent à fragiliser le déroulement des enquêtes classiques à savoir le caractère extraterritorial et évolutif(1), le caractère dématérialisé de l'enquête et la volatilité des données (2) et enfin par l'anonymat des utilisateurs et la multiplicité des intervenants (3).

1.1.1-le caractère extraterritorial et évolutif

Le cyber espace constitue un village planétaire. Il est perçu comme un espace sans frontières qui se joue non seulement des cadres physiques mais aussi juridiques (Myriam Quemener, Yves Charpenel, 2010). Dès lors les frontières existantes sont bousculées par ce phénomène abaissant la souveraineté des états. Le cyber espace déroge à toute contrainte territoriale. La territorialité ne permet plus de répondre de manière satisfaisante à un besoin croissant de répression des cyber infractions d'où l'inapplicabilité du principe de compétence territoriale dans le cyber espace (Jean Baptiste Maillart, 2018). En effet les cybercriminels, les victimes et les infrastructures techniques se retrouvent sur des territoires distincts, ce qui complique grandement la conduite des enquêtes et les poursuites. C'est ainsi que les différents réseaux emportent la création d'un espace global à la grandeur de la planète. Il est impossible de relier à un territoire précis les relations cyber spatiales et ce surtout à cause de l'ubiquité des informations disponibles au même moment sur le réseau internet et à plusieurs endroits (Mohamed Karim Missaoui, Abdelaziz Elhila, 2021).

Le caractère évolutif de la cybercriminalité se traduit par une criminalité grandissante qui s'effectue dans le cyber espace. Le cyberespace a fait naître de nouveaux comportements qui ne peuvent être sanctionnés par les infractions du Code pénal traditionnel et le juge ne peut donc pas incriminer des faits non qualifiés par la loi (Cica Mathilda Dadjo, 2003). Certes le législateur a rattrapé son retard en élaborant la loi de 2010 sur la cyber sécurité et la cybercriminalité et notamment créé de nouvelles incriminations afin de lutter contre ce phénomène. Toutefois il faut le relever le cyber espace offre aux délinquants de nombreuses facilités de commission d'infraction et ceux-ci deviennent de plus en plus performants et le droit pénal a tendance à être en retard face à cette criminalité galopante et technologique (Marie-Charlotte Roques- Bonnet, 2010).

1.1.2- le caractère dématérialisé de l'enquête et volatil des contenus ou données

Les échanges dans le cyber espace sont entièrement dématérialisés. La dématérialisation peut être définie comme le processus par lequel la manipulation du papier est supprimée, il n'y a plus de support papier et les données sont écrites en langage numérique. A la différence d'un écrit papier, une donnée numérique présente plusieurs caractères spécifiques. La problématique de la preuve est l'une des questions les plus complexes du droit du cyber espace. En effet les saisies et les perquisitions ne s'effectuent pas forcement sur des objets matérialisés ou physiques mais sur des données, des systèmes d'informations ou réseaux informatiques d'où la nature dématérialisée de l'objet de l'activité infractionnelle. Ainsi dans une enquête de cybercriminalité, les enquêteurs de la police judiciaire ou les experts traitent une quantité illimitée et diversifiée de données qui posent des problèmes ayant trait à leur intégrité, loyauté, proportionnalité et de conservation des données (Mahougnon Franc Kai, 2021).

Le caractère fugace ou volatile des données ou contenus s'explique par le fait que les données peuvent être effacées ou modifiées rapidement et par conséquent fragilisent les recherches probatoires effectuées par les autorités policières et judiciaires. Il en résulte un besoin de vitesse dans la recherche et la collecte des données ce qui conduit inéluctablement à la mise en pratique des techniques de stockage et de conservation des données.

1.1.3- L'anonymat des utilisateurs et la multiplicité des intervenants du réseau internet

L'anonymat est un concept essentiel de la protection de la liberté d'expression ainsi que du droit au respect de la vie privée, il constitue l'une des caractéristiques du cyberespace. En effet l'anonymat est particulièrement lié au cyberespace (Lorenzo Ancona , Gabriel Karl, Arnau Marti, et Victor Samek, 2023). L'anonymat peut être défini soit comme le fait d'agir et de communiquer sans utiliser ou présenter son nom ou identité soit comme le fait d'utiliser un nom inventé ou supposé qui n'est nécessairement associé à son identité (Aurelie Jean, 2022.) Beaucoup de malfaiteurs se dissimulent derrière cet état de choses pour commettre des délits sans toutefois être inquiétés ou du moins pendant un certain temps. L'anonymat est visible à plusieurs degrés dans le cyber espace. Prenons le cas dans un cyber café où plusieurs personnes peuvent utiliser le même ordinateur, l'adresse IP[4] qui est un numéro d'identification unique

[4] Une adresse IP(internet Protocol) est un numéro d'identification unique attribué de façon permanente ou provisoire à chaque périphérique faisant partie d'un même réseau informatique utilisant l'internet Protocol. L'adresse IP est à l'origine du système d'acheminement (le routage) des paquets de données sur internet.

attribuée de façon permanente ou provisoire à l'ordinateur ne permettra pas d'identifier l'utilisateur concerné. Il en est de même du proxy[5] et des VPN[6] qui peuvent être utilisés comme des vecteurs de l'anonymisation sur internet. En effet le proxy fait office d'intermédiaire entre un ordinateur et internet et par conséquent certains utilisateurs criminels font recours à ce procédé en vue de masquer l'adresse IP de leurs ordinateurs et notamment leur identité et localisation. La même situation est récurrente dans le darknet ou darkweb où on ne peut accéder que par le navigateur Tor. Ce réseau a été détourné de la main de ses concepteurs pour devenir une niche à promouvoir la criminalité organisée, trafic de drogue, pédopornographie, vente d'armes, commerce illicite d'animaux, proxénétisme ,traite des êtres humains etc. La difficulté que rencontre les enquêteurs sur ce réseau est lié au fait qu'il permet aux criminels d'opérer sous anonymat total (Franc Mahougnon Kai, 2021).

La multiplicité des intervenants dans le cyberespace cause de nombreux problèmes dans la détermination et la mise en jeu de la responsabilité pénale. En effet lorsque l'activité criminelle est réalisée au moyen des réseaux électroniques comme internet, la question de la recherche du responsable pénal prend une dimension toute particulière (Papa Assane Touré, 2014). Le foisonnement des prestataires techniques qui interviennent dans le processus de circulation des informations sur les réseaux rend mal aisé la détermination du responsable de la cyber infraction commise. On assiste donc à des responsabilités en cascade ou à un foisonnement de responsabilités car chacun de ces intervenants a des obligations et le manque de respect de celles - ci entraine des sanctions. Les critères pour juger de la responsabilité se fondent sur les rôles assumés par les différents participants à la chaine de valorisation de l'information (Pierre Trudel, 2000). On distingue les fournisseurs d'accès à internet dit FAI qui sont des sociétés qui fournissent l'accès à internet à un utilisateur particulier ou personne morale désirant se connecter au réseau internet ainsi que les moyens matériels et techniques permettant de bénéficier des services s'appuyant sur ce réseau (Leon Patrice Saar,2010). Ils sont soumis à l'obligation de filtrage et de conservation des données[7]. Ils bénéficient en principe d'un régime d'irresponsabilité. Le fournisseur d'hébergement qui est une personne physique ou morale qui assure même à titre gratuit le stockage et la gestion de contenus permettant à un fournisseur de

[5] Le proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.
[6] VPN signifie virtual private network et décrit la possibilité d'établir une connexion réseau protégée lors de l'utilisation de réseaux publics. Les VPN chiffrent votre trafic internet et camouflent votre identité en ligne.
[7] Voir art 35 a1 de la loi de 2010 relative à la cyber sécurité et à la cybercriminalité.

contenu de rendre ses pages accessibles au public Il a une responsabilité atténuée voire allégée en ce sens que sa responsabilité ne peut être engagée que dans l'hypothèse où il a effectivement eu connaissance de l'activité ou de l'information illicite et qu'il n'a pas agi promptement en vue de retirer les informations ou de rendre l'accès à celles-ci impossible. Autrement dit l'hébergeur doit faire preuve de promptitude dans le retrait du contenu illicite[8]. Le fournisseur de contenu quant à lui produit l'information disponible sur internet. Il existe des fournisseurs de contenu professionnels tels que l'éditeur et d'autres non professionnels tels que le bloggeur. Le fournisseur de contenu est responsable de plein droit de l'ensemble des informations qu'ils publient contrairement aux prestataires techniques qui bénéficient d'une responsabilité aménagée. Enfin il y a l'utilisateur qui se connecte au réseau internet qui peut commettre des infractions spécifiques au réseau internet ou des infractions classiques grâce à l'outil internet.

1.2- Les limites des méthodes d'investigation classiques dans le cyberespace.

L'apparition de la cybercriminalité caractérisée par l'immatérialité de son objet a fini par rendre inapproprié la plupart des moyens d'investigation de recherche de la preuve (Papa Assane Toure, 2014). En effet l'enquête préliminaire relative au meurtre ou l'instruction d'un dossier de vol de chèvre est différente de celle impliquant des cd roms ou des supports physiques de stockage de données. Les méthodes de recherche probatoires se révèlent inadaptées dans le cyber espace. C'est ainsi que la perquisition classique (1) et la saisie classique (2) ne peuvent pas être utilisées dans l'environnement numérique.

1.2.1-L'inadaptation de la perquisition classique dans l'environnement numérique

La perquisition est classiquement définie comme la recherche policière et judiciaire des éléments de preuve d'une infraction. Elle n'est donc pas la simple présence de l'enquêteur sur les lieux de l'infraction ; elle suppose une intrusion, une pénétration à l'intérieur d'un domicile d'une personne privée ou dans les locaux appartenant à une personne morale en vue de la recherche d'objets relatifs aux faits poursuivis. Il peut donc s'agir d'un domicile privé à l'instar d'une maison ou d'un bureau bref à l'intérieur d'un lieu normalement clos. Malheureusement une telle mesure ne peut être prise lorsqu'il s'agit de se rendre dans un lieu virtuel où tout est immatériel (Anatole kobore, 2009). Le monde virtuel est fort différent du monde physique. Il

[8] Art 34a2 de la loi de 2010 sur la cyber sécurité et la cybercriminalité au Cameroun.

n'a ni barrière ni frontière géographique d'où son caractère atterritorial ou transfrontalier. Il ne s'agira pas de perquisitionner un bureau mais un système informatique pour y saisir non pas des documents sur support papier mais des données informatiques qui désignent toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique.

Bien plus la perquisition classique s'effectue dans un espace géographique bien défini et délimité[9]. Il peut donc arriver que lors d'une perquisition nationale, les enquêteurs puissent avoir accès à des systèmes informatiques localisés à l'étranger et liés au système initial faisant l'objet d'une perquisition nationale, dans ce cas quelle est la conduite à tenir ? Est-ce que les enquêteurs peuvent-il légalement accéder à ces systèmes informatiques hébergés à l'étranger ? Ou alors les autorités judiciaires camerounaises doivent-elles délivrer des commissions rogatoires internationales aux autorités judiciaires et policières de ces pays étrangers ? La chambre criminelle de la cour de cassation (arrêt rendu le 6 novembre 2013) a résolu ce problème en énonçant que la consultation des données à l'étranger par les enquêteurs ne constitue pas une nouvelle perquisition mais une simple mesure d'investigation s'inscrivant dans le cadre de la perquisition initiale des locaux. Par conséquent la perquisition numérique contrairement à la perquisition classique peut s'étendre sur des systèmes informatiques situés en dehors du domicile perquisitionné[10] donc élargit la compétence territoriale des autorités policières.

Par ailleurs la perquisition classique est encadrée dans un temps bien limité par la loi. D'après l'article 99(1) du Code de procédure pénale qui affirme que « toute perquisition dans un lieu privé est interdite entre 18 heures et 6 heures du matin ». Or dans l'hypothèse de la diffusion de contenus illicites sur Internet, réseau aux contenus volatiles, le respect de cette règle peut aboutir à ce qu'une infraction commise intervienne en dehors des heures légales de perquisition, et de ce fait interdise la mise en œuvre des mesures tendant à la récupération des éléments de preuve, quand bien même les autorités répressives en seraient informées.

[9] Voir article 177 du Code de procédure pénale.

[10] Cette solution respecte l'intention du législateur en consacrant l'accessibilité des données sur des serveurs différents et éparpillés dans le monde entier depuis le domicile perquisitionné et partant élargit le domaine de compétence des enquêteurs en réduisant considérablement le risque de paralysie dont auraient souffert les services d'enquête et l'engorgement des cabinets de juges dans les enquêtes où la preuve de l'infraction réside.

Bien plus la perquisition classique est opérée en présence du maitre des lieux, du détenteur des biens à saisir ou de leur représentant ainsi que de témoins pris parmi les personnes présentes ou les voisins[11]. Néanmoins il peut arriver qu'une perquisition numerique à distance soit entreprise sans toutefois nécessiter la présence du concerné ou même à l'insu de la personne visée.

Enfin la perquisition classique doit être réalisée en relation avec l'infraction poursuivie cependant lors des perquisitions en matière de cybercriminalité ; l'ensemble des données peuvent être fouillées au peigne fin voire sauvegardées sans toutefois avoir un lien étroit avec l'infraction commise[12].

1.2.2-L'inadaptation de la saisie classique dans le monde numérique

Le dispositif pénal de la saisie conçu pour des objets et documents corporels peut difficilement être transposé au cyberespace. La saisie classique porte sur des objets corporels ou matériels cependant la saisie numérique quant à elle porte sur des biens immatériels. En effet la saisie requiert une soustraction physique de l'objet visé .Comment le juge d'instruction va-t-il se saisir physiquement des données ? L'apposition de scellés, traditionnellement utilisée sur les objets corporels saisis, peut difficilement être mise en œuvre pour les besoins d'une procédure initiée par exemple contre l'auteur du stockage et de la transmission d'informations illicites. Certes, on pourrait, dans ce cas, recourir à la saisie du support des informations. Ainsi, peut-on imaginer des perquisitions qui aboutiraient à la saisie des disques durs d'une entreprise ou d'un individu, dans le but de pouvoir prendre connaissance de quelques fichiers stockés dans la mémoire de l'ordinateur, qu'il s'agisse d'images pédophiles, de contrefaçons au droit d'auteur, de données de navigation et d'accès non autorisé à des sites et systèmes informatiques tiers (Anatole Kabore, 2009). Cependant la saisie de l'ensemble du matériel informatique d'une entreprise ou d'un

[11] Voir art 93 du Code de procédure pénale.

[12] [12] En effet les perquisitions numériques aboutissent à une collecte en masse des données. Lors du dépouillement et l'analyse de celles-ci certaines données recueillies peuvent ne pas avoir de relation ou de lien direct avec l'infraction commise, dans ce cas celles –ci peuvent être détruites sur instruction du procureur de la république pour des raisons de sécurité et de préservation des libertés individuelles des parties concernées. Ainsi seules seront gardées les données pouvant être utilisées pour la manifestation de la vérité.(art 53 (2-3) de la loi de 2010 sur la cybercriminalité.

individu soupçonné de détenir des copies illicites d'un logiciel est de nature à lui causer des dommages particulièrement irréversibles[13].

Par conséquent il faut aménager ces techniques de recherche de preuve classiques jugées inadaptées et même d'instituer de nouvelles techniques d'investigation.

2-L'institution de nouvelles techniques d'investigation numériques.

Les outils procéduraux aux fins de la recherche des preuves numériques ont dû s'adapter aux évolutions technologiques afin de freiner l'action des cyberdelinquants (Myriam Quemener , Yves Charpenel, 2010). Dans un souci réel d'étendre les pouvoirs d'investigation des enquêteurs et des magistrats, la loi de 2010 sur la cybercriminalité a mis sur pied de nouveaux mécanismes procéduraux de recherche de preuve. Ces nouvelles techniques de recherche probatoire parfois revisitées ont pour but essentiel de permettre aux autorités policières et judiciaires d'accéder et d'obtenir des données pour des besoins d'investigation en vue de la manifestation de la vérité. Il faut distinguer d'une part des techniques d'investigation numériques intrusives (2.1) et des techniques d'investigation numériques collaboratives (2.2)

2.1-Les techniques d'investigation numériques intrusives

Il faut entendre par techniques numériques d'investigation intrusives, des actes permettant la recherche par des actions fortes parfois coercitives des enquêteurs (Bruno Roussel ,2020). C'est un véritable arsenal procédural qui est aujourd'hui mis à la disposition des enquêteurs pour procéder à des investigations numériques intrusives. Dans le cadre de la présente étude, il est préférable de répartir les investigations numériques intrusives selon la méthode qui permet d'obtenir des données. Une première catégorie regroupe les données qui sont traitées lors d'actes de fouilles. Le mot « fouille » se réfère à l'action « d'explorer minutieusement un lieu pour trouver quelque chose, quelqu'un » (dictionnaire grand Larousse illustré, 2023). En procédure pénale il s'agit donc de fouiller des supports contenant des données pouvant permettre à la manifestation de la vérité, il s'agit précisément de la perquisition numérique(1) et la saisie électronique ou numérique(2) qui constitue le résultat des fouilles. Une seconde catégorie réunit les données qui sont générées ou collectées lors de l'exécution d'actes de

[13] La cour de cassation dans un arrêt du 14 novembre 2001 admettait déjà que la copie du disque dur du système informatique effectuée par un expert doit avoir pour but de perturber le moins possible le fonctionnement de l'activité du saisi.

surveillance (3). Cette surveillance est tout aussi intrusive dans la vie privée que les actes de fouille, mais elle se déroule systématiquement à l'insu de l'individu visé par la mesure. Nous citons à cet effet les interceptions et la géolocalisation.

2.1.1-La perquisition numérique ou en ligne

Elle est prévue à l'article 53 alinéa 1 de la loi de 2010 portant répression de la cyber sécurité et la cybercriminalité. Elle constitue l'une des mesures les plus importantes dans les enquêtes aussi bien policières que judicaires. Seuls les officiers de police judiciaire, les agents spécialisés de L'ANTIC[14] et le juge d'instruction sont habilités à procéder à des perquisitions. La perquisition numérique permet de faciliter le déroulement de l'enquête dans le monde virtuel en permettant l'accès aux données informatiques, la captation de ces données et la conservation ou le stockage de ces données pour les utiliser comme preuve (Nadir Ouchene, 2018). La perquisition peut avoir lieu dans le domicile d'un individu et elle s'effectuera sur le matériel informatique de ce dernier notamment lap top, disque dur, disquette, clé USB. Bref elle va porter sur des objets matériels, des supports physiques contenant des données ou des copies, telle est la substance de l'article 53 a 1 de la loi de 2010 qui affirme que « les perquisitions en matière de cybercriminalité sont susceptibles de porter sur les données qui peuvent être des supports physiques ou des copies réalisées en présence des personnes qui assistent à la perquisition ». Il revient donc de se demander si le législateur de 2010 limite –t-il la perquisition qu'aux données contenues dans les supports physiques et ne l'étend pas sur les systèmes informatiques ? Autrement dit Peut-on dire qu'une perquisition sur les systèmes informatiques n'est pas possible au Cameroun ? En effet les articles 14 et19 de la convention de Budapest[15] donnent la possibilité à toute partie prenante à la convention de procéder à la perquisition sur un système informatique ou à une partie de celui. Ainsi l'article 14 de la convention de Budapest ayant trait à la portée d'application des mesures du droit de procédure impose aux parties prenantes d'instaurer les pouvoirs et les procédures prévues dans la présente convention et sauf disposition contraire chaque partie applique les pouvoirs et les procédures

[14] Les agents de l'ANTIC ont effectué des perquisitions dans l'affaire Ministère Public c/ Biloa Atangana Brigitte Christelle Alias Cynthia Fianga et ont constaté que son compte Facebook avait été piraté et par conséquent n'était pas à l'origine de la publication d'images obscènes.

[15] Le Cameroun a adhéré à la convention de Budapest sur la cybercriminalité, adoptée le 23 novembre 2001 à Budapest (Hongrie) par un décret no 2022/169 du 23 mai 2022. On attend par adhésion l'acte par lequel un état accepte l'offre ou la possibilité de devenir partie à un traité déjà négocié et signé par d'autres Etats. L'adhésion se produit lorsque le traité est déjà entré en vigueur. L'adhésion a le même effet juridique que la ratification.

mentionnés ci-dessus. Malheureusement le Cameroun n'a pas encore pris de manière explicite des mesures internes[16] visant à appliquer pleinement la convention. Néanmoins une lecture minutieuse de la loi de 2010 sur la cybercriminalité et la cybersecurité fait montre que le législateur incrimine des atteintes à la confidentialité, à la disponibilité et à l'intégrité des données et des systèmes informatiques [17] et de ce fait les enquêtes sur les systèmes informatiques peuvent donc être effectuées en vue de constater la commission ou non des dites atteintes et notamment par le biais les perquisitions. La perquisition en ligne comme la perquisition classique est encadrée afin d'éviter des abus et assurer le respect des droits des personnes perquisitionnées. Ainsi la cyber perquisition ne peut se faire qu'en présence de la personne perquisitionnée ou des personnes trouvées dans le dit domicile qui peuvent être réquisitionnées pour fournir les renseignements sur les objets, documents et données. La présence de la personne perquisitionnée ou d'un tiers lors de la perquisition est justifiée par le souci d'éviter que le concerné ne conteste ultérieurement la perquisition effectuée en son absence ainsi que la découverte d'objets compromettants. En outre la perquisition numérique ne peut s'effectuer que pour collecter les éléments de preuve sur l'infraction dont le juge a été saisi (Papa Assane Toure, 2014). Par ailleurs la perquisition en ligne doit respecter les heures légales de perquisition à savoir de 6h à 18h[18]. Cependant des difficultés peuvent surgir lors d'une perquisition en ligne à distance, il peut arriver qu'une perquisition autorisée par le juge et soit effectuée à distance et à tout moment dans les locaux des agents de l'ANTIC sans que le suspect ou l'inculpé soit informé ou soit présent. Une telle perquisition peut-elle être valable au regard de la loi ? Le juge camerounais n'a pas encore eu l'occasion de se prononcer sur cette question cependant en France la perquisition informatique à distance existe depuis la loi n0 2003-239 du 18 mars 2003, l'article 57-1 alinea2 dispose que l'accès à des données distantes contenues sur un système informatique est possible. Ainsi les enquêteurs peuvent accéder depuis leurs locaux aux données stockées sur l'ordinateur d'un suspect situé n'importe où. Autrement dit l'enquêteur peut alors fouiller à distance les données présentes sur un ordinateur connecté, lire, conserver et stocker les fichiers.

[16] Comme par exemple son homologue sénégalais en son nouvel article 677-36 du Code de procédure pénale

[17] Art 60 et suivants de la loi de 2010 sur la cybersecurité et la cybercriminalité.

[18] Art 99 Code de procédure pénale.

Néanmoins un flou existe toujours dans l'encadrement du système de la perquisition informatique car les règles d'administration de celle-ci souffrent généralement du manque de clarté aboutissant à un vide législatif et mettant en branle les droits des personnes perquisitionnées. Il serait donc judicieux pour le législateur de prendre des mesures claires et précises en vue d'un encadrement judicieux de la perquisition numérique soucieuse du respect des garanties de protection des libertés individuelles des personnes perquisitionnées (Samuel Tepi, 2020). Quid de la saisie électronique ?

2.1.2 -la saisie électronique ou numérique

La saisie est normalement le résultat d'une perquisition fructueuse. Lorsque la perquisition effectuée révèle l'existence de données ou d'objets susceptibles de contribuer à la manifestation de la vérité, il peut procéder à leur saisie d'où l'article 53a3 de la loi de 2010 qui affirme « sur accord du procureur de la république, seuls seront gardés sous scellés par l'officier de police judiciaire, les objets, les documents et données utilisés à la manifestation de la vérité ». La saisie est donc la mise d'un bien sous-main de la justice. Elle peut donc s'effectuer soit par la saisie du support physique de ces données soit par une copie de ces données. Par saisie du support physique des données, il faut entendre tout objet avoir servi à la commission de l'infraction, c'est le cas par exemple du support de stockage qui fait l'objet d'une telle mesure. Il s'agit-là de l'application du principe de spécialité aux saisies. Ainsi lorsque les éléments de preuve sont contenus sur des supports matériels tels que cd-room , disquettes, clé USB, les enquêteurs peuvent sans difficulté particulière les placer sous-main de la justice. Les objets et documents saisis sont immédiatement inventoriés et placés sous scellés. Les scellés ne seront ouverts et dépouillés que dans le cabinet du juge d'instruction en présence de l'intéressé ou des tiers, chez qui la saisie a eu lieu. Tout de même la saisie des supports tangibles est délicate[19], périlleuse et exige en conséquence une méthode pour préserver la preuve de l'infraction.

[19] C'est par exemple le cas de la saisie de l'ordinateur ou du matériel informatique d'une entreprise ou d'un individu soupçonné de détenir des copies illicites d'un logiciel est de nature à lui causer des dommages particulièrement irréversibles. La cour de cassation française dans un arrêt du 14 novembre 2001 admettait déjà que la copie d'un disque dur du système informatique effectuée par un expert désigné par le juge doit avoir pour but de perturber le moins possible le fonctionnement de l'activité du saisi. En tout état de cause cette mesure est tout à fait inconcevable lorsque les données utiles à la manifestation de la vérité sont disséminées dans tout le système informatique d'une entreprise ou les données litigieuses sont stockées sur un serveur qui abrite les données d'autres personnes que celle visée par l'enquête, tel est le cas pour les serveurs hébergeant une multitude de sites internet la saisie du serveur perturbe alors également les services des personnes tierces. C'est aussi le cas des services de stockage dans le nuage en anglais Cloud ou les données d'un même utilisateur peuvent être stockées sur une multitude de serveurs

Lorsque la saisie des supports physiques est impossible, le juge d'instruction ou l'enquêteur réalisent l'opération par copiage des données sur des supports de stockage informatique pouvant être matériellement saisis et placés sous scellés. La loi n'a pas précisé la nature des supports de la saisie mais ils peuvent être des bandes magnétiques, des cartes mémoire, des disques durs externes etc. Ces copies seront donc dépouillées en vue de la recherche de la manifestation de la vérité et l'enquêteur peut constater que ces données saisies sont inintelligibles pour avoir été cryptées ou codées par les cybercriminels , dans ce cas la loi lui donne la possibilité de réquisitionner toute personne physique ou morale qualifiée en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair des dites données[20].

Il peut s'en suivre qu'une copie des données saisies a été faite et que celle-ci soit détruite sur instruction du procureur de la république pour des raisons de sécurité.[21] Il peut s'agir des données contraires à l'ordre public, aux bonnes mœurs, ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées (virus, chevaux de troie).

Néanmoins il peut arriver que le copiage soit impraticable pour des raisons techniques liées notamment au volume des données stockées dans le système qui excède ses capacités de support de l'autorité de saisie, dans ce cas le blocage de l'accès des données constitue un substitut à la copie des données devenue impossible.

2.1.3- Les actes de surveillance dans la recherche de la preuve numérique

On peut citer comme acte de surveillance dans la recherche de la preuve numérique les interceptions des données relatives aux contenus des communications et la géolocalisation. Concernant les interceptions des données, il faut signaler que l'affirmation du principe de la confidentialité des données électroniques souffre des dérogations tenant aux nécessités d'ordre public de l'enquête. En effet le juge d'instruction peut utiliser les moyens techniques appropriés pour collecter ou enregistrer le contenu des communications transmises au moyen d'un système informatique en recourant à des experts en la matière. Les articles 44a1 et 49 de la loi de 2010 relative à la cybersecurité permettent aux juges et aux officiers de police judiciaire de collecter et d'enregistrer en temps réel les données relatives au contenu des communications. Nous

[20] Art 55a 1de la loi de 2010 la cybersecurité et la cybercriminalité.

[21] Art 53 a2 de la loi de 2010 sur la cybersecurité et la cybercriminalité.

entendons par intercepter le fait de s'emparer de ce qui est adressé, envoyé à quelqu'un. L'interception s'applique aux données relatives au contenu de communication encore appelées données de contenu qui constituent le sens de la communication ou l'information véhiculée par la communication en dehors des données relatives au trafic[22] et des données de connexion[23]. Il peut s'agir des données transmises par le biais des réseaux sans fil dont les systèmes de téléphonie mobile que celles communiquées au moyen des réseaux informatiques (données, vidéos, etc). Ce moyen d'investigation obéit à la condition de nécessité et de proportionnalité vérifiée en fonction de l'implication de l'inculpé dans les faits. L'opération d'interception fait général appel à des services techniques d'un expert en informatique. L'autorité judiciaire a également la faculté de mettre à la charge du fournisseur de services l'obligation de collecter ou d'enregistrer les données de contenu et de garder le secret[24].

Cependant il faut le souligner l'équilibre entre la sécurité et la liberté a quelque peu été rompu par le choix législatif d'étendre cette procédure à risque pour les libertés individuelles à l'enquête préliminaire. En effet la liberté donnée aux officiers de police judiciaire de procéder aux opérations d'interception nous parait dangereuse pour les libertés individuelles dont le seul garant est l'autorité judiciaire (Papa Assane Toure, 2014). En effet en cas de commission d'infraction cybernétique, les OPJ dans le cadre soit de l'enquête flagrante ou de l'enquête préliminaire seraient habilités à intercepter des courriers électroniques sans le consentement des intéressés ni requérir une autorisation judiciaire, ce qui nuit gravement aux libertés individuelles.

Toutefois les enquêteurs éprouvent d'énormes difficultés à mettre en œuvre les opérations d'interceptions découlant sur l'identité des auteurs de l'infraction du fait des cyber cafés non règlementés, de l'utilisation des données mobiles et Le VPN ou virtual private Network[25] . Cette situation offre aux cyberdelinquants un havre de paix pour mener en toute quiétude leurs agissements délictuels. Même si les enquêteurs peuvent retracer l'adresse IP jusqu'à dans un

[22] On entend par données relatives au trafic toute donnée traitée en vue de l'acheminement d'une communication sur un réseau de communication électronique ou pour la facturation de cette communication et comprend les données relatives à l'acheminement, à la durée ou à l'heure d'une communication

[23] On entend par données de connexion, toute donnée relative au processus de connexion à un système informatique

[24] Il s'agit d'assurer la confidentialité des communications interceptées et en même temps garantir l'efficience de cette mesure intrusive par nature qui n'est efficace que si elle est effectuée à l'insu des personnes faisant l'objet de l'enquête. Voir art 51 de la loi de 2010 sur la cybercriminalité et la cyber sécurité.

[25] [25] Le VPN est un réseau crypté qui empêche l'interception des données et rend difficile la localisation de l'utilisateur en dissimulant son adresse IP. Dès lors le fournisseur d'accès ainsi que les enquêteurs n'ont que de faibles marges de manœuvres pour intercepter vos données d'utilisateurs.

cybercafé, le problème de rattachabilité de l'acte fait défaut parce qu'aucune mesure permettant d'identifier les usagers ou clients n'est prise par le gérant (Dr Papa Gueye, 2018).

Quant à la géolocalisation, elle constitue un moyen d'enquête efficace permettant de déterminer la localisation de façon plus ou moins précise d'un objet ou d'une personne par le biais d'un système de GPS[26] ou d'un téléphone mobile (Laurent Benoît, Cyril Roth, Gildas Barbier, Pascale Labrousse,2014). La géolocalisation est obtenue par les données générées par l'utilisation d'un objet numérique en temps réel lors du fonctionnement naturel de cet objet. Il s'agit généralement du téléphone mobile d'un individu d'où la géolocalisation par le bornage du téléphone. En effet tout objet connecté à un réseau de téléphonie mobile génère des données de localisation. Ainsi, le réseau de téléphonie mobile repose sur un maillage d'antennes relais réparties sur le territoire couvert par ce réseau. Pour fonctionner, l'objet communicant doit se connecter à l'une des antennes relais. C'est ce que l'on nomme le bornage. Les magistrats sont parfaitement familiarisés avec ce vocabulaire[27] puisqu'ils n'hésitent pas à employer ce mot dans leurs décisions. Bien évidemment, au sein des objets connectés, c'est le téléphone mobile qui intéresse le plus, potentiellement, les enquêteurs car il est le plus souvent porté en permanence par son propriétaire. Il permet donc de géolocaliser indirectement un individu. Par conséquent les enquêteurs adressent une demande d'activation du bornage de l'appareil à l'opérateur de téléphonie mobile qui leur fournira un historique du bornage de l'appareil.

La géolocalisation est particulièrement intrusive dans la vie privée pour la personne visée par la mesure, puisqu'elle permet de connaître, en permanence, la totalité de ses déplacements, y compris ceux qui n'ont rien à voir avec des agissements délictuels ou criminels. Il était donc indispensable de placer cet acte sous le contrôle d'un juge, ce qui n'était pas le cas avec la loi de 2010 sur la cybercriminalité et la cybersécurité[28] .

La recherche de la preuve numérique ne se fait pas seulement par l'usage des techniques intrusives d'investigation, elle passe aussi par les techniques collaboratives d'investigation numérique (2.2)

[26] TGI de Yaoundé Centre administratif, jugement no 4587 /CRIM du 24 juillet 2021, Affaire Ministère public et Onana Jean c/ Lissouck Gabriel. Il s'agit du meurtre du fils du plaignant dont le téléphone avait été dérobé lors de l'agression et retrouvé grâce à la technique de géolocalisation.
[27] TGI de Yaoundé Centre administratif, jugement no 4587 /CRIM du 24 juillet 2021, Affaire Ministère public et Onana Jean c/ Lissouck Gabriel
[28] Voir art 52a3 de la loi de 2010 sur la cybersecurité et la cybercriminalité.

2.2-les techniques collaboratives d'investigation numérique

Nous entendons par techniques collaboratives d'investigation numérique, des méthodes impliquant la participation de chaque acteur dans la recherche de la preuve numérique. En effet le cyberespace se particularise par une multitude des acteurs à savoir les prestataires techniques qui sont les fournisseurs d'accès à internet, les fournisseurs de service de communication électroniques, les fournisseurs de contenus et les exploitants de systèmes d'information et les internautes. Il est donc de bon ton d'impliquer tous ces acteurs à la croisade contre la cybercriminalité. L'approche retenue par la loi de 2010 sur la cybersecurité et la cybercriminalité constitue une démarche de politique criminelle participative (Yves Poullet, François Lerouge, 2002). A ce propos le législateur de 2010 a donc institué des obligations à chaque acteur notamment aux fournisseurs d'accès internet qui sont tenus de conserver les données qui peuvent plus tard faire l'objet des réquisitions(2.2.1) et aussi aux personnes physiques ou morales qui ont des aptitudes à mettre en clair les données cryptées d'où le déchiffrement (2.2.2). Toutefois il faut le souligner l'irruption du réseau internet constitue de nos jours l'illustration parfaite de la montée en puissance du phénomène international, le cyberespace s'identifie à un espace aterritorialisé, un réseau sans frontières terrestres. Ce glissement du phénomène criminel de la sphère locale vers l'international impose une internationalisation de la réponse à la cybercriminalité[29] d'où la coopération internationale (2.2.3).

2.2.1-Les réquisitions judicaires aux fins de communication des données

Les prestataires techniques sont tenus de conserver des données de trafic, de connexion et de contenus pendant une période de 10ans[30]. Ils ont l'obligation de mettre à la disposition des enquêteurs ces données lors des investigations judicaires et sont astreints au secret professionnel[31]. Ce mécanisme de conservation des données constitue un formidable moyen d'investigation pour les autorités judiciaires. Ces données stockées constituent une aide

[30] Voir article 29a1, art 25a1, 35a1de la loi de 2010 sur la cybercriminalité. En effet le délai de conservation sous d'autres cieux est plus court à l'instar de la France qui est de 1 an. La loi de 2010 a préféré adopter le délai de 10 ans afin que les informations détenues par les prestataires techniques soient toujours disponibles même si l'enquête prend du temps d'autant plus que plusieurs mois peuvent s'écouler entre la commission de l'infraction et la recherche des preuves et aussi pour contrecarrer les lenteurs judiciaires qui peuvent être observées dans les enquêtes cybernétiques. Voir à ce propos Tepi Samuel, *la cybercriminalité au Cameroun, enjeux d'une législation en quête d'efficacité,* Harmattan, 2020, p97.

précieuse dans la recherche des cyber délinquants[32]. En effet le juge d'instruction peut sur nécessité de l'instruction ou de l'enquête requérir les opérateurs de télécommunication, de fournisseurs d'accès à internet de mettre à sa disposition les informations utiles à la manifestation de la vérité via les données stockées dans les systèmes informatiques qu'ils administrent[33]. Cette conservation exige que les données qui sont stockées soient protégées contre tout ce qui risquerait d'en modifier ou d'en dégrader la qualité ou l'état actuel.

Cependant cette technique d'investigation peut mettre à mal le respect des libertés individuelles. La rétention des données et la transmission de celles-ci pose un problème d'atteintes aux libertés individuelles. En effet les réseaux électroniques sont devenus les supports de la malveillance informatique et il est de bon ton que les organes répressifs de l'état, soucieux de vaincre l'impunité dans le cyber espace aient adopté comme moyen d'investigation la traçabilité des internautes. Cela risquerait d'engendrer une dérive sécuritaire préjudiciable à la protection de la vie privée bref aux droits et libertés des personnes. Le sort funeste de l'internaute serait tracé en permanence d'où le nécessaire compromis de trouver un équilibre entre la sécurité des personnes et le respect des droits fondamentaux des celles-ci (Papa Assane Toure, 2014). C'est tout le débat de la protection de la vie privée dans le cadre de la lutte contre la cybercriminalité.

Par ailleurs l'obligation de conservation des données pose également un problème de coût très important. Les fournisseurs de service internet, petites ou grandes entreprises devront assumer le coût de stockage des données, de la formation du personnel entrainant considérablement des dépenses de plus en plus élevées parfois préjudiciables pour la survie des petites entreprises.

[32] Comme l'a fait valoir le garde des sceaux en France Marylise Lebranchu « les évènements récents ont démontré que l'utilisation des moyens de télécommunication, des réseaux numériques et de l'internet était au cœur des échanges d'informations entre les membres des réseaux terroristes. De telles enquêtes supposent que puissent être exploitées les données enregistrées par les opérateurs de télécommunications. Ces données sont en effet des traces laissées par les intéressés dans le monde virtuel comme seraient des empreintes dans le monde réel. »

[33] TPI de Yaoundé Centre administratif, jugement n0 2215/ COR du 05 avril 2022, Affaire Ministère Public et Ngo Mayka C/ Emessi Kevin, inédit. Il s'agit d'une tentative d'intrusion dans un réseau, le prévenu a tenté de pirater le compte Orange Money de la plaignante et le juge de céans a demandé une réquisition aux fins de communication des données à l'opérateur de téléphonie mobile Orange Money. TPI de Yaoundé Centre administratif, jugement n02703/ COR du 22 mai 2023, Affaire Ministère Public et Beyala Bikanda Christelle Claudia c/ Eba Anicet Joseph Marie, inédit. Il s'agit ici d'un chantage et publication illicite par voie électronique et une demande de communication des données a été faite à l'operateur de fournisseur d'accès à internet Camtel.

2.2.2-Le déchiffrement

L'utilisation croissante du chiffrement par les particuliers et les entreprises permet d'assurer un niveau élevé de confidentialité[34] sur internet. Logiquement cette généralisation du cryptage ou chiffrement handicape fortement les enquêtes judiciaires, ainsi pour faciliter celles-ci le législateur a trouvé opportun d'instaurer les articles 55 et 88 de la loi de 2010 relative à la cybersecurité et à la cybercriminalité. En effet lorsque les données saisies ou obtenues au cours d'une enquête ou de l'instruction ne sont pas claires, les autorités judiciaires peuvent réquisitionner toute personne physique ou morale d'obtenir la version en clair des dites données. Il peut donc s'agir des experts qui pourront traduire en termes compréhensibles les données cryptées. Cependant il n'est pas aisé pour ces experts de lever le secret de ces données cryptées (Nadir Ouchene ,2018) et pour venir à bout de cette difficulté que la loi a institué que le déchiffrement puisse aussi s'opérer par toute personne ayant connaissance de la convention secrète de déchiffrement ou d'un moyen de cryptographie susceptible d'avoir été utilisé pour préparer , faciliter ou commettre un crime ou un délit. En cas de refus le dit contrevenant sera sanctionné d'un emprisonnement de trois ans à cinq ans et d'une amende de un million à cinq millions[35]. Dans la même lancée l'assemblée plénière de la cour de cassation [36] estime que refuser de remettre aux enquêteurs la clé de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer ou commettre un crime ou délit peut être pénalement sanctionné. Cependant cette décision de l'assemblée plénière pose une nouvelle fois le problème du respect de la vie privée et la lutte contre les nouvelles formes de criminalité en affaiblissant le droit à ne pas s'incriminer.

2.2.3-La coopération internationale

L'infraction cybernétique est par nature une infraction transnationale. Afin de lutter contre cette forme de criminalité, la coopération internationale est donc indispensable. La loi de 2010 sur la

[34] Les avantages du chiffrement sont nombreux à savoir la confidentialité, l'intégrité, l'authenticité d'un document

[35] Art 88 de la loi de 2010 sur la cybersecurité et la cybercriminalité.

[36] Il s'agit d'une affaire de trafic de stupéfiants dans laquelle un homme interpellé en possession de cannabis et soupçonné de détenir sur ses téléphones des informations pouvant faire progresser l'enquête a refusé de communiquer les codes permettant le déverrouillage de son téléphone. Le tribunal correctionnel de Lille et la cour d'appel de Douai ont estimé que le suspect était dans son bon droit sur ce point puisque le code de deverourraillage de son téléphone ne constituait pas une convention de déchiffrement mais la chambre criminelle de la cour de cassation a censuré cette décision. Voir Cass. Ass. Plen, 7 novembre 2022, no 21-83146.

cybersecurité et la cybercriminalité met un point d'honneur sur la coopération internationale dans ses articles 91 à 94 à travers l'extradition, l'entraide judiciaire, la coopération policière, la reconnaissance mutuelle des jugements étrangers (Tepi Samuel, 2020). Dans le cadre de la lutte contre la cybercriminalité le procédé le plus adapté est la coopération juridique entre les états d'une part et la coopération entre les autorités policières et judiciaires d'autre part.

En effet l'articulation des réponses nationales au phénomène encouragé par des documents pertinents de la société de l'information est certes nécessaire mais illusoire si elle est exclusive d'où une riposte coordonnée et concertée. L'on a même parlé de la nécessité de l'élaboration d'une politique criminelle mondiale (Siméon Patrice Kouam, 2018) en vue de la création d'un droit pénal mondial du cyberespace. Cela est possible par les instruments juridiques internationaux à l'instar de la convention de Budapest[37] contre la cybercriminalité, la convention de l'union africaine sur la cybersecurité et la protection des données à caractère personnel, le projet de convention de l'union africaine sur la mise en place d'un cadre juridique de confiance pour la cybersecurité en Afrique. L'harmonisation de la répression internationale contre la cybercriminalité est incontournable car mettra fin aux divergences de vue entre les états sur les valeurs à protéger[38] dans l'univers numérique et favorisera l'intensification de la coopération policière et judiciaire. Celle-ci est visible à travers certains organismes à l'instar d'Interpol qui s'investit dans les enquêtes sur la cybercriminalité, propose de nouvelles technologies innovantes et des formations aux autorités policières des états membres. Quant à l'aspect de la coopération judiciaire, elle regroupe les mécanismes de l'entraide judiciaire à l'instar de l'extradition, la recherche des preuves dans un système ou un réseau situé hors de son territoire ou même solliciter l'accomplissement d'un acte d'instruction à l'étranger (Papa Assane Toure, 2014).

Conclusion

En définitive l'outil internet a fortement révolutionné le monde et par conséquent est au cœur de tout développement de la société. Malgré ses avantages considérables, le réseau internet traine derrière lui beaucoup de casseroles. En effet l'évolution des mœurs entraine inéluctablement de nouvelles formes de criminalité et l'outil internet n'échappe pas à cette

[37] Le Cameroun a adhéré à la convention de Budapest sur la cybercriminalité, adoptée le 23 novembre 2001 à Budapest (Hongrie) par un décret no 2022/169 du 23 mai 2022.

[38] Ceci participera à éradiquer les paradis pénaux où les cyber délinquants pourront se réfugier en toute impunité.

règle. Il est donc impérieux de réglementer ce nouvel espace en créant des incriminations et de sanctionner tout contrevenant. Toutefois la nature singulière du réseau internet rend la répression un peu plus difficile car bouleverse l'ordre pénal classique notamment les méthodes traditionnelles d'appréhension de la criminalité. Les méthodes d'investigation conçues et élaborées pour un environnement matérialisé et national se sont vite révélées inappropriées et inadaptées pour saisir la nouvelle réalité du crime. La numérisation de notre société, dont la donnée informatique est le support, a des conséquences sur la dématérialisation des investigations au sein de l'enquête. Comment donc faire pour procéder à des investigations dans un contexte global de numérisation ? Comment peut- on appréhender la donnée informatique en vue de la recherche des preuves ? La loi de 2010 sur la cybersecurité et la cybercriminalité répond à ce questionnement en éditant des nouvelles techniques d'investigation probatoires à savoir des méthodes intrusives d'investigation numérique (perquisition numérique, saisie numérique , interceptions des données relatives aux contenus de communication, géolocalisation) et les techniques collaboratives d'investigation numérique (les réquisitions judiciaires aux fins de communication des données, le déchiffrement, la coopération internationale). Cependant la plupart de ces techniques d'investigation numérique connaissent des limites voire des insuffisances d'où le vide juridique observé dans certains aspects de leur mise en œuvre et par ricochet heurtent le respect des libertés individuelles. De ce fait il y a lieu de se poser la question de savoir si l'ordre public numérique est-il supérieur au respect des libertés individuelles des citoyens ? On comprend que les organes répressifs de l'état sont soucieux de vaincre l'impunité dans le cyber espace mais ils doivent rechercher tout aussi un équilibre entre la sécurité des personnes et le respect des droits fondamentaux de celles-ci d'où le débat incessant entre la protection de la vie privée et la sécurité dans le cyber espace.

.

Bibliographie

Ouvrages généraux

-Dr Papa Gueye, (2018). *Criminalité organisée et terrorisme et cybercriminalité : réponses de politiques criminelles*, Harmattan.

-Judith Rochfed, Martial Braz, (*2019). Droit des données personnelles. Les spécificités du droit français au regard du RGPD,* Dalloz.

-LAURENT Benoît, ROTH Cyril, BARBIER Gildas, LABROUSSE Pascale, *(2014). Géolocalisation par suivi dynamique du téléphone portable : conditions de licéité au regard de l'article 8 de la Convention européenne des droits de l'homme,* Recueil Dalloz.

-Myriam Quemener, Yves Charpenel (2010). *Cybercriminalité : droit pénal appliqué*, Economica.

-Papa Assane Touré(2014). *Le traitement de la cybercriminalité devant le juge, l'exemple du Sénégal*, Harmattan.

-Samuel Tepi, (2020). *La cybercriminalité au Cameroun, enjeux d'une législation en quête d'efficacité*, Harmattan.

-Spener Yawaga, (2007). *L'information judiciaire au Cameroun dans le code camerounais de procédure pénale,* Presses universitaires d'Afrique.

Articles

-Djorbele Bambe, (2020). « Le procès pénal camerounais entre l'accusatoire et l'inquisitoire » International Multilingual journal of science and technology, p 1053-1073.

-Halimi, D. (2023) « les contraintes relatives aux procédures d'investigation sur les cybercrimes », revue internationale du chercheur.4, 4, p 237-256

-Nadege Ingridgouanlong kamgang, Tchari Adam Boukar. (2023). « Les facteurs explicatifs de l'achat via les réseaux sociaux par les camerounais : une analyse du point de vue des consommateurs », revue internationale du chercheur, 4,4 p 1268-1300

-Mohamed Karim Missaoui, Abdelaziz Elhila, (2021). « Le droit pénal et l'éthique à l'épreuve de la cybercriminalité », revue scientifique marocaine, vol4, no 2, p 128-145

-Pierre Trudel, (2000). « Les responsabilités dans le cyberespace », les dimensions internationales du droit du cyberespace, collection Droit du cyberespace, Paris, éditions UNESCO, Economica, p 235-269

-Siméon Patrice Kouam, (2018). « Les mouvements du champ pénal au Cameroun. Contribution à l'étude des transformations contemporaines du droit pénal », revue africaine de droit et de science politique, Vol 6, no 13, p 62-115

Thèses- mémoires

-Anatole kobore, (2009). La problématique des perquisitions et saisies en ligne en Afrique de l'ouest : état des lieux et perspectives cas du Burkina Faso, du Mali, du Sénégal et du Togo, mémoire de master professionnel, université Gaston berger.

-Bruno Roussel, (2020). Les investigations numériques en procédure pénale, thèse, université de Bordeaux.

-Cica Mathilda Dadjo, (2003). Les contrats dans le cyber espace à l'épreuve de la théorie générale : problèmes et perspectives, mémoire de maitrise en droit des affaires et carrières judiciaires, université d'Abomey Calavi.

-Jean Baptiste Maillart, (2018). Le principe de compétence territoriale à l'épreuve de la cybercriminalité, thèse, université de Genève.

-Leon Patrice Saar, (2010). La répression de la cybercriminalité en droit sénégalais à l'épreuve de l'anonymat dans le cyber espace, mémoire de master, université cheikh Anta Diop,

-Mahougnon Franc Kai, (2021). La preuve numérique à l'épreuve de la cybercriminalité, mémoire de master, université de Limoges.

-Nadir Ouchene, (2018). L'applicabilité de la loi pénale à l'endroit de la cybercriminalité dissimulée, thèse, université de Paris II Panthéon Assas.