International Multilingual Journal of Science and Technology (IMJST)
ISSN: 2528-9810
Vol. 6 Issue 7, July - 2021

La Preuve Du Cybercrime, Les Victimes À La Traversée D'un Labyrinthe

Job NZOH SANGONG

Docteur Ph/D, Assistant à l'Université de Ngaoundéré

RESUME

Dans les cyber-relations, on côtoie le risque. On s'y cultive à l'anéantir, et on déploie aussi allégrement tous les moyens pour l'évincer. Or, le risque zéro dans les relations en général et dans le monde des affaires en particulier n'existe pas. Un tel postulat est renchéri dans les cyber-relations par la virtualité des échanges, l'absence des parties prenantes, la malléabilité des contenu, et partant, de l'incertitude de leurs identités réciproques. La notion de preuve est à cet effet importante, car elle préside à la sécurité des transactions. Sur Internet, la preuve des cybercrimes s'avère complexe au regard des possibilités matérielles et techniques lui permettant d'usurper des identités, voire de se travestir d'une part et de manipuler, falsifier et crypter les documents et contenus numériques. Ainsi, au-delà de l'identification et de la production des preuves qui sont un préalable de sécurité juridique des transactions, il parait crucial de relever qu'il s'en dégage une interrogation jusque-là inédite celle de la pertinence des preuves des cybercrimes ? Cela étant, prouver le cybercrime est une aporie processuelle pour les victimes internautes et pour les autorités judiciaires. En effet, la conduite d'un procès pénal relatif à la cybercriminalité expose la victime et le ministère public à deux principaux écueils : l'identification du cybercriminel et la preuve de son infraction. Il en résulte une complexité de l'identification du cybercriminel d'une part et une instabilité des documents et contenus cybercriminels d'autre part.

Mots clés : internaute, cybercriminel, victime, preuve, identité, cybersécurité, cybercriminalité.

INTRODUCTION

«Je m'avance masqué.» Cette assertion de Réné DESCARTES prend tout son sens avec l'avènement du cybermonde. Ce nouvel espace informatisé qui ne prend forme qu'habillé des pixels de nos écrans, où des millions d'ombres aux noms bizarres de menaces à nos individualités estampillées. Espace criminogène, le cyberespace[1] se caractérise pour les « cyberphobes » par l'escroquerie en ligne, vol d'identité, diffamation, *cybersquatting* et *phishing* notamment. Ces quelques « cybercrimes » paraissent pour certains évidents à prouver et certains un peu moins. À la vérité, il n'est rien, car ces cyber infractions sont généralement commises par des internautes pas toujours identifiables et de plus, la valeur probante des preuves obtenues par les victimes est très mitigée. Cependant, l'époque des craintes irraisonnées est révolue, de nombreuses recherches ont montré que les jeunes sont beaucoup plus habiles et rationnels qu'on ne le pense généralement dans la gestion de leur identité en ligne et à la manipulation des contenus numériques. Mais pour qui n'est pas déjà immergé dans ce « nouveau monde », il est essentiel de comprendre qu'il s'agit bien d'un nouvel espace public qui peut être occupé par des identités privées, numériques et variables, aux contenus numériques versatiles au gré des nécessités. Et comme l'identité piagétienne dans la « vraie vie » et l'écrit manuscrit, ces éléments de preuves, possiblement numériques se construisent ou se péjorent au gré des navigations et des rencontres dans cet espace d'un nouveau genre. Il en résulte que la constitution de la preuve des cyber infractions s'avère être un véritable serpent de mer pour les internautes victimes. Le dynamisme de ces concepts appelle à des clarifications sémantiques.

Les preuves sont les faits pertinents au moyen desquels la culpabilité ou l´innocence d´une personne est établie lors d´un procès[2]. Les preuves électroniques comprennent toutes les preuves existant en forme digitale ou électronique. Les preuves électroniques sont fondamentales, non seulement dans le cadre des poursuites et des enquêtes sur la cybercriminalité, mais de plus en plus pour la criminalité en général. Les cadres juridiques

[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 ». Dans ses écrits, le « cyberespace » s'agissait d'un espace utopique et abstrait où circule l'information. Voir Martin DODGE, *Mapping Cyberspace* éd. New York, Routledge, 2001, p. 1 ; Voir aussi Pierre TRUDEL, « Les Responsabilités dans le Cyberespace » in Teresa FUENTES – CAMACHO : *Les Dimensions Internationales du Droit du Cyberespace*, Paris, Economica, 2000 ; James BARLOW, un des paroliers de Grateful dead et auteur de la « Déclaration d'Indépendance du Cyberespace » a repris cette expression pour designer l'espace créé par les réseaux d'ordinateurs. Voir <http://www.elf.org/barlow/~library.html> (visité le 08/12/2003).

[2] Gérard CORNU, *vocabulaire juridique de l'association Henri Capitant*, 10e éd. paris, PUF (quadrige), 2014, preuves.

optimises pour les preuves électroniques, ainsi que la capacité des services répressifs et de la justice pénale d´identifier, de collecter et d´analyser les preuves électroniques, sont donc essentiels pour une riposte efficace contre la criminalité.

L'infraction encore appelée crime au sens large peut être définie comme l'acte qui est sanctionné par une peine[3]. Une liste des actes serait impossible à dresser. En effet, son importance varie selon les époques et les pays. Par exemple, des actes comme le suicide, le blasphème, l'hérésie, la sorcellerie, l'homosexualité, qui étaient incriminés en France au Moyen Âge ne le sont plus aujourd'hui. Inversement, des incriminations nouvelles sont apparues dues à des facteurs comme l'industrialisation[4] ou l'accroissement de la solidarité humaine[5] et l'émergence de nouvelles formes de crime[6]. L'infraction a ainsi trois éléments constitutifs à savoir : élément légal : un comportement n'est une infraction légale que si un texte étatique le dit[7]. L'élément matériel : il n'y a d'infraction légale que si les actions ou omissions reprochées à la personne poursuivie ont bien été commis. L'élément moral : il n'y a d'infraction légale que si le fait matériel a été commis par une personne apte à comprendre et à vouloir. Transposée dans le cybermonde, les cybercrimes doivent être compris comme les infractions dont les éléments matériels sont produits sur la toile.

Étymologiquement, le terme « victime » pourrait être rattaché à *vincere*, *vici*, *victum*, et ainsi désigner la personne vaincue[8]. Pourtant, c'est du latin classique *victima*, signifiant « bête offerte en sacrifice aux dieux » que proviendrait le terme moderne de « victime », apparu au XVème siècle[9]. Eu égard à cette origine, le terme a longtemps conservé une signification théologique[10] avant que celle-ci ne soit étendue jusqu'à le conduire à désigner toute personne souffrant des agissements d'autrui. En droit, la victime est classiquement une notion antagoniste, définie comme la personne qui subit un dommage par opposition à celle qui le cause[11], généralement afin de permettre à celle-ci de demander réparation du dommage à celle-là. Parmi l'ensemble des victimes, certaines se voient reconnues par le droit et notamment par le droit pénal. À l'inverse du droit civil ou du droit administratif ayant essentiellement vocation à protéger les victimes et à leur assurer réparation des dommages qu'elles subissent, le droit pénal s'inscrit dans une démarche répressive. En droit pénal, la victime est celle dont la souffrance provient de la commission d'une infraction, infraction dont il conviendra de sanctionner l'auteur. De façon précise, les textes camerounais en la matière ne produisent pas une véritable définition de la notion de victime. Au niveau interne[12], selon l'article 61 du Code de procédure pénale camerounais, l'action civile en réparation du dommage causé par une infraction appartient à tous ceux qui auront personnellement souffert du dommage directement causé par cette infraction. Le dommage doit donc avoir été directement causé par l'infraction et personnellement subi par la personne en cause. Lorsque ces deux conditions sont remplies, cette personne peut être qualifiée de victime de l'infraction, ou de partie lésée.

Paradoxalement, les victimes des cyberinfractions, en plus d'être les parties lésées lorsque survient le fait dommageable sont confrontées aux difficultés probatoires desdites infractions. En effet tout d'abord, malgré les innombrables manières dont les identités numériques sécurisées et vérifiables sont utilisées, la majorité des utilisateurs d'Internet est aujourd'hui plus facile à identifier qu'avant. Cet état de faits pourrait rendre périlleuse aux victimes l'identification des cybercriminels. Ensuite, l'informatique offre aux cybercriminels de grandes possibilité non seulement de falsifier les éléments susceptibles de les incriminer mais également de brouiller leurs traces à travers la technique du cryptage. Enfin, à l'issue éventuelle de cet impasse, la question de la force probante des potentiels preuves obtenues se posera avec acuité. C'est la raison pour laquelle la présente étude situe les personnes ayant subi des faits dommageables répréhensibles sur la toile comme étant à la croisée

[3] V. Bernard BOULOC et HARITINI MATSOPOULOU, droit pénal général et procédure pénale, sirey, 19e éd. 2014, p. 20.

[4] Infractions en matière de sécurité routière, du droit du travail.

[5] Il s'agit de l'omission de porter secours à autrui, abus de la faiblesse d'autrui.

[6] La piraterie maritime, le terrorisme, le coupeur de route…

[7] Ceci est appelé "le principe de légalité des infractions" selon la formule latine *« nullum crimen nulla poena sine lege »*. Ce principe a été inventé par FEURBACH au 19e siècle. Son sens moderne a pris véritable son départ avec BECCARIA dans traité des délits et peines de 1764.

[8] Yves JEANCLOS, *Dictionnaire de droit criminel et pénal. Dimension historique*, Economica, coll. Corpus Histoire du droit, 2011, n° 151, entrée « Victime ».

[9] *Dictionnaire historique de la langue française*, ss la dir. d'A. REY, éd. Le Robert, 2004, entrée « victime ».

[10] V. Jean AUDET et Jean -François KATZ, *Précis de victimologie générale*, Dunod, 2ème éd., 2006, pp. 5 et 6.

[11] *Vocabulaire juridique*, ss la dir. de Gérard CORNU, Association Henri Capitant, PUF, coll. Quadrige, 10ème éd., 2014, entrée « Victime ».

[12] Au niveau international, l'article 1er de la Déclaration des principes fondamentaux de justice relatifs aux victimes de la criminalité et aux victimes d'abus de pouvoir, adoptée par la Résolution n° 40-34 de l'Assemblée générale de l'O.N.U. du 29 novembre 1985, définit les victimes comme « *des personnes qui, individuellement ou collectivement, ont subi un préjudice, notamment une atteinte à leur intégrité physique ou mentale, une souffrance morale, une perte matérielle, ou une atteinte grave à leurs droits fondamentaux, en raison d'actes ou d'omissions qui enfreignent les lois pénales en vigueur dans un État membre, y compris celles qui proscrivent les abus criminels de pouvoir* ».

d'un labyrinthe[13], lorsqu'il s'agit de produire des faits pertinents au moyen desquels la culpabilité ou l´innocence de leurs « bourreaux » est établie lors d´un procès. Il s'agit de d'analyser les risques d'égarement auxquels victimes et ministère public peuvent être confrontés dans l'administration des preuves de cybercrimes.

Il faut le relever, si les nouvelles TIC participent de manière positive au développement de la vie économique[14], elles présentent aussi, comme déjà relevé, de nouveaux moyens de commettre des infractions d'affaires, ce qui fait apparaître des dangers non négligeables, vue l'importance qu'elles ont désormais acquise. Au cœur de cette ambivalence cybernétique se trouve la preuve des cyber infractions. En effet, l'identification est le préalable nécessaire à la mise en œuvre des notions telles la personnalité juridique et ses pendants : le patrimoine et la responsabilité notamment. L'identification est ainsi l'un de ces mécanismes d'aménagement des droits et obligations de la personne par le droit et partant de rattachement des preuves à un délinquant. Dans le champ juridique en général, la preuve tend à amener la règle de droit à se saisir des droits de la personne prise dans son individualité, de son rattachement à une infraction, c'est-à-dire à devenir un outil pour régler l'imputation d'un fait à une personne précise. La preuve sur les réseaux numériques constitue un sujet d'actualité au vue de la multiplication des comportements délictuels sur le net. Son administration à de nombreuses conséquences juridiques. En ce sens, la preuve de l'identification des utilisateurs peut apparaitre comme étant un problème juridique bien spécifique au réseau internet. Toutefois, l'anonymat dans le cyberespace facilité par plusieurs techniques constitue un obstacle majeur pour l'identification des internautes délinquants[15]. En effet, plusieurs personnes sont capables de dissimuler, falsifier leur identité, leurs faits de telle sorte qu'elles puissent déambuler sur internet d'une manière quasi-invisible. Cette notion de preuve se retrouve de fait au cœur de la dialectique confidentialité et cybersécurité. Pour l'internaute, la preuve de son identité est autant un atout de choix dans ses rapports sociaux et dans ses affaires, autant elle permet également, lorsqu'elle est fictive, usurpée de stimuler la commission des cyberinfractions[16] d'une part et de rendre aporétique les procédures judiciaires notamment.

L'avènement du web ne rend pas impossible la production des preuves. En effet, les preuves sont avant tout susceptibles de production dans le monde matériel. Il en ressort une utilité indubitable des preuves traditionnelles[17] qui peuvent être associés à ceux qu'offre la technique. Pour ce faire, la présente étude n'entend pas se limiter à l'analyse des éléments probatoires des cyber infractions, mais accordera une attention particulière sera également accordés aux différentes manipulations informatiques que peuvent subir les preuves et leur traitement juridiques. Il serait faux de croire que les questions et problèmes soulevés par la preuve des cybercrimes sont épuisés et définitivement tranchés. Malgré de nombreuses études déjà réalisées[18] avant la présente, la question de la pertinence des preuves des cybercrimes demeure. On ne pense pas travestir les idées émises dans ces études en disant qu'il s'en dégage une interrogation jusque-là inédite : quelle est la pertinence des preuves des cybercrimes ?

En effet, ces études, en présentant les éléments d'identification de l'internaute en général et ceux participant de la construction de l'identité numérique en particulier d'une part, et la recevabilité et fonction probatoire des contenus et documents numériques sont restées prémonitoires à la question de la pertinence des preuves des cybercrimes. Elles servent de fondation au postulat d'un possible régime juridique des preuves des cybercrimes. Cela étant, il convient de relever que la question est au demeurant très intéressante, car elle est au cœur de la dialectique du droit substantiel et du droit processuel. Dans un premier temps, la quasi-totalité des relations dans le monde physique exige des protagonistes qu'ils se connaissent, du moins que les identités soient connues en prélude à la constitution de toute preuve. Le monde virtuel ne s'affranchit pas d'une telle exigence. En effet, elle permet de démontrer que l'identification de l'internaute permet *a priori* d'assurer une prévisibilité de cyber-relations non seulement en exaltant un climat de confiance entre les parties prenantes, mais également en anticipant sur l'issue éventuellement triste de leur relation. Dans un second temps, en considération de la récurrence de partenaires peu scrupuleux d'affaires, il importe de

[13] Edifice d'antiquité composé d'un grand nombre de chambre et de galeries dont la disposition était tel, que ceux qui s'y engageaient parvenaient difficilement à en trouver l'issue.

[14] Joseph FOMETEU, « l'influence des moyens électroniques sur le droit des contrats », *Actes du colloque sur » Les pratiques contractuelles d'affaires et les processus d'harmonisation sur les espaces régionaux*, Libreville du 26-28 octobre 2011, *Publication ERSUMA*, juin 2012, p. 214.

[15] Solange GHERNAOUTI, *La cybercriminalité : le visible et l'invisible*, Collection le savoir suisse, 2009, p. 17.

[16] Jacques VETOIS, *Technologies et usages de l'anonymat sur internet*, éd. l'Harmattan, 2012, p. 42.

[17] Il s'agit notamment des documents écrits qui peuvent être transposée aux TIC. Il s'agit des documents numérisés, des témoignages des aveux.

[18] François FILLIETTAZ, « Comprendre l'identité numérique », *DIP DSI-SEM*, 2011, pp. 2-20 ; Jeanine MARTELLIET Anne-Sophie GRENIER, « l'identité numérique », *Journées du réseau DV IST* 9 avril 2013, pp. 3-39 ; Vincent GAUTRAIS et Patrick GINGRAS, « La preuve des documents technologiques », *Les Cahiers de propriété intellectuelle*, Vol. 22, nº 2, 2010, pp. 268-313.

pouvoir les identifier pour qu'ils répondent de leurs actes. Ainsi, la nécessité d´identifier, de collecter et d´analyser les preuves électroniques par l´entremise de la criminalistique numérique est d'un enjeu crucial. Elle examine la recevabilité et l´utilisation des preuves électroniques lors d´un procès et montre comment de multiples difficultés en matière de poursuites peuvent avoir une incidence sur la performance du système de justice pénale. Elle fait le lien entre les besoins de capacités des services répressifs et de la justice pénale, et des activités d´assistance technique requise et octroyée. Ainsi, il en résulte *a posteriori* que la production des preuves irréfragables des cybercrimes est un préalable procédural impératif à la lutte contre la cybercriminalité.

Au Cameroun, l'arsenal juridique applicable aux e-relations[19] fournit des réponses notoires au questionnement sus-relevé. La prévention de la cybercriminalité fait partie intégrante de toute stratégie nationale de cybersécurité et de protection des infrastructures essentielles de l'information, ce qui comprend notamment l'adoption d'une législation appropriée contre l'utilisation des TIC à des fins criminelles ou autres et contre les activités visant à nuire à l'intégrité des infrastructures essentielles du pays. Au niveau national, il s'agit là d'une responsabilité commune, qui demande de la part des autorités, du secteur privé et de la population une action coordonnée en matière de prévention, de préparation, de résolution des incidents. Au niveau régional et international, cela suppose une coopération et une coordination avec les partenaires concernés. C'est le lieu de relever les efforts règlementaires consistants du législateur CEMAC en la matière, et embryonnaires pour le législateurs OHADA. En Collationnant ces textes nationaux, communautaires et internationaux, il en ressort une possibilité alambiquée d'apporter des moyens permettant d'établir sur des faits la culpabilité ou l'innocence de l'accusé lors du procès. Il pourrait recourir à de fichiers informatiques, de transmissions, de relevés, de métadonnées ou de données réseau. La criminalistique numérique a pour objet de récupérer des informations souvent instables, au regard leur manipulation aisée et facilement contaminées, ces documents peuvent avoir une valeur probante. Cela étant, prouver le cybercrime est une aporie processuelle pour les victimes internautes et pour les autorités judiciaires. En effet, la conduite d'un procès pénal relatif à la cybercriminalité expose la victime et le ministère public à deux principaux écueils : l'identification du cybercriminel et la preuve de son infraction. Il en résulte une complexité de l'identification du cybercriminel d'une part et une instabilité des documents et contenus cybercriminels d'autre part.

I- La complexité de l'identification du cybercriminel

En conjuguant ces textes nationaux, communautaires et internationaux, il en ressort une possibilité d'identification des cybercriminels. Toutefois, les techniques disponibles sont cantonnées à l'identification des internautes professionnels[20] par les moyens juridiques consacrés, de nature à exclure les internautes non-professionnels. (A) Par ailleurs, le cybermonde a connu l'avènement des moyens techniques d'identification. En l'espèce, on peut constater pour le déplorer une précarité fonctionnelle des mesures techniques susceptibles de contribuer à l'identification des internautes(B).

[19] Au niveau national, on peut noter la Loi n° 2010/21 du 21 décembre 2010 régissant le commerce électronique au Cameroun, http://www.legicam.org ; Loi n° 2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun, http://www.legicam.org; Loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et la cybercriminalité. La loi n°2010/013 du 21 décembre 2010 régissant les communication électroniques au Cameroun , http://www.legicam.org; Loi-cadre n° 2011/012 du 6 mai 2011 portant protection du consommateur, http://www.minpostel.gov.cm; Décret n° 2012/1318/PM du 22 mai 2012 fixant les conditions et les modalités d'octroi de l'autorisation d'exercice de l'activité de certification électronique, www.minpostel.gov.cm; Décret n° 2012/1640/PM du 14 juin 2012 fixant les conditions d'interconnexion, d'accès aux réseaux de communications électroniques ouverts au public et de partage des infrastructures, www.minpostel.gov.cm Le décret n°2013/0399/PM du 27 février 2013 fixant les modalités de protection des consommateurs des services de communication électronique http://www.legicam.org. Au niveau communautaire, on note le Règlement n°21/08-UEAC-133-18 relatif à l'harmonisation des réglementations et des politiques de régulation des communications électroniques au sein de la CEMAC ; Ces directives sont : La Directive n°06/08-UEAC-133-CM-18 fixant le régime du service universel dans le secteur des communications électroniques au sin de la CEMAC ; La Directive n°07/08-UEAC-133-CM-18 fixant le cadre juridique de la protection des droits des utilisateurs des réseaux et services de communications électroniques au sein de la CEMAC ; La Directive n°08/08-UEAC-133-CM-18 relative à l'interconnexion et à l'accès des réseaux et des services de communications électroniques dans les pays membres ; La Directive n°9/08-UEAC-133-CM-18 portant harmonisation des régimes juridiques des activités de communications électroniques dans les Etats membres de la CEMAC ; La Directive n°10-11 portant harmonisation des modalités d'établissement et de contrôles des tarifs et services de communications électroniques des Etats membres de la CEMAC. On y ajouter l'Acte uniforme relatif au droit commercial général en son livre V traitant de l'informatisation du RCCM et l'Acte uniforme relatif au droit des sociétés commerciales et les groupements d'intérêts économiques.

[20] Le recours à la notion de professionnel permet de prendre en considération commerçants et entreprenants notamment de l'AUDCG.

A- L'exclusivité professionnelle des mesures juridiques identificatrices

Globalement, les actes de cybercriminalité sont amplement répartis entre des infractions de nature financière et des infractions liées au contenu informatique, et incluent également des actes contre la confidentialité, l´intégrité et la disponibilité des systèmes informatiques. On peut y percevoir une omniprésence de la criminalité dans le cybermonde. Cependant, compte tenu de la virtualité de cet environnement, de l'ubiquité des internautes et de leur capacité à se dissimuler dans leurs odyssées virtuelles, il est crucial de pouvoir les identifier. A la lecture de l'arsenal juridique camerounais, plusieurs moyens juridiques peuvent contribuer à identifier les internautes criminels. Toutefois, ces moyens sont caractérisés par leur limitation à l'identification des internautes professionnels (1). Il en résulte un affranchissement des internautes du secteur informel (2), de nature à éprouver les différents moyens juridiques existants.

1- La limitation des moyens juridiques à l'identification des professionnels

L'internaute avant de recours au web est d'abord un acteur ordinaire du monde des affaires. Ainsi, il ne saurait s'affranchir totalement des moyens d'identification des acteurs du monde des affaires. Par ailleurs, les moyens juridiques d'identification des internautes ont connu une évolution du fait du dynamisme des législateurs national, communautaire et international. Ce dynamisme permet de distinguer deux catégories de moyens d'identification. Certains sont dits classiques et d'autres nouveaux. Dans les deux cas, il en résulte une insuffisance des moyens classiques et une relégation des moyens nouveaux d'identification des internautes.

Sur l'internet comme déjà mentionné plus haut, les identifiants traditionnels utilisés dans le monde réel, comme le nom, le prénom, l'adresse, le sexe, les photographies., se retrouvent naturellement. Si tous les individus ont une identité, les éléments identifiants varient de l'un à l'autre, .d'un groupe social à un autre, d'une société à une autre. À l'évidence, l'espace et le temps dans lesquels une personne vit et évolue exercent une influence sur son identité[21]. Cette influence n'a aucune incidence sur le contrat et les identifiants traditionnels. Les règles classiques du droit commun des contrats et du droit des affaires offrent un ensemble de moyens importants susceptibles de contribuer à l'identification des internautes, et partant, des cybercriminels. Ces moyens sont dits classiques. Les moyens classiques d'identification des internautes criminels sont de deux ordres. Les premiers sont issus des règles contractuelles et les seconds ressortent des différentes obligations de publicité légale faites aux professionnels.

Dans l'univers classique, plusieurs éléments permettent d'identifier la personne physique ou morale. Pour les premières, plusieurs éléments participent de leur identité. Traditionnellement, les identifiants les plus évocateurs, composant l'état civil sont : le nom, le prénom, le sexe, la date de naissance, le domicile. Plus largement, peuvent être inclus tous les éléments caractérisant l'individu et de nature à lui donner un sentiment d'identité[22]. Les personnes morales présentent aussi des identifiants les caractérisant. Il s'agit notamment du nom, statut, adresse, nom des représentants, nationalité et siège social[23]. En matière contractuelle, ces éléments se trouvent requis dans les différentes obligations d'information. Ces obligations d'information vont de la publicité[24] à l'information contraction, en passant par l'obligation précontractuelle d'information[25] à travers les offres contractuelles[26]. Les différentes dispositions légales traitant de ces obligations mettent en première ligne les divers identifiants susmentionnés.Ainsi, le contractant se déployant dans le web est soumis à un ensemble d'obligations d'information garantissant son identification et une protection de son cocontractant. Le respect de ces obligations et surtout de véracité et clarté des informations y afférentes conditionnent la validité du contrat susceptible d'en résulter. En outre, les cocontractants peuvent en faire une condition sine qua non de leur engagement.

Dans le même ordre d'idées, les professionnels au sens du droit OHADA sont soumis à des mesures de publicité légales. En effet, avec la consécration du statut de l'entreprenant par l'article 30 de l'AUDCG, la notion de professionnel sied mieux à la désignation des acteurs du mondes des affaires. Elle inclut commerçants[27] et entreprenants. Ces acteurs sont soumis respectivement aux formalités d'immatriculation et de déclaration. Comme informations à produire dans l'accomplissement de ces formalités se trouvent les différents identifiants

[21] Pour une illustration : Céline CASTETS-RENARD, « Vie privée du salarié et TIC : attention à la violation de la charte informatique ! », note sous Cass. Soc., 15 déc. 2010 ; *RLDI* 2011/69, n° 2270. Pour une analyse d'ensemble : Céline CASTETS-RENARD, « TIC et droit du travail », *Jcl Communication*, LexisNexis, Fasc. n° 4820.

[22] Daniel GUTMAN, *Le sentiment d'identité*, préf. François TERRÉ, LGDJ, Thèses, Bibl. droit priv., 2000, t. 327.

[23] Paul Gérard POUGOUE et Athanase FOKO, *Le statut du commerçant dans l'espace OHADA.: une prospective à l'épreuve du droit matériel uniforme OHADA*, PUA, Yaoundé, 2005, pp. 66-69.

[24] V. Article 5 de la loi de 2010 relative au commerce électronique.

[25] V. Article 15 de la loi de 2010 relative au commerce électronique.

[26] V. Article 30 de la loi de 2010 relative au commerce électronique.

[27] André Desmonds EYANGO DJOMBI, « La nouvelle définition du commerçant dans l'Acte uniforme OHADA au regard de la théorie de l'acte de commerce », *Revue de droit des affaires OHADA*, n° 02, juin-décembre 2012, p. 243.

précédemment mentionnés. De plus, avec l'informatisation du registre du commerce et du crédit mobilier (RCCM) consacrée par le livre V de l'AUDCG, ces formalités peuvent s'accomplir via documents électroniques et les dossiers sont consultables en ligne[28]. Cet état de chose rend accessible l'identité de tous les professionnels à travers les fichiers locaux, nationaux et régional[29]. La commission d'infractions par ces acteurs n'est pas de nature à affranchir les professionnels de toute responsabilité. Dans le même temps, l'identité des professionnels s'avère également accessible lorsque ces derniers recourent aux moyens techniques, *a priori* conçus pour des besoins de sécurisation. Malgré leur faible attrait, ces moyens permettent d'identifier l'internaute. La relégation dont ils sont victimes est donc déplorable.

En vue de l'émission des certificats électroniques, autorités de certification assure le relai entre l'Agence et les demandeurs de certification. Il est tout de même déplorable de noter que les internautes ne font pas montre d'un enthousiasme particulier à l'égard de ces mécanismes nouveaux. Force est de relever que les professionnels se montrent être les internautes les plus attirés par ces moyens. En effet, le certificat électronique subit une double relégation. D'une part, il ne séduit pas véritablement les non-professionnels. Ce défaut d'attractivité est justifié par le formalisme y afférent qui s'avère non seulement lourd[30], mais également soumis à renouvellement et actualisation annuelles. D'autre part, les professionnels qui manifestent leur intérêt pour cette technique de sécurisation ne sont pas légion[31]. Ainsi, il ressort que les mesures juridiques d'identification se servent des identifiants traditionnels. Ces identifiants que l'on retrouve dans les diverses obligations d'information, dans les obligations de publicité légale et dans les mesures nouvelles de sécurité des internautes sont de nature à permettre d'identifier les internautes, et partant, les cybercriminels exerçant une activité professionnelle. Toutefois, on peut constater une double limite en ces mesures : un cantonnement aux cybercontractants d'une part et un désintérêt des internautes non professionnels d'autre part. Cela pourrait conduire à un postulat d'affranchissement des internautes du secteur informel.

2- L'affranchissement des internautes du secteur informel des mesures d'identification

Le secteur informel couvre toutes les formes d'activités de production des biens, mais surtout de services effectués à petites échelles et échappant totalement ou partiellement aux obligations institutionnelles, fiscales et d'assurance. Au Cameroun, le secteur informel n'est plus pour les pouvoirs publics camerounais synonymes d'économie illicite. Dès lors que les professionnels qui y opèrent s'acquittent des obligations dont ils sont tenus, les pouvoirs publics leur permettent d'exercer leurs activités et de faire concurrence à un opérateur du secteur formel à moins que l'activité à laquelle ils se livrent soit de celles qui leur sont interdites. Il en résulte un secteur informel toléré et un secteur informel interdit. Dans les deux cas, il est difficile d'identifier ces acteurs. De plus, les mineurs, acteurs non susceptibles d'exercer des activités professionnelles sont une véritable aporie d'identification.

Les pouvoirs publics camerounais ont doté le secteur informel d'un statut juridique qui tient compte de la taille de leur exploitation. Ce statut est contenu dans trois textes. [32] Tout d'abord le premier texte fixe d'une part les conditions d'exercice du commerce ambulant et d'autre part les conditions de vente sur la voie publique. Ensuite, le deuxième répartit les commerçants en trois groupes, intègre les petits commerçants dans le groupe 3 : commerçants ambulants, *buy and sellam*, vendeur à la sauvette. Les conséquences de cette catégorisation des commerçants exerçant dans ce secteur informel sont les suivants : les commerçants du groupe 3 sont tenus de se faire immatriculer sur le répertoire ouvert à cet effet auprès de la commune de leur lieu d'activité ou de leur principal point d'attache. Ils sont également tenus de s'inscrire au registre statistique. Ils sont enfin tenus de se faire délivrer une carte professionnelle dont la détention est obligatoire. Enfin, le troisième introduit dans le Code Général des Impôts, un article 50 nouveau qui institue pour les contribuables exerçant une activité commerciale ou industrielle ne relevant ni du régime du bénéfice réel ni du régime simplifié d'imposition un impôt libératoire exclusif du paiement de la patente, de l'impôt sur le

[28] Job NZOH SANGONG, *La documentation électronique dans l'Acte Uniforme portant Droit Commercial Général*, Mémoire de Master Recherche, Université de Ngaoundéré, 2013, pp. 32-50.

[29] V. Fabius Corneille KAMLA FOKA, « Le Registre du Commerce et du Crédit Mobilier (RCCM) OHADA depuis la réforme du 15 décembre 2010 : de la transformation à la transfiguration », *RDA* 1ère année de parution, 2012-n°1, pp.189-205.

[30] V. La procédure de délivrance d'un certificat électronique, Livre Blanc de l'ANTIC, Les systèmes d'infrastructures à clé publique, édition de juin 2015, pp. 37-38.

[31] V. Ministère des postes et des télécommunications, Plan Stratégique Cameroun Numérique 2020, 2016, p. 17.

[32]Il s'agit de l'arrêté n° 045/CAP/MINDIC du 15 novembre 1991 réglementant le commerce ambulant. Ce texte fixe d'une part les conditions d'exercice du commerce ambulant et d'autre part les conditions de vente sur la voie publique ; le décret n° 93/720/PM du 22 novembre 1993 fixant les modalités d'application de la loi n° 90/031 du 10 août 1990 régissant l'activité commerciale au Cameroun. Ce texte qui ; la loi n° 96/08 du 01 er juillet 1996 portant loi de finance de la république du Cameroun pour l'année 199-1997.

revenu des personnes physiques et de la taxe sur la valeur ajoutée.

Le professionnel du secteur informel se distingue du traditionnel à travers la dématérialisation de ses activités due à l'utilisation d'Internet. Ainsi, la dématérialisation de ses activités, en dépit des avantages, pose deux séries de problèmes dues à l'ubiquité et à la dépersonnalisation. L'ubiquité se manifeste par le fait que le site Internet du professionnel du secteur informel est accessible presque partout. La dépersonnalisation crée des risques dus d'une part, au défaut de présence physique des parties contractantes et d'autre part, à l'utilisation du support électronique pour conclure le contrat. L'objectif est d'anéantir les effets néfastes de l'ubiquité et de la dépersonnalisation dans le but de sécuriser l'environnement du professionnel du commerce électronique. Les formalités de publicité légale confrontées à la dépersonnalisation revitalisent l'intérêt de l'identification.

Les exigences sus-évoquées permettent d'envisager un registre des acteurs du secteur informel toléré, selon leurs catégories respectives. Cependant, à la lecture de cette règlementation du secteur informel toléré, force est de constater que le législateur camerounais n'a pas conçu ces règles pour les internautes. De plus, à l'observation, de nombreux internautes se sont spécialisés en vente en ligne et ont développé une nouvelle forme de secteur informel qui échappe à la règlementation en vigueur. Cet état de chose est de nature à faire de ce nouveau secteur informel un *far west* virtuel susceptible d'optimiser la commission des infractions axées autour du vol d'identité, de la concurrence déloyale et de l'escroquerie.

Sur la toile, le commerce des objets d'occasion tels que les matériaux de construction, les pièces d'automobile et des appareils électroniques électro ménagers de toute sorte est devenu un véritable circuit d'écoulement des objets volés. Ce type de commerce est devenu de plus en plus constant et se développe informellement sur la toile. Par ailleurs, il est plus difficile d'identifier les acteurs en cas d'infraction, du fait de leur affranchissement à tout registre d'identification institutionnel.

Dans une autre perspective, il faut relever que les mineurs sont des personnes vulnérables, en considération de leur statut d'incapable. Pour ce faire, ils méritent une attention juridique particulière. Sur la toile, la vulnérabilité des mineurs est optimisée. En effet, les atteintes aux droits des mineurs sont une réalité du développement des TIC à laquelle sont confrontés les États du monde entier[33]. Les Codes, civil et pénal, distinguaient les mineurs des adultes. Le critère de l'âge semble toutefois avoir été un premier élément de différenciation de ces deux catégories. De prime à bord, les mineurs sur Internet sont destinataire de protection. Les atteintes aux mineurs sont une réalité du développement des TIC à laquelle sont confrontés les États du monde entier[34]. Cette technologie permet aux jeunes d'accéder facilement et parfois involontairement[35] à des sites potentiellement traumatisants[36]. Pour cette raison, une attention particulière doit être portée sur eux. Il est possible pour un site Web d'orienter certaines, voire la totalité de ses activités vers ces nouveaux internautes, les enfants constituant une importante part de marché que ce soit en termes d'audience, de fréquentation ou encore de revenus. Cependant, les mineurs ne sont pas que victimes sur le web. Ils sont également des potentiels cybercriminels.

Par conséquent, le traitement accordé aux internautes-adultes doit être étendue aux internautes-enfants. En effet, tout comme les adultes, ils doivent pouvoir être mis en cause selon les règles pénales relatives à la responsabilité. Face à cela, on peut se demander quelle est la valeur d'un acte commis par un enfant ? Ce dernier est-il en mesure de réaliser toutes les implications reliées aux actes commis avec l'ordinateur de ses parents ? La réponse parait évidente. Si dans l'univers matériel on est responsable dès l'âge de 10ans, Internet ne devrait pas se soustraire à cette règle.

La difficulté pourrait résider de la commission des infractions par les enfants de moins de 10ans d'une part, et dans la détermination de l'âge de l'internaute avant son identification. Dans un premier temps, l'irresponsabilité des mineurs de 10ans peut être réaffirmée. Dans un second temps, les internautes mineurs en âge de responsabilité pourraient être difficilement identifiables. En effet, leur exclusion de la sphère des activités professionnelles les soumet à l'exercice dans un secteur essentiellement informel. Ainsi, ils bénéficient du même affranchissement à leur identification que les professionnels du secteur informel. Toutefois, doit-on clamer péremptoirement leur affranchissement de toute responsabilité ? L'avènement des mesures techniquement d'identification des internautes invite relativiser la réponse à cette question.

B- La précarité fonctionnelle des mesures techniques identificatrices

Sur Internet, il existe des procédés techniques permettant de suppléer la défaillance des moyens

[33] Rosalie DIARRA, *La répression de la cybercriminalité en Afrique de l'ouest*, L'Harmattan, 2021, p. 157.

[34] Jean-Claude VIMONT, « Des coupables aux victimes, l'archéologie de l'identité du mineur délinquant au XIXe siècle », *Revue d'histoire de l'enfance « irrégulière »* [En ligne], 18 | 2016, p. 7.

[35] Rosalie DIARRA, *La répression de la cybercriminalité en Afrique de l'ouest*, L'Harmattan, 2021, p. 167.

[36] Myriam QUEMENER « Réponses pénales face à la cyberpédopomograpgie ». *Actualité Juridique pénale* n° 3/2009, édition Dalloz 2009, pp. 107-111.

habituels d'identification des personnes[37]. L'adresse IP est, à l'évidence, un outil privilégié pour ce faire. Cependant, elle est caractérisée par une instabilité relativement surmontable par la conservation des données. L'adresse IP peut être complétée par le recours aux fichiers témoins. Mais dans la pratique, ces données sont caractérisées par une véritable imprévisibilité. Il en résulte une précarité fonctionnelle des mesures techniques d'identification des cybercriminels se caractérisant par une adresse IP ondoyante (1) et des fichiers témoins imprévisibles dans données de connexion qui en résultent (2).

1- L'ondoyance de la fonction identificatrice de l'adresse IP

L'internaute peut être tenté de commettre des infractions sur l'internet, très faciles à réaliser, à l'instar du téléchargement illicite d'œuvres protégées par le droit d'auteur. Fort de l'immatérialité du réseau, il peut avoir le sentiment d'impunité, notamment en dissimulant son identité véritable par l'usage de pseudonymes. Mais cette sensation « de ne pas être vu et reconnu » est trompeuse[38], puisqu'il existe des moyens techniques de retrouver et d'identifier la personne par son adresse IP. L'adresse IP correspond au numéro de connexion donné par le fournisseur d'accès à l'internet au moment de la conclusion d'un contrat d'accès au réseau. Techniquement, il est le point d'entrée de l'ordinateur sur le réseau internet. À partir du numéro, le fournisseur d'accès l'ayant attribué a l'obligation de retrouver l'identité physique de son client, c'est-à-dire son nom et son prénom. L'adresse IP servant à identifier un internaute délinquant peut elle-même être difficilement identifiable puisque ce dernier peut la falsifier. De plus, elle est variable.

Une adresse IP peut être attribuée de manière permanente à une machine, si celle-ci est reliée à un réseau local lui-même connecté de manière permanente à Internet. Ce premier cas peut être comparé à celui de l'abonné au téléphone qui conserve le même numéro durant toute la durée de son abonnement. Dans ce cas, l'adresse IP permet d'identifier tant personne physique à travers ses identifiants classiques qui seront générés par le fournisseur d'accès Internet. Par ailleurs, la mise en œuvre de la responsabilité de l'auteur d'une infraction, identifié à l'aide de l'adresse IP, n'est pas l'apanage des personnes physiques. À partir du moment où une personne morale peut conclure un contrat d'accès à l'internet et être identifiée par une adresse IP, elle pourra aussi engager sa responsabilité en cas de commission d'infraction via la connexion[39]. C'est ainsi que les employeurs, titulaires d'une connexion internet, peuvent être rendus responsables, en tant que commettants des actes commis par leurs préposés[40] dans le cadre du travail et avec les moyens informatiques de l'entreprise[41].

L'adresse IP dynamique est une adresse affectée à tout appareil connecté à l'internet, et qui est différente à chaque connexion[42]. En effet, Le fournisseur d'accès attribue pour la durée de la connexion à internet un numéro IP unique choisi au hasard au sein de la classe d'adresses qu'il a obtenu directement de l'ICANN. Lors des sessions ultérieures, le même internaute se verra attribuer par le même fournisseur d'accès un numéro IP différent du précédent[43]. Cette situation peut être comparée à celle d'une personne ne disposant pas d'un abonnement téléphonique et n'utilisant que des cabines téléphoniques et rarement les mêmes. Il est dans ce cas très complexe de vérifier qui exactement a fait quoi à partir de ladite adresse[44].

Cependant, dans tous les cas, le fournisseur d'accès va inscrire pour les besoins d'identification en cas d'actes illicites sur le net, dans un journal de bord l'heure et les coordonnées du client à qui il a donné une adresse IP particulière. A l'heure actuelle, les adresses IP ne sont pas encore définitivement attribuées à chaque ordinateur. Toutefois, dans un futur proche, les adresses IP seront fixes et seront en conséquence aussi stables que l'adresse d'un appartement ou d'une maison[45]. Mais en attendant cette époque, force est de relever que les adresses IP telles que connues aujourd'hui sont davantage à l'image des identifiants traditionnels. Ils permettent d'identifier les internautes. Toutefois, comme le vol d'identité rattaché aux identifiants classiques, l'adresse IP peut faire l'objet d'une usurpation. Cette usurpation est de nature à renchérir l'affirmation de l'ondoyance de l'adresse IP.

L'adresse IP servant à identifier un internaute délinquant peut elle-même être difficilement identifiable puisque ce dernier peut la falsifier. En cette matière, on peut évoquer l'adresse IP dynamique et l'IP *spoofing*. L'IP *spoofing* est une technique qui permet d'usurper une adresse IP afin de

[37] Christiane FERAL-SCHUHL, *Cyberdroit : le droit à l'épreuve de l'internet*, 6ème éd., Dalloz, Coll. Praxis Dalloz, Paris 2019, p. 268.

[38] Pour une illustration : Richard MELTZ, "Une vie transparente sur internet", in *Internet et réseaux sociaux*, dir. Dominique CARDON, Problèmes politiques et sociaux, la Documentation française, n° 984, mai 2011, pp. 103 et s.

[39] Chamseddine BARNAT, « l'identification de l'internaute délinquant », *Infojuridique*, n° 46-47, Mai 2008.

[40] C. civ., art. 1384 al. 5.

[41] Céline CASTETS-RENARD, « Personnalité juridique et identification numérique », In : *La personnalité juridique*, *Op. cit*, p. 306.

[42] Rosalie DIARRA, *La répression de la cybercriminalité en Afrique de l'ouest*, L'Harmattan, 2021, p. 78.

[43] Céline CASTETS-RENARD, « Personnalité juridique et identification numérique », In : *La personnalité juridique*, *Op. cit*, p. 308.

[44] *Ibid*. p. 311.

[45] Jacques VETOIS, *technologies et usages de l'anonymat sur internet*, éd. l'Harmattan, 2012, p. 44.

se faire passer pour une autre personne. Il est ainsi possible à un technicien averti de falsifier son adresse IP et ainsi d'induire en erreur sur l'identité véritable de la connexion. Cette technique permet à un pirate d'envoyer à une machine des paquets semblant provenir d'une adresse IP autre que celle de la machine du pirate. Par ailleurs, l'internaute peut utiliser des logiciels spécifiques permettant de cacher ou falsifier son adresse IP, le rendant de ce fait difficilement identifiable. Il s'agit là d'une forme d'usurpation d'adresse IP[46]. Bien que le législateur ne l'ait pas encore clairement consacré, car l'usurpation d'identité reste définie au sens classique du terme, en faisant référence aux identifiants traditionnels, le législateur français s'est déjà montré plus dynamique.

Ainsi, La loi n° 2011-267 dite LOPPSI 2 du 14 mars 2011 a consacré une infraction pénale d'usurpation d'identité[47]. Codifiée à l'article 226-41 du Code pénal, cet article prévoit que : « *Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende* ». L'alinéa 2 ajoute que « cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne », de même que la tentative[48]. La rédaction redondante de l'alinéa 2 peut surprendre mais se justifie par le fait que l'infraction avait initialement été conçue pour ne s'appliquer qu'à l'internet, avant d'être étendue au monde physique. Il est vrai qu'une telle usurpation d'identité n'est pas l'apanage de l'internet et en décider autrement aurait sans doute constitué une rupture d'égalité devant la loi pénale. On aurait donc pu faire l'économie de ce deuxième alinéa. Placée désormais au chapitre des « atteintes à la vie privée », cette infraction prend mieux sa place qu'au chapitre des « violences », tel que le prévoyait initialement le projet de loi comme le pense madame Céline CASTETS-RENARD [49].

D'un autre côté, l'usurpation d'adresse IP n'est pas toujours criminelle. En effet, suite au développement extraordinaire qu'a connu l'Internet, une pénurie des adresses IP a caractérisée le monde du net. Il a fallu trouver une parade pour faire face à cette situation qui risquerait de contrecarrer ce développement. La solution technique a consisté à faire correspondre plusieurs ordinateurs à une seule adresse IP. Autrement dit, plusieurs ordinateurs peuvent surfer en même temps via une connexion Internet unique, sans pour autant pouvoir être identifié individuellement. Concrètement, le principe revient à masquer les adresses IP des stations locales[50] sous une adresse globale, le routeur se chargera de faire coïncider les deux. Les ordinateurs qui se connectent auront la même adresse IP vu de l'extérieur, les machines ne sont pas visibles ou directement identifiables. Ainsi les stations locales, qui devraient normalement devoir disposer chacune d'une adresse unique sur internet, se verront attribuer une IP privée non routable, seul le routeur disposera d'une IP routable reconnue sur le réseau. Celui-ci masquera les IP privées pour les remplacer par la sienne. Par conséquent, vu de l'extérieur tout se passe comme si seul le routeur était connecté, le réseau local restant invisible. Bien que le point de départ ne soit pas empreint d'intention criminelle, force est de relever que cet état de la technique est de nature à favoriser la dissimulation des internautes délinquants.

On comprend de ce qui précède que le routeur permet de masquer l'ensemble des ordinateurs situés à son amont, ce qui complexifie encore plus le processus d'identification. On peut donc conclure que compte tenu de l'essor d'internet, il existe potentiellement aujourd'hui une multiplicité d'ordinateurs derrière une même adresse IP, et une multiplicité d'individus derrière un même ordinateur[51]. Les caractéristiques de l'adresse IP font qu'il est pratiquement impossible d'identifier l'internaute en tant que visiteur unique en se référant uniquement à cet identifiant certes unique mais facilement falsifiable. Si l'adresse IP peut être utilisée par les autorités de police judiciaire pour poursuivre les infractions, l'identification réelle de leurs auteurs implique l'intervention des opérateurs techniques, censés conserver les données de leurs clients[52]. Ces données peuvent malgré la complexité du mécanisme être complétées par celles recueillies par les fichiers témoins. Toutefois, ce mécanisme est peut prévisible.

2- L'insuffisance de la fonction identificatrice des fichiers témoins

Il existe une autre technique importante d'identification et de pistage des données[53] des internautes qui passe par l'utilisation des *cookies*[54].

[46] *Ibid.* p. 46.
[47] V. Article 2.
[48] C. pén., art. 226-5.
[49] Antoine LEPAGE, « Le délit d'usurpation d'identité : questions d'interprétation », *JCP* 2011, I, 913. Cet auteur évoque même une "conception renouvelée de l'identité" de concert avec madame Céline CASTETS-RENARD.

[50] Les ordinateurs d'une faculté, d'une entreprise, cybercafé…
[51] Il s'agit de cybercafés, cercle familial…
[52] Céline CASTETS-RENARD, *Droit de l'internet : droit français et européen*, *Op. Cit*, p. 224.
[53] Fabrice ROCHELANDET, *Économie des données personnelles et de vie privée*, La Découverte, collec. Repères, n° 546, 2011, pp. 77 et s. L'analyse économique révèle toutefois que le paradoxe de ce comportement qui paraît peu raisonnable, peut en réalité se justifier par une analyse des coûts.
[54] La loi camerounaise sur la cybercriminalité et cybersécurité assimile les *cookies* aux logiciels trompeurs: logiciel effectuant des opérations sur un équipement terminal d'un utilisateur sans informer préalablement cet utilisateur de la nature exacte des opérations que ce logiciel va effectuer sur son équipement terminal ou sans demander

Les données de connexion comme l'adresse IP constituent un moyen d'identification de l'internaute délinquant. Afin de faciliter les enquêtes judicaires par une meilleure « traçabilité[55] » des utilisateurs des réseaux, le législateur a imposé aux intermédiaires techniques la conservation des données numériques d'identification. Cependant, l'imprévisibilité des données de connexion est due au fait que les données permettent d'identifier l'ordinateur utilisé et non l'utilisateur. Il en résulte une indentification incomplète du cybercriminel en l'espèce.

En effet, les *cookies* sont des petits fichiers textes, sorte de code barre informatique que le serveur d'un site web glisse, le plus souvent sans que l'utilisateur ne le sache, au sein du disque dur de l'internaute visitant le site[56]. On comprend donc que les fichiers témoins, à la différence des fichiers journaux conservés sur le serveur du site web, sont stockés sur le disque dur de la machine cliente lors de la première visite sur un site donné[57]. Il faut préciser que le fichier témoin porte un nom unique ce qui permettra au serveur qui en est à l'origine de le reconnaitre, et ce, quelle que soit l'adresse IP attribuée à la connexion. Le fichier témoin agit comme un identifiant[58]. L'objectif étant une identification future de l'internaute lors de ses prochaines visites au site en question. Le recours à la technique des *cookies* vise bien plusieurs finalités : l'objectif premier de ce fichier informatique est de faciliter la navigation de l'internaute sur le serveur web. Les *cookies* peuvent en effet faciliter l'accès de l'internaute au site dont il émane et ainsi lui faire gagner du temps[59]. Les *cookies* peuvent également profiler l'internaute et reconstituer son parcours lors de sa navigation. Les informations sur la navigation de l'internaute ne peuvent être lues que par le serveur qui les a créées. Les données récupérées par les *cookies* peuvent surtout être utilisées dans le cadre d'enquêtes policières ou plus généralement de procédures judiciaires où elles servent à des besoins d'identification.

Toutefois, dans la pratique, le recours aux *cookies* au Cameroun n'est pas libre. Il est soumis au consentement des internautes. Les cyberlégislations camerounaises donnent une visibilité de l'encadrement des techniques d'adhésion. Une lecture conjointe des articles 6 et 7 de la loi sur le commerce électronique permet de relever que le législateur camerounais a opté pour un système consacrant deux techniques. Il s'agit du *opt-in* et *opt-out*. Ainsi, le recours aux *cookies* est licite sous condition du consentement de l'internaute[60]. On est là en présence d'une manifestation du désir à protéger la vie privée des personnes qui se meuvent en ligne. La protection de la vie privée en ligne procède donc de la collecte loyale des données personnelles des internautes. Tout prestataire de collecte des données à caractère personnel est astreint à solliciter le consentement de l'internaute avant toute collecte.

En considération du rôle important des données connectées, obligation est faite aux FAI de conserver les données de connexion des internautes potentiels délinquants. Les articles 28 et 29[61], 35, 46 de la loi camerounaise relative à la cybersécurité et à la cybercriminalité imposent à ces opérateurs de conserver les données d'identification de leurs clients et de les communiquer à la demande du juge. Ces opérateurs sont les seuls à pouvoir associer le nom d'une personne à une adresse IP, aussi leur coopération est-elle essentielle[62], c'est la raison pour laquelle le législateur camerounais lui a accordé tout un titre dans la loi relative à la cybersécurité et cybercriminalité. Les juges leur ordonnent de communiquer l'identité physique des personnes soupçonnées d'avoir commis une infraction et dont l'adresse IP a été collectée par les enquêteurs des services spécialisés. On comprend de ce qui précède que l'obligation de conservation qui pèse sur les principaux acteurs de l'internet a comme objet les seules données portant sur l'identification des personnes utilisatrices des services fournis par ces opérateurs et les caractéristiques techniques des communications assurées par ces derniers[63]. Par conséquent, les données recueillies ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit. Bref, les données de connexion peuvent être utilisées dans le cadre d'enquêtes policières ou plus généralement de procédures judiciaires ou elles servent à des besoins d'identification.

à l'utilisateur s'il consent à ce que le logiciel procède à ces opérations. Article 4. 53.

[55] En dehors du recours aux *cookies*, les données sur le client peuvent être colligées explicitement ou implicitement, au moyen de nombreuses technologies utilisées par les sites Web des vendeurs telles celle sus-étudiée et d'autres telles des Web *bugs*, des *spywares*, des *log files*. V. Job NZOH SANGONG, *La publicité en ligne, Contribution à la définition de la nature juridique de la publicité sur Internet*, Th. Université de Ngaoundéré, 2019, pp. 46-48.

[56] Keneth LAUDON, *Management des systèmes d'information*, éd. PEF, 2010, p. 131.

[57] Cynthia CHASSIGNEUX, « Vie privée et commerce électronique », éd. Eyrolles, 2004, p. 30.

[58] *Ibid*, p. 31.

[59] Willy DUHEN, « FAI face à l'anonymat sur internet : vers de nouvelles responsabilités », *Revue terminal*, 2010, p. 33.

[60] V. L'article 66 alinéa 1 de la loi camerounaise relative à la cybersécurité et à la cybercriminalité.

[61] Cet article dispose que les exploitants des systèmes d'information ont l'obligation de conserver les données de connexion et de trafic de leurs systèmes d'information pendant une période de dix (10) ans.

[62] V. les articles 90-94 de la loi camerounaise relative à la cybersécurité et à la cybercriminalité.

[63] Willy DUHEN, « FAI face à l'anonymat sur internet : vers de nouvelles responsabilités », *Op. Cit.*, p. 44.

En effet, les fichiers témoins permettent d'enregistrer des informations relatives à la navigation d'un internaute : pages consultées, la date et l'heure de consultation. Il faut enfin préciser que les *cookies* permettent d'identifier non pas l'internaute, mais l'ordinateur utilisé par ce dernier. Ces donnée[64]s sont également générées par le fournisseur d'accès à internet. Les données de visite sont générées sur les serveurs des sites internet visités, traçant les adresses IP des tiers qui ont visités ces sites à un moment donné. Il faut alors conserver pendant une durée de dix années[65], les données électroniques d'identification suivantes : « *les informations permettant d'identifier l'utilisateur ; les données relatives aux équipements terminaux de communication utilisés ; les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ; les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ; les données permettant d'identifier le ou les destinataires de la communication* ». On comprend que la conservation de ces données a pour objectif de permettre l'identification des délinquants et de matérialiser des éléments de preuve des infractions.

Toutefois, l'insuffisance de cette obligation de conservation dans le processus d'identification des cybercriminels réside dans le fait que la conservation renvoie à la machine connectée et non au cybercriminel dans son individualité[66]. Par ailleurs, compte tenu de l'ubiquité des internautes, les opérateurs techniques doivent fortement coopérer avec les autorités publiques, sous peine d'engager leur responsabilité[67]. Le rôle de ces techniciens est primordial, car le droit est dépendant de la technique, ce qui est source de risques, car on sait très bien que tout dispositif technique comporte des failles et des possibilités de contournement. Il convient donc de nuancer l'efficacité du procédé d'identification et d'admettre que des outils techniques puissent déjouer l'identification par l'adresse IP, rendant par la suite toute poursuite impossible[68].

De tout ce qui précède, on peut le relever pour le décrier, l'identification du cybercriminel est une véritable aporie processuelle pour les cyber-victimes. Cette angoisse processuelle est prolongée par la rigidité du régime d'administration des preuves par ces cyber-victimes.

II- L'instabilité des documents cybercriminels

L'informatique est une épine au pied de l'instance judiciaire. Dans un litige relatif aux cyber-crimes, les données convoquées ne sont pas toujours d'une accessibilité intelligible. Les données sont généralement générées par des procédés techniques dont la compréhension échappe au juge. En effet, en présence d'un cyber-crime, le juge se trouve face à une boîte noire, lorsqu'on lui présente une preuve qui est le résultat d'un processus technologie invisible on non intelligible. Il en résulte un aveuglement du juge face aux cyber-preuves du fait de leur malléabilité. Cet aveuglement est précédé de par une imprécision de la portée de la preuve électronique porteuse d'insécurité juridique. Il en résulte une passibilité de la valeur probatoire des documents électroniques.

A- La malléabilité des cyber-preuves

La performance essentiellement croissante des TIC est le gage du progrès de la société de l'information. Toutefois, ce progrès n'est pas sans effet pervers pour la sécurité juridique des internautes. Au centre de cette insécurité juridique se trouve la manipulation des dates et des contenus débouchant sur une intemporalité des preuves électroniques d'une part, et d'autre part, la falsifiabilité des contenus de toute nature.

1- La falsifiabilité des contenus numériques

La criminalistique numérique se rapporte à la récupération des informations – qui sont souvent volatiles et facilement contaminées – pouvant avoir une valeur probante. Les techniques de criminalistique incluent la création de copies « bit à bit » des informations stockées et effacées, le « blocage d´écriture », afin de garantir que les informations originales ne sont pas altérées, et des « hachages » cryptographiques de fichiers, ou des signatures digitales, qui peuvent révéler des changements dans les informations[69]. Les réponses ainsi susceptibles

[64] Les données de connexion peuvent être divisées en trois catégories : les données de connexion simple, les données de navigation et les données de visite. Les données de connexion simple sont générées chez le fournisseur d'accès à internet : chaque fois qu'un abonné rentre sur le réseau, celui-ci doit donner le nom de compte et le mot de passe qui lui sont associés. Ces données rassemblent donc les éléments suivants : identité de l'abonné, heure et début de connexion, l'adresse IP qui a été attribuée à l'abonné durant cette connexion. Les données navigation sont des données relatives aux sites internet visités ou aux services accédés par le titulaire d'une adresse IP connecté à un moment donné.

[65] Article 29 suscité.

[66] David CHILSTEIN, « Les nouveaux défis du droit pénal : incriminations générales et spéciales à l'épreuve de l'économie numérique », in Les nouveaux défis du commerce électronique, dir. Justine ROCHFELD, LGDJ, Montchrestien, 2010.

[67] Sur cette question, voir : Céline CASTETS-RENARD et Georges AZZARIA, « Le renouvellement du droit de la responsabilité sur l'internet », Lexisnexis, Litec, coll. Actes et colloques, sept. 2011, p. 66.

[68] Céline CASTETS-RENARD, « Personnalité juridique et identification numérique », In : *La personnalité juridique*, *Op. cit*, p. 311, n° 25.

[69] C'est dans cette optique que l'article 58 de la loi camerounaise relative à la cybersécurité et à la cyber criminalité prescrit aux personnes physiques ou morales qui fournissent des prestations de cryptographie visant à assurer

d'être apportées traduisent l'idée d'un fort potentiel de malléabilité des cybercriminels. En effet, l´interaction d´un usager avec des dispositifs électroniques produit de nombreuses traces numériques[70] générées par un système informatique. Les données informatiques et les communications électroniques qui sont potentiellement importantes pour un acte criminel peuvent inclure des giga-octets de photographies, de vidéos, de courriels, de journaux, de conversations et de données du système[71]. Localiser les informations pertinentes dans ces données peut exiger beaucoup de temps. La variété de formats de fichiers possibles, de systèmes d´exploitation, de logiciels d´application et d´éléments de hardware peut aussi compliquer le processus d´identification des informations pertinentes[72].

Les artefacts informatiques peuvent être facilement modifiés, écrasés ou effacés et posent donc des problèmes car les sources d´informations numériques doivent être authentifiées et vérifiées[73]. Les règles de la preuve varient considérablement en fonction de la juridiction, et même entre les pays qui ont des traditions juridiques similaires. Cependant, les systèmes juridiques dans la tradition de Common Law tendent généralement à avoir des règles définies en matière de recevabilité de la preuve. Dans les systèmes juridiques dans la tradition de droit civil, dans lesquels des juges professionnels maintiennent un niveau élevé de contrôle sur les procédures du tribunal, la recevabilité de la preuve peut être flexible, même si la pondération des éléments de preuve[74].

De manière pratique, cette malléabilité se traduit par l'introduction dans un système informatique, en modifiant ou effaçant des données, qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, et par là, modifier la portée juridique de telles données[75]. Il en résulte la réunion de trois éléments constitutifs. En effet, d'après eux il faut : une altération de la vérité[76] ; l'introduction, la modification, par tout moyen technologique, de l'utilisation possible des données dans un système informatique[77] ; une modification de la portée juridique des données[78].

De plus, les intérêts juridiques protégés dans des délits contre l´intégrité, la disponibilité et la confidentialité des systèmes et des données informatiques, sont les informations et les données informatiques elles-mêmes. C'est la raison pour laquelle on peut déplorer leur violation dans d'autres actes tels la manipulation des données informatiques ou l´interférence avec un système informatique, qui procurent des bénéfices économiques au délinquant ou à d´autres personnes, l´altération, la suppression, la transmission et toute autre manipulation des données informatiques, pour obtenir de fausses données destinées à être traitées ou utilisées comme si elles étaient authentiques.

En principe, la survenance de tels faits est la résultante d'une inobservation du contenu de l'article 25 de la loi camerounaise relative à la cybersécurité et à la cybercriminalité. En substance, on peut y lire que les opérateurs des réseaux de communications électroniques et les fournisseurs de services de communications électroniques doivent prendre toutes les mesures techniques et administratives nécessaires pour garantir la sécurité des services offerts. A cet effet, ils sont tenus d'informer les usagers : du danger encouru en cas d'utilisation de leurs réseaux ; des risques particuliers de violation de la sécurité notamment, les dénis de service distribués ; le re-routage anormal, les pointes de trafic, le trafic et les ports inhabituels, les écoutes passives et

une fonction de confidentialité, sont tenues de remettre aux Officiers de Police Judiciaire ou aux agents habilités de l'Agence, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Toutefois, il ne sera pas toujours aisé de retrouver le cocontractant de la convention de cryptage ou de chiffrement de contenu.

[70] Elles sont techniquement parfois appelées empreintes numériques ou artefacts.

[71] Vincent GAUTRAIS et Patrick GINGRAS, « La preuve des documents technologiques », *Les Cahiers de propriété intellectuelle*, Vol. 22, nº 2, 2010, p. 311.

[72] Estelle LODOMEZ, *Le faux informatique : le (faux) frère jumeaux du faux en écritures ?*, DSPC, 2018, p. 16.

[73] *Ibid.*

[74] Vincent GAUTRAIS et Patrick GINGRAS, « La preuve des documents technologiques », *Les Cahiers de propriété intellectuelle*, Vol. 22, nº 2, 2010, p. 288.

[75] Olivier LEROUX, « Chapitre IX. – Criminalité informatique », in *Les infractions*, vol. 1 : Les infractions contre les biens, 2ème éd., Bruxelles, Larcier, 2016, p. 449.

[76] Il en résulte une possible diffamation à laquelle le législateur camerounais apporte un remède dans le contenu de l'article 39 de la loi camerounaise relative à la la cybersécurité et à la cybercriminalité qui dispose que toute personne victime d'une diffamation au moyen d'un service de communications électroniques, dispose d'un droit de réponse et peut en exiger la rectification.

[77] Au sens de l'article 72 de la loi camerounaise relative à la la cybersécurité et à la cybercriminalité.

[78] Cette possible falsifiabilité justifie le contenu des articles 33 et 34 de la loi camerounaise relative à la la cybersécurité et à la cybercriminalité qui disposent en substances que Les personnes dont l'activité est d'offrir un accès aux services de communications électroniques, informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposer au moins un de ces moyens. C'est la raison pour laquelle la responsabilité des personnes qui assurent, même à titre gratuit, le stockage des signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par les destinataires de ces services,
peut être engagée.

actives, les intrusions et tout autre risque ; de l'inexistence de moyens techniques permettant d'assurer la sécurité de leurs communications. Cette disposition révèle les attentes du législateur camerounais envers les opérateurs de réseaux de communication. Il parait logique que cette attente peut être étendue aux hypothèses dans lesquelles la date des contenus numériques est en cause.

2- L'intemporalité des contenus numériques

Dans l'environnement numérique, en particulier sur les réseaux, le « temps virtuel[79] » paraît dénaturé[80] : tantôt accéléré, au regard de la vitesse de transmission des informations ; tantôt « dilaté »[81] en un éternel présent où les communications s'effectuent simultanément – ou « en temps réel » – ; parfois même aboli, puisque les données peuvent s'évanouir sans laisser de trace dans l'histoire numérique. Ainsi, dans cet univers où règnent l'instantané, le simultané et l'éphémère, il importe d'établir avec certitude *l'existence*, *à un moment précis*, d'une opération portant sur un ensemble défini de contenus numériques[82] et, partant, *la chronologie* de plusieurs opérations. D'un point de vue juridique, ces questions s'avèrent cruciales à plus d'un titre, que ce soit pour déterminer le moment de conclusion d'un contrat ou de l'envoi d'un document, vérifier le respect d'un délai[83], ou encore établir l'antériorité d'un acte par rapport à un autre ou encore la portée probatoire d'un contenu numérique au sens temporel du terme[84].

Or, s'il est vrai que tout système d'exploitation attribue une date aux fichiers qu'il gère et aux opérations qu'il traite, on ne saurait se fier à un tel procédé de datation[85] : les risques de falsification de la date sont bien réels, sans compter les possibles dysfonctionnements. En effet et à titre palliatif, on pourrait se contenter d'inscrire la date désirée *dans le contenu* de l'acte électronique lui-même et de garantir son intégrité en utilisant, par exemple, une signature électronique. Certes, cette méthode présente l'avantage de la simplicité. Cette simplicité est préjudiciable aux victimes de cybercrimes. Les différents contenus numériques notamment écrits, photos, vidéo et audio sont manipulables quant à leur date de conception et de réalisation surtout. C'est à ce niveau que se situe tout le risque d'intemporalité de cette méthode de datation. Elle ne bénéficie toutefois pas des atouts majeurs de l'horodatage électronique, à savoir l'automatisation totale du processus, sa haute précision, la possibilité de dater tout type de donnée informatique, ainsi que la fiabilité apportée par le recours à un tiers de confiance.

Face à un litige, la détermination de la date d'un acte peut s'avérer cruciale à bien des égards comme déjà susmentionné. Dans l'environnement numérique, on trouve de nouveaux motifs de s'inquiéter de la localisation d'un événement dans le temps. Ainsi, l'on sait que, depuis l'AUDCG[86], la signature électronique est assimilée à la signature manuscrite, lorsqu'il s'agit d'une signature électronique avancée, réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique[87]. Il va de soi que pareille signature ne sera valable que si elle est utilisée endéans la période de validité du certificat qualifié qui l'accompagne. En effet, ce dernier a une durée de vie limitée pour des raisons techniques, étant donné l'évolution rapide des standards de sécurité. La loi exige d'ailleurs que le certificat qualifié comporte l'indication du début et de la fin de sa période de validité, et que le prestataire de service de certification veille à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision[88]. Toutes ces précautions s'avèrent d'une piètre utilité s'il est impossible de déterminer aussi précisément à quel moment une signature électronique est utilisée, afin de s'assurer de sa validité.

En outre, la datation d'un contenu numérique pourrait également jouer un rôle de première importance dans le domaine des droits de propriété intellectuelle. Ainsi, un auteur pourrait y recourir afin de se ménager facilement une preuve de la date de création de son œuvre numérique, au lieu d'effectuer le dépôt de celle-ci auprès d'une société de gestion des droits d'auteur.

[79] L'expression est de F. OST, « Le temps virtuel des lois contemporaines ou comment le droit est traité dans la société de l'information », *J.T.*, 1997, pp. 53 et s.

[80] A ce sujet, voy. *Ibidem*, spéc. pp. 56 et 57 ; *Idem*, "Le commerce en ligne : courtscircuits et excès de vitesse", in B. DE NAYER et J. LAFFINEUR (Eds), *Le consentement électronique*, Coll. Droit et consommation, Bruxelles, Bruylant, 2000, pp. 185 et s.

[81] P. VIRILIO, *La vitesse de libération*, Paris, Galilée, 1995, cité par F. OST, "Le commerce en ligne : courts-circuits et excès de vitesse", *op. cit.*, pp. 187 et 188.

[82] Il s'agit de la création, la transmission, la modification, la suppression, etc.

[83] Marie DEMOULIN, « Aspects juridiques de l'horodatage des documents électroniques », *CAHIERS DU CRID – n° 23*, 2005, p. 43.

[84] C'est encore en vue d'éviter une modification ultérieure de la date – chose relativement facile lorsque celle-ci est exprimée en chiffres –, que la loi exige parfois qu'elle soit inscrite en toutes lettres. Le souci d'exactitude de la date se cache également derrière l'exigence expresse de l'indication des jour, mois et année, permettant de situer précisément dans le temps le moment où l'acte est passé.

[85] T. LIEUTENANT et S. MARIN, « Archivage et horodatage de documents électroniques », document CRID, mai 2001, p. 15.

[86] Voir les articles 83 à 100 de l'AUDCG. Ces dispositions renchéries par le chapitre IX de la loi relative à la cybersécurité et à la cybercriminalité.

[87] Article 18 de la loi relative à la cybersécurité et à la cybercriminalité.

[88] Article 22 de la loi relative à la cybersécurité et à la cybercriminalité.

Aussi s'avère-t-il nécessaire de recourir à un service d'horodatage électronique répondant à certaines normes techniques et confier à un tiers de confiance, chargé d'estampiller les données qu'on lui soumet afin d'attester leur contenu et leur existence à un moment précis. L'horodatage électronique est un procédé attribuant avec certitude une marque de temps précise à un document électronique, grâce à l'intervention d'un tiers de confiance appelé tiers horodateur[89] Techniquement, le système procède de la même manière que la signature numérique fondée sur la cryptographie asymétrique[90]. La personne qui souhaite horodater un document électronique doit d'abord lui appliquer un algorithme de hachage, c'est-à-dire une fonction de compression irréversible permettant de calculer l'empreinte du document. Cette empreinte est ensuite transmise au tiers horodateur, qui lui attribue une marque de temps, puis la signe au moyen d'une clé générée exclusivement à cet effet. On qualifie parfois cette opération de « signature de date »[91]. Au terme de ce processus, le document électronique est ainsi doté d'un certificat d'un type particulier, contenant l'empreinte horodatée et signée. Par la suite, sur la base de ce certificat, il sera possible de s'assurer que le contenu a bel et bien été horodaté au moment indiqué, en vérifiant la signature du tiers horodateur. De surcroît, le certificat permet de garantir que le document n'a subi aucune modification entre-temps. A cet effet, il suffira de lui appliquer la fonction de hachage afin d'obtenir une nouvelle empreinte, et de comparer cette dernière à celle qui figure dans le certificat, pour contrôler leur parfaite similitude.

Un tel mécanisme serait une véritable panacée à l'intemporalité des contenus numériques. Toutefois, il importe de questionner la fonction et la valeur probatoire non seulement des contenus numériques, mais surtout de tous ceux soumis à horodatage.

B- La passibilité de la valeur probatoire des contenus numériques

De nombreux pays ont introduit l'admissibilité de la preuve électronique dans leurs procédures juridiques. Le Cameroun n'est pas en reste. Une lecture collationnée de la loi camerounaise relative à la cybersécurité et à la cybercriminalité, de la loi relative au commerce électronique et l'AUDCG dans son livre V permet de renchérir cette affirmation. La collation de ces textes permet ainsi de relever une consécration rigide de la fonction probatoire des contenus numériques (1) débouchant sur une judiciarisation mitigée des preuves électroniques (2).

1- La rigidité de la fonction probatoire des contenus numérique

Qu'il soit technologique ou non, tout acte sous seing privé déposé en preuve se doit de respecter les règles de droit applicables. De ce fait, la partie qui entend invoquer un tel acte doit en faire la preuve puisqu'elle incombe en effet à celui qui prétend en application de la règle *actor incumbit probatio*. La rigidité de la fonction probatoire des contenus numériques est perceptible à au moins deux égards : les caractères exigés des documents numériques et le domaine d'admission desdits documents à titre preuve en l'état actuel du droit camerounais.

Dans plusieurs systèmes juridiques[92] déjà mentionnés *supra*, la qualité des procédures appliquées pour maintenir l´intégrité des informations numériques depuis le moment de leur création jusqu'à leur introduction devant le tribunal, doit être démontrée par le proposant de la preuve. L´intégrité et l´authenticité des informations numériques ont une influence directe sur le poids de la preuve, pour ce qui concerne sa crédibilité et sa véracité. La partie qui cherche à présenter une preuve doit généralement démontrer la pérennité de la preuve ou la chaine de garde, afin de démontrer que les preuves n´ont pas été falsifiées ni altérées. La pérennité de la preuve est généralement une question de fait et le processus de la chaine de garde est le mécanisme applique pour maintenir et documenter l´historique chronologique de la preuve qui a été déplacée d´un lieu à l´autre[93].

Ces exigences d'intégrité, d'authenticité et de pérennité sont les caractères reconnus à la signature électronique appliquée. Or, dans nombre de cyber-

[89] En anglais, *Time Stamping Authority – TSA*.

[90] Concernant les aspects techniques de l'horodatage, v. Tomas. LIEUTENANT et Simon. MARIN, "Archivage et horodatage de documents électroniques", *op. cit.*, pp. 15-18 ; Thierry. PIETTE-COUDOL, *Echanges électroniques, certification et sécurité*, Paris, Litec, 2000, pp. 145-147, nos 259-262. Voy. également le protocole d'horodatage (*Time Stamping Protocol*) établi par l'I.E.T.F (*Internet Engineering Task Force*) dans le RFC n° 3161 (*Request for Comments*), finalisé en août 2001 et disponible sur le site de l'I.E.T.F (http://www.ietf.org). Ce protocole étend le célèbre protocole Internet X.509 qui définit les normes internationales pour les infrastructures à clé publique (*Public Key Infrastructure*).

[91] Pour plus de détails sur les aspects techniques de la signature numérique fondée sur la cryptographie asymétrique, voy. notamment Armand. JAMAR, "La sécurité des transactions – Introduction technique", in *Le commerce électronique : un nouveau mode de contracter ?*, Liège, Ed. du Jeune Barreau, 2001, pp. 21 et s. ; J. HUBIN, *La sécurité informatique, entre technique et droit*, Cahiers du CRID, n° 14, Ed. Story- Scientia, 1998, pp. 68-112 ; S. PARISIEN et Pierre TRUDEL, *L'identification et la certification dans le commerce électronique*, Québec, Ed. Yvon Blais Inc., 1996, pp. 93-113.

[92] Voir Dominic JACKSON et Sarah SUMMERS, *L´internationalisation de la preuve criminelle : au-delà de la Common Law et de la tradition de droit civil*. Cambridge : Cambridge University Press. 2012.

[93] Emilie CASEY, *Preuves électroniques et délits informatiques : la criminalistique, les ordinateurs et l´internet*. New York : Elsevier, 2011, p. 54.

infractions, les contenus en cause sont généralement exempts de tout recours à ladite signature. Il apparait donc difficilement concevable pour les cybervictimes de produire des preuves dont l'intégrité, l'authenticité et la pérennité seraient incontestables. Dans le cas des informations numériques, la pérennité de la preuve doit être maintenue et concerne le *dispositif physique* qui héberge les données et les *données stockées* contenues dans le dispositif. Ainsi, la partie qui présente la preuve doit démontrer au sens de l'article 26 de la loi camerounaise relative à la cybersécurité et à la cybercriminalité que : les informations numériques obtenues à partir du dispositif sont une représentation véridique et précise des données originales contenues dans le dispositif ; et que le dispositif et les données que la partie souhaite présenter comme preuve sont les mêmes que ceux qui ont été initialement découverts et qu´ils ont été postérieurement places sous surveillance. La finalité est de démontrer que le dispositif est ce qu´il est prétendu être et que les informations numériques sont véridiques et n´ont pas été falsifiées ni altérées[94].

La recevabilité désinformations générées par ordinateur qui détaillent les activités sur un ordinateur, un réseau ou tout autre dispositif, peut être contestée si le système qui génère les informations n´a pas de solides contrôles de sécurité[95]. Outre le fait de devoir démontrer l´authenticité et l´intégrité de la preuve, des difficultés relatives à l´utilisation de preuves électroniques peuvent surgir, dans certaines juridictions, avec l´application de *règles de preuves* particulières. Il peut, par exemple, être nécessaire de démontrer que les preuves électroniques tombent sous le coup d´une interdiction générale de preuve par ouïe dire avec des exceptions particulières[96], ou que, par exemple, l´impression de données informatiques satisfait les exigences de la règle de la meilleure preuve[97]. Cet ensemble de constat pourrait conduire à une présomption de non fiabilité des documents électroniques utilisés à titre de preuves.

2- L'inintelligibilité éprouvante de certains documents numériques

Dans le désir de s'affranchir de toute éventuelle action en responsabilité, certains cybercriminels recourent à des techniques rendant inintelligibles les éléments de preuves susceptibles de les compromettre. Il s'agit respectivement du cryptage et de la sténographie. Ces techniques permettent de complexifier la fonction probatoire des documents électroniques. En effet, que vaut un texte inintelligible entre les mains des services d'investigation ou des juges ? C'est à cette difficulté que sont confrontés les acteurs soumis aux documents pour lesquels les auteurs ont eu recours au cryptage ou à la sténographie.

Le cryptage peut se définir au sens de l'article 4-28 de la loi camerounaise relative à la cybersécurité et à la cybercriminalité comme l'utilisation de codes ou signaux non usuels permettant la conservation des informations à transmettre en des signaux incompréhensibles par les tiers. Cette technique de confidentialité des documents a été accueillie par les cybercriminels. Dans la pratique, il n y a pas de manière simple de surmonter le défi de taille que représente l´encryptage car « cela requiert des capacités et une assistance technique expertes. Il peut en effet arriver de faire face au cryptage de données lors des enquêtes menées par les services répressifs et de l´analyse des preuves électroniques. En fonction du type de délit, le cryptage devient beaucoup plus commun.

Toutefois, cette technique n'est pas insurmontable. Si le suspect ne révèle pas la clé de décryptage, les enquêteurs peuvent utiliser divers logiciels, entreprendre une expertise technique, ou transmettre la preuve potentielle aux laboratoires criminalistiques ou au personnel spécialise pour tenter de la décoder. Une fois de plus, le recours à l'expertise extérieure aux juridictions peut être sollicité. En plus de ce décryptage, il existe des logiciels de décryptage. Leur usage n'est toujours aisé et peut à certains égards se montrer limité.

Outre les difficultés que représente la technologie de cryptage pour la criminalistique numérique, les délinquants peuvent aussi utiliser la « sténographie ». Elle consiste à dissimuler des informations ou des

[94] Junior MARCELLA et André Jean GREENFIELD, *Cyber criminalistique : un manuel de terrain pour collecter, examiner et préserver les preuves des délits informatiques*, 2nd edn. Boca Raton : CRC Press, 2002, p.136.

[95] David CHAIKIN, *Enquêtes de réseau des cyber attaques : les limites des preuves numériques*. *Criminalité, droit et changement social*, 2006, p. 249.

[96] La preuve par ouïe dire est souvent définie comme *« la preuve d´une déclaration faite à une autre occasion, dans le but d´établir la véracité de son contenu »* (*Halbury »s Laws*, Vol. 17). Certains types de preuves électroniques peuvent constituer strictement une preuve par ouïe dire, mais pourraient être admises sous des exceptions telles que des ≪ documents commerciaux ≫. Voir Thomson, L.L., 2011. La recevabilité des documents électroniques en tant qu´éléments de preuve dans les tribunaux des U.S. Appendice IX.B.1,
Centre de bibliothèques de recherche, étude des droits de l´homme sur les preuves électronique.

[97] Selon le principe général, la meilleure preuve doit être présentée devant les tribunaux courts. Si la règle de la meilleure preuve est appliquée, les copies de l´original peuvent ne pas être recevables comme éléments de preuve a moins qu´il ne soit possible de démontrer que l´original n´est pas disponible car il a été détruit ou en raison d´autres circonstances. L´impression des informations contenues dans un ordinateur ou un autre dispositif de stockage ne devrait pas techniquement être considérée originale. Cependant, dans certaines juridiction la règle de la meilleure preuve n´exclut pas les impressions lorsque l´impression reflète avec exactitude les données réelles.

communications dans des fichiers innocents, comme des images graphiques, des documents, des échantillons audio ou des applications. Les fichiers multimédias sont les hôtes idéaux pour la sténographie, car ils sont généralement volumineux et ne suscitent pas immédiatement des soupçons. Dans certains pays développés, les organisations criminelles tentent de rendre les enquêtes difficiles en stockant les données liées aux actes criminels dans des serveurs étrangers ou dans des systèmes de stockage en nuage, et utilisent la cryptographie et d´autres techniques d´offuscation de données. Du point de vue de la criminalistique, l´identification de données cachées peut s´effectuer en comparant des fichiers suspects ou des flux de données avec les originaux connus.

L´utilisation accrue de l´informatique en nuage représente un problème pour la criminalistique informatique. Les informations stockées à distance par les cybercriminels dans les services d´informatique en nuage peuvent devenir visibles pour les enquêteurs durant une recherche ou une analyse criminalistique comme lorsque des sessions d´internet en direct sont localisées sur des ordinateurs en fonctionnement, ou au moyen de services à distance disponibles sur les dispositifs mobiles saisis. Outre les considérations juridiques relatives à l´accès direct ainsi relevées, des services répressifs aux données extraterritoriales, le stockage des données en nuage complique le processus criminalistique d´identification, de collecte et d´analyse des informations stockées sous forme informatique[98]. La possibilité qu´un internaute utilisateur de nuage obtienne un accès aux données d´une autre personne constitue une illustration supplémentaires concernant l´authenticité des données, et partant de la passibilité des contenus numériques.

Cependant, face à ces problèmes, on peut mentionner une variété de techniques susceptibles d'être utilisées pour garantir que l´intégrité des preuves électroniques collectées au moyen de la criminalistique numérique soit maintenue[99]. Ainsi, on peut relever la possible utilisation de l´imagerie criminalistique ; l´utilisation de déclarations sous serment attestant l´authenticité des données[100] ; des valeurs de hachage; l´utilisation de bloqueurs en écriture ; la capture de données d´internet par capture d´écran ; l´étiquetage systématique, les méthodes de documentation, d´emballage et de transport et le scellement des images enregistrées sur un disque optique[101]. Il en résulte que l'hybridation de la criminalistique serait une importante solution à cette virtualisation du crime.

En sus, il ne faut surtout pas mettre de côté le fait que les documents électroniques, lorsqu'ils sont produits ne constituent qu'un commencement de preuve. A la réalité, une lecture *a contrario* de l'article 17 de la loi de 2010 la loi camerounaise relative à la cybersécurité et à la cybercriminalité permet de noter que, les documents électroniques non empreints de signature électronique qualifiée ne sauraient avoir la même valeur juridique que ceux sur lesquels l'on a apposé une signature manuscrite encore moins ceux conclus devant un officier public. Au sens de cette disposition, en l'absence de signature électronique qualifiée ou avancée, le document électronique est à considérer comme tout écrit n'ayant pas fait l'objet de signature manuscrite. Les victimes se trouvent ainsi dans un labyrinthe duquel toute issue semble être un verrou.

CONCLUSION

En définitive, le nouveau paradigme qu'est les web est bien qu'étant un eldorado d'opportunités, ne vient pas sans effets pervers. Son caractère criminogène est renchéri par l'ensemble d'écueils auxquels il soumet les internautes victimes. Il menace la cybersécurité des personnes physiques et morales. Des réponses ont déjà été apportées à certaines difficultés, mais d'autres questions restent en suspens. Il ne sera pas simple de relever le défi de la protection de la personnalité juridique dans le cybermonde, quand bien même la volonté de l'individu serait de se montrer. Rapporter la preuve d'un cybercrime est expose les victimes à deux principales difficultés : l'identification complexe des cybercriminels et les preuves essentiellement instables. Les mesures d'identification qu'offre le législateur camerounais méritent déjà fort bien d'être saluées. Toutefois, les mesures juridiques s'apparentent à une éclipse solaire, car elles procurent clarté d'identité des professionnels, mais maintiennent les acteurs du secteur informel dans une obscurité revitalisée. Les secondes mesures d'identification, les mesures techniques semblent être des constellations éphémères susceptibles d'apporter de la lumière temporairement à l'identité des cybercriminels. Ce caractère météorique est matérialisé par la variabilité de l'adresse IP conjuguée au cantonnement des identifiants qu'offrent les données de connexion. Ils se bornent à identifier la machine utilisée pour commettre l'infraction et non l'utilisateur. Ces différents feux d'artifices méritent d'être complétés par un ensemble de mesures orientées vers une prise en compte du secteur informel en ligne, un contrôle de l'activité des mineurs en ligne et une coopération entre les acteurs judiciaires et les prestataires techniques, au risque pour les internautes potentiellement criminel de

[98] Il s'agit de recourir une fois de plus à la coopération internationale précédemment mentionnée.

[99] Vincent GAUTRAIS et Patrick GINGRAS, « La preuve des documents technologiques », *Les Cahiers de propriété intellectuelle,* Vol. 22, nº 2, 2010, p. 309.

[100] *Ibid*

[101] Dominic REILLY, Carl WREN et Tomas BERRY, « Informatique en nuage : avantages et inconvénients pour les enquêteurs en criminalistique Informatique », *International Journal Multimedia and Image Processing*, 2011, pp. 26-34.

continuer à s'avancer masqués[102]. Par ailleurs, après l'épreuve ardue de l'identification du cybercriminel, les preuves susceptibles d'être rapportées par les victimes mettent une fois de plus ces dernières dans un tunnel dont le bout est difficilement perceptible. A certains égards ces preuves sont le fruit d'une manipulation des cybercriminels, à d'autres elles subissent des techniques de cryptage et de sténographie les rendant non seulement intelligibles pour les victimes elles-mêmes, mais également pour les juges. Quand bien même ces contenus n'auraient pas l'objet de manipulation ou auraient été décryptés, lorsqu'une signature électronique qualifiée n'aurait pas été apposée, les documents fournis par les victimes à titre de preuve n'en seront qu'un commencement. Il en résulte donc pour les victimes et le ministère public de cybercrimes, une véritable traversée d'un labyrinthe. Le salut de ces deux acteurs pourrait provenir d'une alternative cumulable à savoir le recours à des experts en informatique à l'occasion d'un litige, ou la formation d'un type de magistrats spécialisés à cet effet.

BIBLIOGRAPHIE INDICATIVE

✓ Xavier BIOY, (dir.). *La personnalité juridique,* Presses de l'Université Toulouse, Capitole, 2013 ;

✓ Bernard BOULOC, *Droit pénal général*, 20ème éd. Dalloz, 2007 ;

✓ Asa BRIGGS, *A Social History of the Media: From Gutenberg to the Internet*, Cambridge, Polity Press, 2002 ;

✓ Céline CASTETS-RENARD, *Droit de l'internet : droit français et européen*, 2ème éd. Montchretien, Paris, 2012 ;

✓ Cynthia CHASSIGNEUX, *Vie privée et commerce électronique*, éd. Eyrolles, 2004 ;

✓ Rosalie DIARRA, *La répression de la cybercriminalité en Afrique de l'ouest*, L'Harmattan, 2021 ;

✓ Christiane FERAL-SCHUHL, *Cyberdroit : le droit à l'épreuve de l'internet*, 6ème éd., Dalloz, Coll. Praxis Dalloz, Paris 2019 ;

✓ Solange GHERNAOUTI, *La cybercriminalité : le visible et l'invisible*, Collection le savoir suisse, 2009 ;

✓ Olivier ITEANU, *L'identité numérique en question*, éd. Eyrolles, 2010 ;

✓ Dominic JACKSON et Sarah SUMMERS, *L´internationalisation de la preuve criminelle : au-delà de la Common Law et de la tradition de droit civil*. Cambridge : Cambridge University Press. 2012.

✓ Keneth LAUDON, *Management des systèmes d'information*, éd. PEF, 2010 ;

✓ Estelle LODOMEZ, *Le faux informatique : le (faux) frère jumeaux du faux en écritures ?*, DSPC, 2018.

✓ Paul Gérard POUGOUE et Athanase FOKO, *Le statut du commerçant dans l'espace OHADA.: une prospective à l'épreuve du droit matériel uniforme OHADA*, PUA, Yaoundé, 2005 ;

✓ Jean PRADEL, *Droit pénal général,* Cujas 2001 ;

✓ Fabrice ROCHELANDET, *Économie des données personnelles et de vie privée*, La Découverte, collec. Repères, 2011 ;

✓ Jacques VETOIS, *Technologies et usages de l'anonymat sur internet*, éd. l'Harmattan, 2012 ;

✓ Job NZOH SANGONG, *La publicité en ligne, Contribution à la définition de la nature juridique de la publicité sur Internet*, Th. Université de Ngaoundéré, 2019 ;

✓ Chamseddine BARNAT, « l'identification de l'internaute délinquant », *Infojuridique*, Mai 2008, pp. 46-47 ;

✓ FOUAD BENSEGHIR, « L'identification de l'internaute délinquant », *Légavox*, 2016, pp. 7-36 ;

✓ Céline CASTETS-RENARD, « Personnalité juridique et identification numérique », In : *La personnalité juridique* [en ligne]. Toulouse : Presses de l'Université Toulouse 1 Capitole, 2013, pp. 305-317 ;

✓ David CHILSTEIN, « Les nouveaux défis du droit pénal : incriminations générales et spéciales à l'épreuve de l'économie numérique », in *Les nouveaux défis du commerce électronique*, dir. Justine ROCHFELD, LGDJ, Montchrestien, 2010, pp. 94-109 ;

✓ Willy DUHEN, « FAI face à l'anonymat sur internet : vers de nouvelles responsabilités », *Revue terminal*, 2010, p. 33-50 ;

✓ André Desmonds EYANGO DJOMBI, « La nouvelle définition du commerçant dans l'Acte uniforme OHADA au regard de la théorie de l'acte de commerce », *Revue de droit des affaires OHADA*, n° 02, juin-décembre 2012, pp. 239- 253 ;

✓ François FILLIETTAZ, « Comprendre l'identité numérique », *DIP DSI-SEM*, 2011, pp. 2-20 ;

✓ Joseph FOMETEU, « l'influence des moyens électroniques sur le droit des contrats », *Actes du colloque sur » Les pratiques contractuelles d'affaires et les processus d'harmonisation sur les espaces régionaux*, Libreville du 26-28 octobre 2011, *Publication ERSUMA*, juin 2012, pp. 214 à 227 ;

✓ Vincent GAUTRAIS et Patrick GINGRAS, « La preuve des documents technologiques », *Les Cahiers de propriété intellectuelle,* Vol. 22, nº 2, 2010, pp. 269- 313.

[102] Pour paraphraser la célèbre assertion de Réné DESCARTES : « Je m'avance masqué ».

✓ Fabius Corneille KAMLA FOKA, « Le Registre du Commerce et du Crédit Mobilier (RCCM) OHADA depuis la réforme du 15 décembre 2010 : de la transformation à la transfiguration », *RDA* 1ère année de parution, 2012-n°1, pp. 189-205.

✓ Antoine LEPAGE, « Le délit d'usurpation d'identité : questions d'interprétation », *JCP* 2011, pp. 913-918 ;

✓ Jeanine MARTELLIET Anne-Sophie GRENIER, « l'identité numérique », *Journées du réseau DV IST* 9 avril 2013, pp. 3-39 ;

✓ Richard MELTZ, « Une vie transparente sur internet », in *Internet et réseaux sociaux*, dir. Dominique CARDON, Problèmes politiques et sociaux, la Documentation française, n° 984, mai 2011, pp. 103 et s.

✓ Myriam QUEMENER « Réponses pénales face à la cyberpédopomograpgie ». *Actualité Juridique pénale* n° 3/2009, édition Dalloz 2009, pp. 107-111.

✓ Jean-Claude VIMONT, « Des coupables aux victimes, l'archéologie de l'identité du mineur délinquant au XIXe siècle », *Revue d'histoire de l'enfance « irrégulière »*, 2016, pp. 7-28.