



LA RESPONSABILITE DES ACTEURS DANS LE CYBER ESPACE : LE CAS DU CAMEROUN

Par

Enyegue Caroline Patricia

Ph.D en droit privé- Université de Yaounde II- Soa Cameroun

Chargée de cours

cpseptembre792002@yahoo.fr Tel 237-699438018

Résumé

Internet est devenu une nécessité car il constitue un outil indéniable de communication, d'échange, de commercialisation des biens ou services. Cependant l'internet a un pan qualifié de liberticide à raison des dangers accrus d'atteintes aux personnes et aux biens d'où l'affirmation d'un auteur selon laquelle internet « inquiète plus qu'il épanouit ». Cette affirmation est d'autant vraie que la recherche des auteurs d'infractions dans le cyberspace est émaillée de plusieurs difficultés dues aux caractères du cyberspace et à l'application du droit dans l'environnement cybernétique. Néanmoins le cyberspace ne constitue pas une zone de non droit et rime donc avec responsabilité. Parler de la responsabilité des acteurs dans le cyberspace est tributaire de l'exigence d'un contenu illicite et de l'imputation de la faute en fonction des activités exercées par les acteurs du cyberspace. Toutefois vu les mutations majeures que cet environnement induit dans le droit, ces paradigmes étatistes paraissent insuffisants pour rendre compte de la globalité de cet espace numérique.

Mots clés : responsabilité- cyberspace- internet- faute- rôle.

Abstract

The Internet has become a necessity because it constitutes an undeniable tool for communication, exchange, and marketing of goods or services. However, the Internet has a side described as liberticidal due to the increased dangers of attacks on people and property, hence the assertion of one author that the Internet "worries more than it fulfills." This assertion is all the more true since the search for perpetrators of offenses in cyberspace is punctuated by several difficulties due to the characteristics of cyberspace and the application of the law in the cybernetic environment. Nevertheless, cyberspace is not a lawless zone and therefore rhymes with responsibility. Talking about the responsibility of actors in cyberspace is dependent on the requirement of illicit content and the role played by the various stakeholders in cyberspace. However, given the major changes that this environment induces in the law, these statist paradigms seem insufficient to account for the entirety of this digital space.

Key words:

Responsibility- cyberspace-internet-fault-attribution



Le terme cyber espace a été créé par l'auteur de science-fiction William Gibson qui l'a popularisé dans son roman neuromancien en 1984¹. Il désigne l'ensemble de l'infrastructure physique et des données numériques interconnectées à travers le monde formant un espace virtuel où s'échangent des informations et où opèrent les systèmes informatiques et les réseaux comme internet². Autrement dit le cyber espace est l'espace de l'internet et des mondes virtuels. Dans le cadre de ce travail le cyber espace sera assimilé à internet. Internet encore appelé village planétaire est devenu une nécessité incontournable car facilite l'accès à l'information, à l'éducation et à la recherche tout en réduisant les coûts et les distances. Par une simple connexion sur le réseau, l'internaute peut tout faire par exemple acheter de la marchandise en ligne, accéder aux réseaux des administrations publiques pour effectuer des opérations administratives à distance, appeler ses proches dans le monde entier, effectuer ses études à distance dans d'autres pays, accéder à l'information etc.

Sur le plan économique, l'internet est un moteur de croissance de développement, facilitateur des échanges commerciaux, levier du commerce en ligne etc. Bref internet est un nouvel eldorado pour tous ceux qui souhaitent communiquer, échanger, commercialiser des biens ou services.

Néanmoins le luxe qu'offre internet a un prix car crée de nouveaux types de dommages qui n'existaient pas avant et intensifie les dommages traditionnels. L'internet mal utilisé porte préjudice aux tiers à travers la diffamation, la pédopornographie, la haine raciale, le terrorisme, l'atteinte aux droits d'auteurs et d'autres³. Les possibilités de communication offertes par internet sont la principale cause des faits illicites que l'on y trouve. Les individus commettent en ligne des actes qu'ils n'oseraient pas faire dans le monde réel⁴. De plus l'ouverture du réseau internet permet aux informations transmises sur ce réseau de circuler à une échelle planétaire, plus ces informations sont accessibles plus elles peuvent être consultées et plus produire de nombreux dommages. Malgré ce côté novateur et avantageux du numérique, l'internet a un pan

¹ Neuromancien est le premier roman de science-fiction de William Gibson publié en 1984. Il est généralement considéré comme le roman fondateur du mouvement cyberpunk.

² A. Kchaou, La responsabilité civile et internet, thèse, Université Jean Moulin Lyon 3, 2022, p 45.

³ A. Elloumi, « la responsabilité délictuelle sur internet » *Etudes juridiques*, no 14, 2007, p53

⁴ A ce propos Katharine Viner, rédactrice en chef du Guardian affirme « à l'heure du numérique, il n'y a jamais été aussi facile de publier des informations mensongères qui sont immédiatement reprises et passent pour des vérités... » Voir Katharine Viner, rédactrice en chef de Guardian « comment le numérique a ébranlé notre rapport à la vérité », 12 juillet 2016.



qualifié de liberticide à raison des dangers accrus d'atteintes aux personnes et de violations de leur intimité d'où l'affirmation d'un auteur qu'internet « inquiète plus qu'il épanouit »⁵.

Il est donc impérieux d'assainir le cyberspace et d'encadrer les rapports entre les différents acteurs d'autant plus que l'internet n'est pas une zone de non droit. Et partant la liberté d'expression, la vie privée des intervenants, la responsabilité de ceux-ci et la protection des données doivent être règlementées par la loi. En effet la confiance des usagers avec internet passe par une responsabilité des acteurs. Parler de la responsabilité des acteurs revient à définir le terme. La responsabilité « est l'obligation de répondre d'un dommage devant la justice et d'en assumer les conséquences civiles, pénales, disciplinaires, etc. »⁶. C'est la responsabilité juridique. Il s'agit de l'obligation de réparer le dommage causé à autrui, dont un intérêt légitime a été injustement lésé par un acte contraire à l'ordre juridique⁷. Dans le cadre de la responsabilité juridique, la responsabilité pénale désigne l'obligation pour une personne physique ou morale de répondre devant la justice d'une infraction commise et de subir la peine prévue par la loi contrairement à la responsabilité civile⁸ dont le but principal est de réparer les dommages subis par la victime soit dans un cadre contractuel⁹ ou délictuel¹⁰. La responsabilité civile repose sur la réunion de trois éléments essentiels à savoir une faute, un dommage et un lien de causalité entre les deux tandis que la responsabilité pénale repose sur un fait ou acte défini et interdit par la loi et vise à sanctionner l'auteur de l'infraction même en dehors de tout préjudice subi par autrui.

Cependant la relation responsabilité et internet fait naître plusieurs difficultés d'ordres différents. En effet l'internet bénéficie de plusieurs atouts notamment le caractère transnational¹¹, le caractère dématérialisé¹², volatil¹³, et anonyme¹⁴ de l'outil internet sans oublier la multiplicité des intervenants à savoir les prestataires techniques comme les fournisseurs d'accès internet, les fournisseurs d'hébergement, et les simples utilisateurs de

⁵ L. Cadoux, « informatique et libertés en 1997, vers où allons-nous ? Éléments de prospective », *Gaz, Pal*, 1997, p 645.

⁶ G. Cornu, *Vocabulaire juridique*, association Henri Capitant, PUF, 15 édition, p821.

⁷ *Ibid*, p452.

⁸ J.Lagoutte, Les conditions de la responsabilité en droit privé : éléments pour une théorie générale de la responsabilité juridique, thèse, université de Bordeaux4, 2012, p 217.

⁹ La responsabilité civile contractuelle découle de l'inexécution ou de la mauvaise exécution d'un contrat.

¹⁰ La responsabilité civile délictuelle ou extracontractuelle résulte d'un acte illicite ou d'une faute commise en dehors de tout lien contractuel.

¹¹ C. Enyegue, « l'enquête pénale à l'épreuve de l'internet » *Revue internationale du chercheur*, vol 5, no 1, 2024, p 1-32.

¹² *Ibid*

¹³ *Ibid*.

¹⁴ *Ibid*.



service ou internaute. La victime se retrouve dans le désarroi en cas de préjudice subi lors de la diffusion de contenus illicites et n'hésite pas parfois à recourir aux intermédiaires techniques car facilement identifiables et plus solvables que la personne ayant commis le délit.

En outre la difficulté en matière de responsabilité sur Internet est de placer un curseur entre responsabilité et liberté car les deux sont des notions intrinsèquement liées. Le cyberspace offre une grande liberté d'expression mais cette liberté ne saurait être absolue et doit être encadrée par le droit de la responsabilité. Ces entraves sont donc à l'origine de l'impunité observée dans le monde numérique créant un climat d'austérité, d'insécurité, et de perte de confiance des internautes sur l'outil internet.

Toutes ces difficultés montrent pourquoi ce sujet mérite qu'on s'y attarde d'autant plus que l'Afrique et en particulier le Cameroun est en construction d'un cadre juridique et institutionnel en matière du contentieux de la responsabilité dans le cyber espace. L'internet devient donc un laboratoire permettant de tester la persistance de l'adaptabilité et de la généralité de la responsabilité tant civile que pénale¹⁵.

Mais il faut le relever des pas considérables sont faits en matière législative pour contrecarrer les dérives constatées sur le net et rendre l'espace numérique plus transparent, plus respectueux des droits des utilisateurs et de meilleur qualité. On voit à quel point les règles posées par les Etats jouent un rôle majeur en ce qu'elles déterminent les responsabilités dans la participation à la communication dans internet¹⁶. L'internet rime donc avec responsabilité. Cela se traduit par les multiples lois¹⁷ adoptées par le législateur qui tant bien que mal essaient de réguler les rapports dans le cyberspace favorisant ainsi un développement harmonieux et durable du numérique. Mais il est aussi naïf d'ignorer les mutations majeures que le cyber espace induit dans le droit¹⁸.

Il revient donc de se poser la question suivante : sur quoi repose la responsabilité des acteurs dans le cyber espace ? Autrement dit quelles sont les conditions de la responsabilité des acteurs dans le cyber espace ?

L'étude de la législation nationale, internationale et de la jurisprudence laisse entrevoir que la responsabilité des acteurs dans le cyberspace est tributaire de l'exigence d'un contenu illicite

¹⁵ A. kchaou, La responsabilité civile et internet, thèse, Université Jean Moulin Lyon 3, 2022, p 245.

¹⁶ P. Trudel, « Les responsabilités dans le cyberspace » in Unesco, *les dimensions internationales du droit du cyberspace*, Paris, Economica, 2000, p236-269,

¹⁷ Loi de 2010 sur la cybersécurité et la cybercriminalité, loi no 2010 /013 du 21 décembre 2010 régissant les communications électroniques au Cameroun, la loi no 2023/009 du 25 juillet 2023 relative à la charte de l'enfant sur internet au Cameroun.

¹⁸ P.Trudel, « Quel droit et quelle régulation dans le cyberspace ? *Sociologie et sociétés*, vol 32, numero2, 2000, p 190-210.



(I) et de l'imputation de la faute en fonction des activités exercées par les acteurs du cyberspace (II).

I- L'exigence d'un contenu illicite

Le cyberspace est un espace d'expression et de communication puissant permettant à chacun de s'exprimer et d'accéder à une multitude d'informations. La liberté d'expression se déploie de manière intense dans le monde numérique par la liberté de création de contenu, de partage, de publications. Cependant, les abus de la liberté d'expression sont renforcés par les réseaux sociaux. Ainsi, comme le souligne Anne Cousin, « les réseaux sociaux sont le principal moyen des abus de tous genres de la liberté d'expression, des plus anodins aux plus graves dans des conditions ou des proportions qui conduisent légitimement à s'interroger sur leur rôle à cet égard »¹⁹. Le contenu illicite dans le cyberspace englobe toutes les informations, données ou activités en ligne qui sont interdites par la loi et considérées comme contraires à l'ordre public. Ces contenus peuvent inclure des éléments à caractère diffamatoire, terroriste, à la haine raciale, pédopornographique ou encore porter atteinte à la vie privée, etc. Ces contenus illicites peuvent découler soit d'une faute civile (A) soit d'une faute pénale(B).

A- L'illicéité en raison d'une faute civile

La faute est le fondement traditionnel de la responsabilité civile délictuelle qui tire sa base de l'article 1382 du Code civil qui dispose que « tout fait quelconque de l'homme qui cause à autrui un dommage oblige celui par la faute duquel il est arrivé à le réparer ». Il revient donc à la victime de prouver l'existence d'un préjudice résultant d'un fait dommageable. Contrairement à la responsabilité pénale, laquelle peut être engagée du seul fait de la tentative, la responsabilité civile suppose un fait dommageable ayant causé un préjudice. En effet l'article 1383 du Code civil dispose que « chacun est responsable du dommage qu'il a causé non seulement par son fait mais encore par sa négligence ou par son imprudence »,

On doit en principe considérer que le fait de nature à engager la responsabilité personnelle de son auteur n'est pas n'importe quel fait mais seulement le fait fautif. Il revient donc de se demander qu'est-ce que la faute ? Le législateur ne définit pas la notion de faute, néanmoins la doctrine à l'instar de Planiol définit la faute comme la violation d'une obligation préexistante, d'autres par contre voient en la faute un acte illicite contraire à la loi. La jurisprudence quant à

¹⁹ E. Guérin, « La liberté d'expression à l'ère du numérique : le délicat équilibre sur les réseaux sociaux », disponible sur www.village.de.la.justice, consulté le 17 juin 2025.



elle considère comme fautifs tous les comportements qui lui paraissent anormaux : imprudence, négligence et même simple maladresse. Parler de la faute civile oblige à mettre en lumière plusieurs types d'atteintes. Nous nous limiterons aux atteintes aux droits subjectifs des personnes en nous appesantissant sur l'atteinte au droit à l'image à l'ère numérique (1) et l'atteinte à la vie privée sur internet (2).

1- Atteinte au droit à l'image à l'ère numérique

L'image peut être définie comme « l'ensemble de points ou éléments représentatifs de l'apparence d'un objet, formés à partir du rayonnement émis, réfléchi, diffusé ou transmis par l'objet »²⁰. L'image d'une personne est l'un des attributs de la personnalité du fait qu'elle dégage son originalité et lui permet de se différencier de ses congénères²¹. Le droit à l'image est un aspect essentiel du droit à la vie privée et à la protection des données personnelles particulièrement pertinent à l'ère du numérique. Il permet à un individu d'autoriser ou de refuser la reproduction et la diffusion publique de son image²². Le droit à l'image comporte deux composantes. La première est morale, elle représente le droit de refuser d'être photographié ou de laisser publier sa photo et la seconde composante est patrimoniale, c'est le cas d'aménager contractuellement l'exploitation de son image²³.

Avec la prolifération des technologies de capture d'images comme les smartphones²⁴, les caméras de surveillance, les réseaux sociaux²⁵, cela soulève des questions sur la protection de l'image personnelle d'où un contentieux complexe et abondant.

Le droit à l'image à l'ère numérique est déterminé par les différents types d'images qui correspondent à une forme d'atteinte particulière. On distingue les atteintes à l'image photographique et les atteintes à l'image numérique.

²⁰ Dictionnaire Larousse, version électronique, 2024, voir image.

²¹ P. Voirin, G. Goubeaux, *droit civil, introduction aux droit des personnes- famille- personnes protégées- biens- obligations- suretés*, LGDJ lextenso, 43 édition, 2024, p255.

²² Toute personne a le contrôle sur la captation de son image et sur l'utilisation de celle-ci. Ainsi toute personne désirant publier une photo ou vidéo faisant apparaître un individu doit recueillir le consentement de ladite personne pour capter son image et l'utiliser ultérieurement soit pour la publier ou la diffuser. Cependant le consentement de la personne n'est pas requis si l'image non cadrée est prise dans le public, si la photographie illustre un sujet d'actualité, un sujet historique marqué par le droit à l'information²², s'il s'agit d'une personnalité publique dans l'exercice de ses fonctions.

²³ M. Serna, *L'image et le droit*, thèse, Université de Paris 2, 1994, p 85.

²⁴ Chaque individu est susceptible de partager des milliers de photos personnelles et des séquences de vidéo sur la toile.

²⁵ Les plates-formes comme facebook, instagram ou tiktok permettent le partage d'images et de vidéos de manière instantanée et virale.



On entend par image photographique, tout cliché quels qu'en soient l'objet, visage et/ou silhouette d'un individu reconnaissable, le contexte de la prise de vue, le support et le média, imprimé, vidéo animée et/ou numérique. L'image peut être fixe ou mobile tant qu'elle rend identifiable la personne. Toute personne a le droit d'accepter ou de refuser que sa photo soit publiée ou diffusée sur les réseaux sociaux. Il convient cependant de souligner que le droit à l'image est protégé²⁶ et toute violation au droit à l'image entraîne la responsabilité civile basée sur le fondement de la faute²⁷ de son auteur qui se résout en paiement de dommages et intérêts. Cette responsabilité civile est fondée sur l'article 1382 du code civil²⁸. Par ailleurs, la loi de 2010 sur la cybersécurité et la cybercriminalité protège le droit à l'image sur internet et punit toute personne qui fait mettre en ligne les données nominatives qui font apparaître ses origines tribales, ses opinions politiques, religieuses, tribales, syndicales ou ses mœurs²⁹, ou qui divulgue des informations relatives à une personne physique identifiée portant atteinte à la considération de la victime³⁰ ou qui diffuse, enregistre à but lucratif par la voie de communications électroniques sans le consentement de l'intéressé des images portant atteinte à l'intégrité corporelle³¹.

En outre la victime peut également demander à l'hébergeur d'internet le retrait des images³². En effet, dès le moment où les hébergeurs ont eu connaissance de l'atteinte au droit à l'image,

²⁶ La diffusion d'une photographie sur internet est illicite si le diffuseur n'a pas obtenu le consentement préalable des personnes concernées à savoir l'auteur de la fixation en vertu du droit d'auteur et la personne, objet de la fixation. Ce consentement doit être exprès, écrit et limité à des utilisations déterminées.

²⁷ La faute de l'auteur est présumée lorsqu'il diffuse l'image d'autrui sans son consentement. Les victimes d'atteinte au droit à l'image peuvent exiger la réparation sur le fondement de la faute, à cet égard elles doivent prouver la faute de l'auteur de l'atteinte pour engager sa responsabilité civile. Voir affaire Altern, affaire mannequin Mademoiselle Estelle Lefebure c/ magazine Voici. En effet la plaignante avait été prise en photo alors qu'elle était nue par son petit ami, quelques temps après Estelle quitta ce petit ami et se maria avec le jeune Hallyday. Quelques années plus tard le journal Voici diffusa ces photos privées en exclusivité, les photos ayant du être fournies par l'ex petit ami sans l'autorisation d'Estelle Halliday. Ce journal a bien entendu été condamné pour cela. Toute publication de l'image d'une personne suppose en principe l'autorisation de l'intéressé. On a constaté sur internet une diffusion d'images particulièrement choquantes. Des internautes mettent en ligne des photographies de leur ex compagne ou compagnon en tenue d'Adam et Eve afin de se venger d'avoir été quittés ou trompés. La mise à disposition en ligne de ces photographies sans accord des intéressés constitue des atteintes à la vie privée.

²⁸ Voir TGI Wouri, jugement no 4210/ CIV du 13 mai 2019, Affaire Samuel Eto'o fils contre Orange Cameroun, inédit, en effet la société Orange Cameroun a été condamnée à verser plus de 650 millions de francs CFA à l'ancien capitaine des lions indomptables en raison d'avoir utilisé illégalement l'image du footballeur dans le cadre de ses activités et campagnes publicitaires.

²⁹ Art 74 a 5 de la loi de 2010 sur la cybersécurité et la cybercriminalité au Cameroun.

³⁰ Art 74 a 8 voir TPI de Yaoundé centre administratif, jugement no 4258/COR, du 12 septembre 2019, Affaire Ministère public et Nnang agnes c/ Onana Vincent, inédit. Sieur Onana a publié sur Facebook la photo de sa débitrice indélicat et celle du géniteur de celle-ci en les traitant d'escroc sans le consentement de ces derniers en vue de les nuire en portant atteinte à leur considération et à leur image.

³¹ Art 75 a1 de la loi de 2010 relative à la cybersécurité et la cybercriminalité au Cameroun.

³² Voir article 34 alinéa2 de la loi de 2010 sur la cybersécurité et la cybercriminalité au Cameroun



ils doivent agir promptement pour retirer les images ou rendre leur accès impossible. Cependant plusieurs questions peuvent se poser à savoir premièrement si les hébergeurs doivent se fier à ce que dit la victime ou alors est ce que l'injonction de retirer la ou les photos doit-elle provenir d'une autorité judiciaire ? En second lieu l'adverbe « promptement » utilisé par le législateur veut dire quoi. En d'autres termes combien de temps dispose l'hébergeur pour retirer la ou les photos publiées sans autorisation.

Par ailleurs une question mérite d'être soulevée à savoir est ce que l'interdiction de la publication d'autrui peut-elle être considérée comme une violation de la liberté d'expression sur internet ? La jurisprudence française a répondu que le droit à l'image n'est pas une information à laquelle le public aurait nécessairement droit au titre de la liberté d'expression³³. Il revient donc de rechercher à concilier la liberté d'expression sur internet avec la nécessaire protection de la vie privée.

On entend par image numérisée, tout individu fiché dans de multiples fichiers privés et publics, image conforme ou non au profil recherché ou établi à partir de données personnelles identifiants. Il s'agit de toute information à savoir l'adresse, la profession, la photo, la vidéo conservée en mémoire, l'empreinte, le nom, permettant l'identification d'un individu d'où le qualificatif de donnée personnelle.

En effet, la divulgation rapide, large et facile de l'information sur internet a provoqué des problèmes juridiques relatifs à la protection des données à caractère personnel, étant entendu que les données personnelles sont devenues la cible privilégiée des cybercriminels en raison de leur forte valeur ajoutée³⁴. Ainsi, la collecte, la conservation et le traitement des données permettent de dresser des portraits de l'intéressé, de repérer les lieux où il se trouve, d'analyser ses comportements de consommateur³⁵ et notamment donner lieu à une menace pour notre vie privée. A cet effet les données personnelles font l'objet d'un contrôle et d'une réglementation³⁶ afin de limiter voire de réduire les risques d'intrusions grâce à des systèmes de surveillance, de traçabilité et de ciblage personnalisé, de diffusion et de divulgation.

Ainsi des principes cardinaux et obligations pèsent sur les opérateurs et services responsables de fichiers. Il s'agit en premier lieu de la loyauté, de la licéité, de la transparence dans la collecte

³³ Voir ch. Civ, 1, 9 juillet 2009, no 07-19-758.

³⁴ En septembre 2018 une faille sur le réseau social Facebook a permis le piratage de 50 millions de comptes, en 2013, la cyber attaque la plus importante de Yahoo a subi la perte de trois milliards de comptes utilisateurs.

³⁵ M. Barre – Pepin, « Droit à l'image en matière d'internet et de réseaux sociaux », article disponible sur <https://hal.archives-ouvertes.fr/hal-01703966/document>, consulté le 2 février 2025.

³⁶ Loi no 2024 /017 du 23 décembre 2024 relative à la protection des données à caractère personnel au Cameroun



avec pour corollaire une obligation d'informer³⁷ les intéressés sur l'objet et la finalité³⁸ du traitement³⁹ des données et dans certains cas recueillir leur consentement exprès⁴⁰, en second lieu la sécurité⁴¹ par la prise en compte des mesures de précaution dans la conservation⁴² et de la confidentialité⁴³. En cas de non-respect de ces obligations, des sanctions ont été instituées par la loi⁴⁴.

2- L'atteinte à la vie privée sur internet

Si l'on en croit Robert Badinter « toute vie s'avère partagée entre deux zones, l'une d'intimité et de secret, l'autre de participation publique à l'activité de la cité »⁴⁵. Cette réflexion confirme l'existence d'une sphère intime de la vie de l'individu qu'il importe de protéger contre les atteintes susceptibles de lui être portées. Le besoin de protection qui n'a cessé de croître avec les progrès de la technologie a ainsi conduit à l'émergence du droit au respect de la vie privée sur internet⁴⁶.

Le droit au respect de la vie privée se différencie du droit à l'image car le droit à l'image est un droit autonome et la seule diffusion de l'image peut constituer en soi une atteinte alors que l'image ne révèle aucun aspect de la vie privée⁴⁷.

L'atteinte à la vie privée peut être définie comme étant tout trouble à l'autonomie, la paix, la tranquillité des activités personnelles et familiales. Ces atteintes à la vie privée⁴⁸ ont considérablement augmenté avec internet ; car ce moyen permet à tout individu de diffuser à

³⁷ Art 14 de la loi n° 2024/ 017 du 23 décembre 2024 relative à la protection des données à caractère personnel.

³⁸ Voir art 11 sur la loi n° 2024/ 017 du 23 décembre 2024 relative à la protection des données à caractère personnel.

³⁹ On entend par traitement des données, toute forme d'opération entièrement ou partiellement automatisée mais aussi manuelle qui peut être appliquée à des données personnelles à condition qu'elle soit méthodique. On peut citer comme opération de traitement la collecte, l'enregistrement, le stockage, la modification, l'extraction, la consultation, la communication, l'interconnexion des données.

⁴⁰ Voir art 9 alinéa 1 de la loi n° 2024/ 017 du 23 décembre 2024 relative à la protection des données à caractère personnel.

⁴¹ Le responsable de traitement est tenu de prendre toute précaution au regard de la nature des données pour empêcher qu'elles soient déformées, endommagées, copiées ou que des tiers non autorisés y aient accès lors de la communication ou du transport de supports de données.

⁴² Voir art 13 de la loi n° 2024/ 017 du 23 décembre 2024 relative à la protection des données à caractère personnel.

⁴³ Art 7 et 15 de la loi n° 2024/ 017 du 23 décembre 2024 relative à la protection des données à caractère personnel.

⁴⁴ Art 74 alinéa 3 de la loi de 2010 relative à la cybersécurité et cybercriminalité.

⁴⁵ Allocution du procureur général près la cour suprême de la république du Sénégal du mardi 25 janvier 2024 sur le thème de « la protection de la vie privée ».

⁴⁶ *Ibid.*

⁴⁷ M. Barre – Pepin, « Droit à l'image en matière d'internet et de réseaux sociaux », article disponible sur <https://hal.archives-ouvertes.fr/hal-01703966/document>, consulté le 2 février 2025.

⁴⁸ Y. R. Kalieu Elongo, « réseaux sociaux, internet et vie privée, » disponible sur <https://kalieu-elongo.com>, consulté le 15 janvier 2025, H. Tchambo Sontang, « vie privée et réseaux sociaux » leçon inaugurale, rentrée solennelle, université de Dschang, 2023- 2024.



l'échelle internationale des informations, y compris celles portant atteinte à la vie privée. Internet représente donc une réelle menace pour le droit à la vie privée qui se dévoile à travers une intrusion dans la sphère privée d'une part et par une absence de consentement d'autre part.

L'intrusion dans la sphère privée s'opère de plusieurs manières. Soit par la négligence et la vulnérabilité des internautes face à la complexité de la matière informatique qui peuvent perdre le contrôle de leurs données personnelles et faciliter ainsi le vol d'identité, de mots de passe, des coordonnées bancaires, etc. Soit par le fonctionnement de certains sites ou réseaux sociaux qui participent au dévoilement par les internautes eux-mêmes de leur vie privée en exposant leur vie quotidienne sur la toile en faisant preuve d'imprudence, d'insouciance.

En effet les sites de réseaux sociaux comme Facebook utilisent deux moyens centrés uniquement sur la personne utilisatrice. Il s'agit de mettre une photographie de soi-même afin d'être identifié par ses connaissances, en second lieu mettre des informations sur sa personne suggérées par le site à savoir le nom, la fonction, etc. Tout profil sur les sites de réseaux sociaux comprend un nombre assez important d'informations diverses sur la personne utilisatrice. Les usagers dévoilent leur vie quotidienne, leurs états d'âme, leurs succès, leurs échecs, leurs exploits sur un media à vocation publique. L'aspect intime de la vie semble se transformer et devient une intimité partagée⁴⁹. Malheureusement ces internautes semblent sous-estimer l'intérêt que leurs informations personnelles peuvent représenter et s'exposent à de nombreux dangers. C'est ainsi que ces informations peuvent être utilisées par des individus malveillants en vue de commettre des infractions⁵⁰. La divulgation de la vie privée d'un individu est tributaire de l'exigence du consentement. A contrario, l'absence de consentement induit à la faute et engage la responsabilité du mis en cause.

En effet, le consentement doit être exprès c'est-à-dire que l'autorisation de l'intéressé doit s'exprimer formellement par écrit, le consentement doit être en plus être spécial. Autrement dit, l'autorisation est donnée dans un but déterminé et sa portée est limitée à une ou plusieurs

⁴⁹ C. Vallet, « le dévoilement de la vie privée sur les sites de réseau social. Des changements significatifs » disponible sur www.cairn.info, consulté le 19 janvier 2025.

⁵⁰ Il est donc possible de choisir sa victime et de personnaliser la mise en contact avec les diverses informations récoltées. Histoire de braquage dont les bandits ont utilisé les informations provenant des réseaux sociaux. Les cybercriminels se retrouvent à recueillir sans grande difficulté une masse importante de données à caractère personnel d'un grand nombre de personnes qui pourraient être de potentielles victimes sans toutefois prendre de véritables risques contrairement au monde réel.



utilisations spécifiées et en outre, le consentement n'est jamais définitif, et ne permet pas une redivulgaration ultérieure d'où la question posée dans le contexte de l'internet du droit à l'oubli⁵¹.

B- L'illicéité en raison d'une faute pénale

Internet a changé le monde en impulsant une révolution perpétuelle dont les répercussions n'ont pas encore fini de secouer notre mode de vie, métamorphosant en profondeur les habitudes ainsi que l'accès à l'information⁵². Non seulement l'internet brise les anciennes habitudes pour en créer de nouvelles⁵³ en développant les domaines économique, culturel, social, agricole etc. Mais malgré ces ressources prometteuses, internet apporte aussi un lot d'inquiétudes et de menaces qui relativisent tous les progrès réalisés. Le doyen Carbonnier observait déjà il y a trente ans que «l'évolution des mœurs et des techniques donne matière à de nouvelles formes de délinquance»⁵⁴, cette observation résonne toujours avec autant de force et de gravité. Incontestablement internet a donné naissance à de nouvelles formes de criminalités(2) et a favorisé la commission exponentielle des infractions classiques(1) rendant les criminels mieux armés et les victimes plus vulnérables.

1-Internet, moyen de développement des infractions classiques

Internet offre de nombreux avantages aux internautes y compris aux criminels qui ont vite compris les privilèges qu'ils pourront tirer du réseau internet et notamment dans la facilitation de la commission des infractions. Les délinquants conscients de cet état de choses se sont mis rapidement à l'heure du web et du darkweb. C'est ainsi que les atteintes aux droits de la personne et particulièrement au sexe ont pu évoluer avec les Tic et constituer un nouveau vecteur de criminalité.

⁵¹ Aujourd'hui entrer le nom d'une personne sur des moteurs de recherche comme Google pour s'informer sur celle-ci est une pratique habituelle, pourtant cette recherche peut porter atteinte au respect de la vie privée d'où le droit à l'oubli numérique consacré par l'art 37 de la loi sur les données personnelles. Le droit à l'oubli numérique est aussi appelé droit à l'effacement qui permet à un individu de demander la suppression d'une information en ligne qui la concerne.

⁵² J. Abbas, *les infractions commises sur internet*, Harmattan, 2021, p85 et ss.

⁵³ On peut conclure un contrat d'affaire à de milliers de kilomètres par un simple clic,

⁵⁴ J. Carbonnier, *sociologie juridique*, Paris, PUF, 3e édition, 2016, p 401



Le législateur de 2010 protège la personne dans son individualité propre en réprimant la diffamation, la violation de correspondance⁵⁵, l'usurpation d'identité⁵⁶, les injures etc⁵⁷.

Quant aux atteintes au sexe, elles constituent des infractions pénales commises par des actes de nature sexuelle incluant des contacts sexuels non consentis, des relations impliquant des mineurs, des personnes de même sexe etc. L'internet a favorisé le développement et l'augmentation des infractions sexuelles, ceci est possible grâce aux caractéristiques de l'internet à savoir l'anonymat, la virtualité, l'absence de barrières géographiques, la création des plates-formes⁵⁸ regroupant des personnes partageant les mêmes vices. Face au développement d'internet, nous avons constaté l'accroissement voire la diversification des comportements délictuels déjà existants tels que la pédopornographie, l'homosexualité.

Les mineurs de par leur vulnérabilité et leur présence sur le réseau internet⁵⁹, sont devenus des partenaires sexuels pour le plus grand plaisir des consommateurs de ce genre de matériel⁶⁰. Face à cette inquiétude, le législateur a initié la loi de 2010 sur la cybersécurité et la cybercriminalité en ses articles 76, 80, 81 afin de lutter contre ce fléau. On entend par pédopornographie ou pornographie enfantine tout acte présentant de manière visuelle⁶¹ un

⁵⁵ TPI de Yaoundé centre administratif, jugement no 457/COR du 5 février 2023, affaire ministère public Ambassa Judith c/ Enanga Seraphin, inédit. Voir art 84 a1 1et 2 de la loi de 2010 relative à la cybersécurité et la cybercriminalité. On peut citer le cas de la violation de la correspondance privée où un individu lit le contenu d'un mail à l'insu de son émetteur ou destinataire d'où le forçage de mail. La question qui s'est posée est de savoir si on peut assimiler le courrier électronique à la correspondance privée au même titre que les lettres, le tribunal de grande instance de Paris du 2 novembre 2000 a répondu par l'affirmative en qualifiant le courrier électronique de correspondance privée. La loi de 2010 sur la cybercriminalité à travers l'art 84 a1 punit toute personne qui prend frauduleusement connaissance des communications électroniques adressées à autrui contrairement à l'art 300a 2du code pénal qui écarte de son champ d'application les conjoints, les père et mère, tuteur ou responsable coutumier de leurs enfants mineurs de 21 ans non émancipé

⁵⁶ Voir art 48a2 de la loi de 2010 relative à la cybersécurité et la cybercriminalité. l'usurpation d'identité qui est le fait de prendre délibérément l'identité d'une autre personne vivante pour réaliser des actions frauduleuses commerciales, civiles ou pénales, accéder aux finances de la personne usurpée ou commettre en son nom un délit etc. Plusieurs modalités d'usurpation sont possibles sur le net, on peut citer la création de fausses pages Facebook au nom de la victime, vol de mot de passe ou de code secret.

⁵⁷ F. Mattatia, « l'usurpation d'identité sur internet dans tous ses états », *RSC*, 2014/2, p 331à337.

⁵⁸ Avant internet une personne qui avait un intérêt sexuel pour les enfants se sentait seul maintenant elle fait partie d'une communauté mondiale, elles interagissent en ligne avec d'autres personnes ayant des intérêts semblables en échangeant des fantasmes, des techniques des images voire de vrais enfants.

⁵⁹ C. vallet, la protection des mineurs face à la cyberpédopornographie, étude comparée entre le droit criminel canadien et français, thèse, université de Montréal, 2009, p45.

⁶⁰ Ibid.

⁶¹ Néanmoins il faut le souligner la loi de 2010 sur la cybersécurité et la cybercriminalité se limite au matériel visuel (images) et se désintéresse de l'ensemble des autres supports à savoir les matériels audio⁶¹ ou écrit qui feraient l'apologie de la pédopornographie. Il serait donc judicieux que le législateur 2010 puisse tenir compte de tous ces supports en reformulant la définition de la pornographie enfantine comme tout acte présentant de manière



mineur se livrant à un comportement sexuellement explicite⁶², une personne qui apparaît comme mineur se livrant à un comportement sexuellement explicite, des images réalistes présentant un mineur se livrant à un comportement sexuellement explicite⁶³. L'infraction de pédopornographie se matérialise à travers plusieurs canaux à savoir la production, la fixation, la mise à disposition⁶⁴, la distribution, l'offre⁶⁵, la diffusion⁶⁶, la transmission, l'acquisition, la détention⁶⁷, le fait de se procurer⁶⁸ ou de procurer à autrui l'image ou une représentation à caractère pédophile. Ces différents moyens ont pour but de sanctionner l'ensemble des actes pouvant permettre à la commission l'infraction⁶⁹. La pédopornographie peut revêtir plusieurs formes soit elle peut être constitutive d'un délit⁷⁰, soit d'un crime⁷¹. Par ailleurs ces faits ci-dessus mentionnés doivent avoir été commis intentionnellement, cette condition est essentielle car permet de punir ou non certains utilisateurs du net qui se retrouveront en possession des images pornographiques sans le savoir⁷².

visuelle, audiovisuelle, textuelle, un mineur se livrant à un comportement sexuellement explicite etc. Ceci permettra de punir toute manifestation ou représentation à caractère pédopornographique.

⁶² L'expression comportement sexuellement explicite désigne tout au moins des comportements réels ou simulés suivants à savoir relation sexuelles entre mineurs ou entre un mineur et un adulte du même sexe ou de sexe différent, exhibition des parties génitales d'un mineur.

⁶³ Le législateur punit aussi bien un adulte apparaissant comme mineur ou un mineur fictif créé par des images numériques pour préserver tout image de l'enfant et éviter tout passage à l'acte afin de lutter contre l'exploitation sexuelle des enfants et la traite virtuelle de ces derniers. Il s'agit de protéger tant l'image que la personne de l'enfant car dans tous les cas, l'enfant est réduit à un objet sexuel.

⁶⁴ La mise en disposition vise à inclure la mise en ligne de pornographie enfantine devant être utilisée par autrui par exemple en créant des sites pédophiles mais aussi en créant ou compilant des hyperliens vers les sites pédophiles en vue de faciliter l'accès à la pornographie enfantine.

⁶⁵ Le terme offrir vise à inclure le fait de solliciter autrui afin qu'il puisse se procurer de la pornographie enfantine. Il laisse entendre que la personne qui offre le matériel en question peut effectivement le fournir.

⁶⁶ Par diffusion il faut entendre la distribution active du matériel incriminé sur le réseau sans que celle-ci s'adresse à une personne ne particulier à la différence de la transmission qui consiste à envoyer à une personne désignée de la pédopornographie soit à titre gratuit ou à titre onéreux. Voir P. Rosine, *la construction de l'espace de liberté, sécurité et justice au sein de l'union européenne face à la cybercriminalité : le défi de la lutte contre la pédopornographie sur internet*, mémoire de master, université robert Schuman de Strasbourg, 2007, p26

⁶⁷ La détention ou acquisition de pédopornographie renvoie à toute possession intentionnelle de ce matériel au sein d'un système informatique ou dans un moyen de stockage de données informatiques.

⁶⁸ Il faut le souligner que la consultation des sites de pornographie enfantine est interdite et puni par la loi. Cass ,20 avril 2011, RTDI, numéro 44, 2011 p 27, disponible sur www.juricaf.org consulté le 22 mai 2024.

⁶⁹ En effet l'infraction de pédopornographie constitue une incrimination large car le législateur cherche à punir tout acte pouvant permettre à la commission de ladite infraction.

⁷⁰ C'est le cas lorsqu'il s'agit de la fixation, de la diffusion, l'enregistrement, la transmission à titre gratuit ou onéreux, l'offre, l'importation, l'exportation, la possession de l'image présentant les actes de pédophilie sur un mineur par voie de communications électroniques ou d'un système d'information. Voir art 80 (1)(2)(3) de la loi de 2010 relative à la cybersécurité et la cybercriminalité au Cameroun.

⁷¹ C'est le cas de l'offre, la production, la mise à disposition de pornographie enfantine en vue de la diffusion, le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système d'information, la diffusion ou la transmission de pornographie enfantine par le biais d'un système d'information. Le législateur met l'emphasis sur le caractère large de destination du public et sur de nombreuses représentations à caractère pédophile.

⁷² Ceci est possible par le biais des courriers électroniques non sollicités ou spam ou de cookies.



En outre les propositions sexuelles faites à un mineur sanctionnent le fait pour un majeur de prendre contact avec un enfant / mineur dans le but de le soumettre à des abus sexuels ou à l'exploitation sexuelle en utilisant un moyen de communication électronique. Le législateur est venu pénaliser la pratique du grooming⁷³ qui est une technique d'approche envers les victimes qui se manifeste par le fait qu'un adulte aborde intentionnellement des mineurs et les manipule à des fins sexuelles. Il s'agit d'une infraction de prévention qui sanctionne seulement la simple proposition sans qu'il soit nécessaire que le mineur ait répondu à la demande. Le but est d'éviter des comportements plus graves en intervenant en amont pour dissuader l'adulte d'entreprendre une telle démarche⁷⁴.

2-internet, lieu de naissance de nouvelles infractions

La cybercriminalité est venue révolutionner le monde juridique, étant marqué fortement du sceau de l'immatériel, un vide juridique s'est très vite créé face au décalage entre les normes pénales classiques et les agissements des cyberdélinquants visant de nouvelles valeurs qualifiées par la doctrine de biens informatiques. Devant l'impossibilité de réprimer ces nouveaux comportements dématérialisés par l'arsenal juridique en vigueur, le législateur camerounais à travers la loi de 2010 sur la cybersécurité et la cybercriminalité, a mis sur pied une pléthore de nouvelles incriminations qui reflètent la singularité des comportements criminels visant les valeurs du cyberspace et réalisés au moyen de procédés nouveaux. Ce nouveau mouvement de politique criminelle oscille entre les incriminations afférentes aux atteintes aux systèmes informatiques d'une part et d'autre part les incriminations relatives aux atteintes aux données

⁷³ On parle aussi de séduction mal intentionnée des enfants, de pédopiegeage ou de manipulation psychologique des enfants. . En d'autres termes l'adulte aborde un mineur de manière psychologique et sociale afin d'obtenir des faveurs sexuelles ou des clichés ou images pornographiques. Le délinquant prend souvent du temps pour essayer de gagner la confiance de l'enfant jusqu' à ce qu'il noue avec lui des liens affectifs. L'objectif pour le délinquant est d'isoler le mineur de sa famille, de ses amis et de ses fréquentations pour créer chez celui-ci un sentiment de dépendance envers lui et par conséquent exercer du pouvoir et un contrôle sur leurs victimes. Les délinquants emploient le plus souvent un certain nombre de stratégies pour arriver à leur fin. On peut dénombrer entre autres l'offre de conseils⁷³ et une écoute bienveillante, l'achat des cadeaux, le partage des secrets, faire des compliments et être attentionné.

⁷⁴ S. Takoudju, « Les règles de droit face à la pédopornographie 2.0 », disponible sur www.village.de.la.justice. Com, consulté le 10 mai 2025, .M. Chawki, *la protection des mineurs contre la pédopornographie en ligne*, Harmattan, 2023 p152, I. Wattier, « La lutte contre l'exploitation sexuelle des enfants et la pédopornographie et la majorité sexuelle : la consécration d'une disparité » disponible sur <https://droit.cairn.info>, consulté le 13 février 2025.



informatisées. On entend par système informatique « tout dispositif isolé⁷⁵ ou groupé⁷⁶ de dispositif interconnectés ou apparentés, assurant par lui-même ou par un ou plusieurs de ses éléments conformément à un programme, un traitement automatisé de données⁷⁷ »⁷⁸. Les systèmes informatiques font l'objet de diverses formes d'atteintes à savoir les atteintes à la confidentialité ; les atteintes à l'intégrité et les atteintes à la disponibilité.

L'article 4 de la loi de 2010 sur la cybersécurité et la cyber criminalité définit la confidentialité comme le maintien du secret des informations afin de prévenir la divulgation non autorisée d'informations aux non destinataires. Comme atteintes à la confidentialité des systèmes informatiques on peut citer l'article 68 de la loi de 2010 qui punit l'accès frauduleux ou maintien à un système informatique⁷⁹. Accéder frauduleusement à un système informatique, c'est l'action de s'introduire sans droit encore appelé piratage. Beaucoup de sociétés privées et publiques ont fait l'objet de piratage au Cameroun notamment la CNPS, Camtel, Orange money⁸⁰, Elecam etc⁸¹. L'objectif étant ici de transmettre, d'endommager, perturber le fonctionnement dudit système. L'élément moral est déterminé par le caractère frauduleux et la doctrine majoritaire s'accorde pour voir dans l'usage de cet adverbe la double exigence du dol général⁸² et du dol spécial⁸³.

Quant aux atteintes à l'intégrité des systèmes informatiques, on peut citer l'article 67 de la loi de 2010 sur la cybersécurité et la cybercriminalité qui affirme que « constitue une atteinte à

⁷⁵ En effet le dispositif isolé est défini comme un ensemble de pièces constituant un mécanisme, un appareil quelconque. L'essentiel est qu'il doit être conçu comme un ensemble constitué d'éléments matériels (unité de traitement, de mémoire, organes d'entrée- sortie et de liaisons etc.) et de composantes immatériels qui concourent à un résultat déterminé. Cet ensemble étant protégé par un dispositif de sécurité. Isolé part du fait que le dispositif n'est pas connecté à un autre système.

⁷⁶ Le dispositif groupé ou interconnecté quant à lui intègre les réseaux informatiques c'est-à-dire les systèmes informatiques peuvent être connectés au réseau en tant que point de sortie ou comme moyen de faciliter la transmission de l'information. L'interconnexion est la mise en relation d'au moins deux éléments distincts et le fonctionnement de chacune d'elle dépend de celui des autres.

⁷⁷ Le traitement automatisé des données quant à lui est défini par le sénat français comme « tout ensemble composé d'une ou plusieurs unités de traitement de mémoire, de logiciels, de données, d'organes, d'entrées- sorties et de liaisons qui concourent à un résultat déterminé, cet ensemble étant protégé par un dispositif de sécurité

⁷⁸ Voir art 4 de la loi de 2010 sur la cybersécurité et la cybercriminalité au Cameroun.

⁷⁹ Art 68 de la loi de 2010 relative sur la cybersécurité et la cybercriminalité au Cameroun

⁸⁰ Voir site orange Cameroun dans la rubrique arnaques.

⁸¹ Voir piratage des données à Elecam disponible sur <https://237actu.com>, consulté le 12 janvier 2025.

⁸² Le dol général réside dans la conscience, l'intelligence ou la volonté d'accomplir un acte illicite.

⁸³ Le dol spécial est le fait que l'accédant ait connaissance de l'absence de droit à accéder au système et en agissant ainsi il usurpe un droit qu'il n'a pas.



l'intégrité d'un réseau de communications électroniques ou d'un système d'information ..., le fait de provoquer une perturbation grave de communications électroniques d'un équipement terminal par l'introduction, la transmission, la modification, la suppression, l'altération des données ». On entend par intégrité un critère de sécurité définissant l'état d'un réseau de communications électroniques, d'un système d'information qui est devenu intact et permet de s'assurer que les ressources n'ont pas été altérées, modifiées ou détruites d'une façon intentionnelle ou accidentelle. Cette incrimination se matérialise par de multiples procédés comme le spamming⁸⁴, le mail bombing⁸⁵. Quant à l'élément moral les auteurs s'accordent pour considérer que cette infraction est un délit intentionnel.

Au sujet des atteintes à la disponibilité des systèmes informatiques, il faut le souligner la disponibilité renvoie au fait que l'état des éléments contenus dans le système doit être laissé à l'usage du maître du système, ce qui s'oppose à toute modification à son insu. C'est un critère de sécurité permettant que les ressources des réseaux de communication électroniques, des systèmes d'information soient accessibles et utilisables selon les besoins. On peut citer l'article 66a1, article 71 de la loi de 2010. L'atteinte à la disponibilité des systèmes informatiques se matérialise par une introduction frauduleuse des données dans un système informatique qui entraîne des conséquences sur le fonctionnement du service⁸⁶. Quant à l'élément moral, l'atteinte à la disponibilité des systèmes exige un double dol à savoir général⁸⁷ et spécial⁸⁸.

En outre les données informatiques⁸⁹ ne sont pas en reste et font l'objet de multiples atteintes à leur intégrité, confidentialité et disponibilité.

La confidentialité des données informatisées est garantie par l'incrimination d'interception frauduleuse des données prévue à l'article 65 alinéa1 de la loi de 2010 sur la cybercriminalité et la cybersécurité. Intercepter signifie arrêter au passage ou s'emparer de quelque chose qui était destiné à autrui. L'interception recouvre plusieurs procédés techniques tendant à prendre

⁸⁴ Le spamming consiste en l'envoi massif de courriers électroniques non sollicités, le plus souvent revêt un caractère publicitaire.

⁸⁵ Le mail bombing est une attaque par laquelle un grand nombre de courriels sont envoyés à une adresse électronique spécifique dans le but de surcharger la boîte de réception voire de provoquer une saturation du serveur de messagerie.

⁸⁶ Il faut le souligner les atteintes à l'intégrité des données et les atteintes à la disponibilité des données peuvent se chevaucher voir S. Tepi, *La cybercriminalité au Cameroun*, Harmattan, 2020, p 89.

⁸⁷ Le dol général se manifeste par le fait que l'infacteur doit avoir la conscience de porter atteinte à la disponibilité du système informatique. Il agit avec conscience au moment où il introduit les données dans le système informatique.

⁸⁸ Quant au dol spécial le délinquant recherche un certain résultat, celui d'entraver le fonctionnement du système

⁸⁹ Selon l'article 4 de la loi de 2010 sur la cybersécurité et la cybercriminalité, l'expression donnée désigne toute représentation des faits d'information ou de notion sous forme susceptible d'être traitée par un équipement terminal y compris un programme permettant à ce dernier d'exécuter une fonction.



connaissance du contenu des données à savoir l'écoute, le contrôle, la surveillance du contenu des communications⁹⁰. L'infacteur sait pertinemment qu'il s'empare des données qui ne lui sont pas destinées sachant que l'interception en question n'est pas autorisée et qu'il agit sans aucun droit⁹¹.

La protection pénale de l'intégrité des données informatisées est mise en évidence dans la loi de 2010 sur la cyber sécurité et la cybercriminalité à travers les articles 67, 68 alinéa 2 de la loi de 2010 sur la cybersécurité et la cybercriminalité. Il s'agit ici de manipulations de l'information de suite d'altération, de modification, de suppression de données contenues dans un système. Le criminel agit en connaissance de cause et a conscience qu'il endommage, efface, détériore, altère ou modifie les données.

La disponibilité des données informatisées quant à elle implique l'inaccessibilité de celles-ci, en effet l'article 66 de la loi de 2010 sur la cybersécurité et la cybercriminalité sanctionne toute perturbation ou interruption du fonctionnement d'un réseau de communication électronique en introduisant, supprimant ou rendant inaccessible les données. L'atteinte à la disponibilité du réseau de communications électroniques impacte inéluctablement à l'impénétrabilité des données. Ainsi les utilisateurs ne peuvent pas avoir accès rapide et fiable au système informatique et aussi aux données contenues dans le système.

II- l'imputation de la faute en fonction des activités exercées par les acteurs du cyber espace

Incontestablement, internet est devenu un outil favorable de communication et a même devancé la radio, la presse écrite ou la télévision. L'un des principes cardinaux de l'internet est la liberté d'expression qui y est consacrée menaçant ainsi la vie privée et autres droits individuels. Il est donc primordial de concilier liberté et responsabilité. L'utilisation de l'internet peut provoquer des dommages matériels et moraux découlant des contenus illicites et fautifs partagés⁹².

La recherche d'un responsable sur internet n'est pas chose facile⁹³. Dans ce contexte particulièrement préoccupant⁹⁴, la question se pose de savoir comment pouvons-nous trouver

⁹⁰ Voir décision de la cour d'appel de Paris en date du 17 décembre 2001 qui affirme que l'interception exige la mise en place d'un dispositif de branchement.

⁹¹ Le délit d'interception ne saurait s'appliquer si l'auteur jouit d'une certaine habilitation légale à l'exemple du juge d'instruction si les nécessités de l'information l'exigent d'utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel des données relatives au contenu des communications.

⁹² A. kchaou, la responsabilité civile et internet, thèse, Université Jean Moulin Lyon 3, 2022, p 148

⁹³ L'anonymat, le caractère transnational, la volatilité des données participent à rendre difficile de retrouver l'auteur de l'infraction et par conséquent dédommager la victime.

⁹⁴ La nouveauté de ce support est la simplicité d'accès à tous les individus et la rapidité de diffusion d'informations partout dans le monde.



un responsable pour assumer la responsabilité des préjudices commis sur internet ? La réponse à cette question est tributaire de l'activité exercée par l'acteur dans le cyber espace. En effet il convient de prendre appui sur la fonction occupée par les intervenants dans le cyberspace. Dans beaucoup de situations où la circulation d'information engendre des dommages, les critères pour juger de la responsabilité se fondent sur les rôles assumés par les différents participants à la chaîne de valorisation de l'information. La responsabilité des acteurs oscille entre neutralité et forte implication dans la commission de l'infraction. On distingue d'une part les prestataires techniques (A) qui se caractérisent par une neutralité qui aboutit à une irresponsabilité de principe ; mais celle-ci connaît des limites en cas de défaillance dans la conduite des activités desdits prestataires techniques. D'autre part, on cite les fournisseurs de contenus qui s'identifient par une forte implication dans la création du contenu illicite engageant ainsi leur responsabilité (B).

A- La neutralité des prestataires techniques

Parmi les prestataires techniques, il convient de distinguer les fournisseurs d'accès(1) et les fournisseurs d'hébergement (2). Ces intermédiaires procurent les moyens techniques de connexion au réseau. Fournissant les « tuyaux » grâce auxquels les données sont transmises⁹⁵, ils sont réputés en principe être dans l'incapacité de connaître le contenu de ce qui transite par leur réseau. Une question mérite d'être posée, à savoir quel type de responsabilité peut être engagé ? S'agira-t-il d'une responsabilité contractuelle, délictuelle ou pénale ?

Concernant la responsabilité contractuelle des intermédiaires techniques, celle-ci est évidente et ne pose pas de problème. Notons que les intermédiaires techniques fonctionnent dans le cadre de contrats proposés par eux et acceptés par les utilisateurs de leurs services. À cet égard, la responsabilité contractuelle paraît donc devoir être appliquée à ces relations contractuelles⁹⁶. Nous nous attarderons sur la responsabilité délictuelle et pénale qui trouvent leur fondement dans la mauvaise exécution des activités incombant aux intermédiaires techniques.

1- Les fournisseurs d'accès et opérateurs de communication électroniques : une irresponsabilité de principe

On les définit comme étant des personnes dont l'activité est d'offrir un accès aux services de communications électroniques. Le fournisseur d'accès offre à ses clients les ressources techniques permettant à ces derniers d'accéder aux services d'Internet. Son rôle se limite à relier

⁹⁵ J. Bossam, « Le droit pénal confronté à la diversité des intermédiaires de l'internet », *RSC*, 2013, p 295-319

⁹⁶ La responsabilité contractuelle ne fera pas l'objet de notre étude car ne soulève pas de questions.



l'internaute avec un contenu avec lequel le fournisseur n'a aucun rapport. Sa fonction est purement technique, il n'a aucun contrôle sur le contenu diffusé sur ses infrastructures. Engager une responsabilité de ce fournisseur pose donc des problèmes : sur quelle base sera engagée sa responsabilité ? N'étant pas intervenu dans le contenu litigieux diffusé⁹⁷, quelle est alors sa faute engageant sa responsabilité ? D'où une irresponsabilité de principe du fait de leur neutralité. C'est dans ce sens que l'article 40 alinéa 1 de la loi de 2010 pose le principe d'irresponsabilité délictuelle et pénale car la maîtrise du contenu fait défaut et que l'intervention de ces acteurs est neutre. Toutefois leur immunité est susceptible de disparaître dans certains cas.

Les fournisseurs d'accès à internet et les opérateurs de communication électroniques sont soumis à un principe d'exonération de responsabilité. En effet les fournisseurs d'accès à internet n'ont pas à contrôler les informations qu'ils transmettent, ni à l'obligation de rechercher des faits ou des circonstances relevant des activités illicites. Ceux-ci ont un rôle purement technique, ils ne sont pas tenus à une action positive de contrôle et d'enquête. Leur exonération de responsabilité pénale ou civile s'explique non pas en fonction du type d'opérateurs mais en considération du type d'activité exercé⁹⁸. C'est dans ce sens que l'article 40 alinéa 1 de la loi de 2010 pose le principe d'irresponsabilité délictuelle et pénale⁹⁹ car la maîtrise du contenu fait défaut et que l'intervention de ces acteurs est neutre, passive se limitant à assurer un simple transport d'informations provenant des tiers. Cette position a été illustrée par un arrêt de la Cour d'appel de Lyon du 22 juin 2000¹⁰⁰ qui a jugé que France Telecom qui assure le fonctionnement du réseau par lequel sont diffusées les informations auprès des clients n'est pas tenue d'exercer un contrôle sur le contenu des messages transmis.

Toutefois cette irresponsabilité peut disparaître si la neutralité requise pour les fournisseurs d'accès à internet fait défaut. La question de responsabilité des FAI est gouvernée par la neutralité de leur intervention dans le processus infractionnel¹⁰¹. Le régime d'exonération de

⁹⁷ E. Montero, « La responsabilité des prestataires intermédiaires de l'Internet », in *Cahiers du CRID* n°19, p.288.

⁹⁸ En effet plusieurs actions ont été intentées contre les fournisseurs d'accès à internet pour barrer la voie à la complexité du cyber espace à savoir l'anonymat des internautes qui sont difficilement identifiables sur internet et même l'inefficacité des recours contre ceux-ci du fait de leur insolvabilité en vue de pouvoir dédommager les victimes de contenus illicites sur internet. Les tribunaux ont donc décidé que les fournisseurs d'accès à internet ne se limitent qu'à un rôle purement technique, neutre ne pouvant pas conduire à une quelconque responsabilité.

⁹⁹ Il sera sans doute difficile de réunir les conditions de la responsabilité pénale et notamment de prouver l'intention ou la volonté de contribuer à la commission de l'infraction.

¹⁰⁰ L. Latapie, « La responsabilité de l'hébergeur », disponible sur <https://www.village-justice.com>, consulté le 22 septembre 2025.

¹⁰¹ J. Bossam, « Le droit pénal confronté à la diversité des intermédiaires de l'internet » *RSC* no 2, 2013, p 295-319.



responsabilité des FAI est tributaire du rôle passif ou neutre de ces derniers qui passe par un simple transport d'informations provenant des tiers. En d'autres termes les FAI doivent avoir un rôle purement technique dans la circulation de l'information, idem dans le contenu du message. Si tel n'est pas le cas ils deviennent des éditeurs de contenus. Ce principe de neutralité constitue l'alpha et l'oméga c'est-à-dire à la fois fondement de l'irresponsabilité des FAI mais aussi la limite de celle-ci. Leur immunité est susceptible de disparaître dans certains cas¹⁰².

En premier lieu lorsque le fournisseur d'accès est à l'origine de la demande de la transmission litigieuse. En second lieu lorsque le fournisseur d'accès sélectionne ou modifie les contenus faisant l'objet de la transmission. En somme les fournisseurs d'accès internet et les opérateurs de communication électroniques peuvent engager leur responsabilité en fonction de leur participation à la création du contenu illicite.

2- Le fournisseur d'hébergement : une responsabilité atténuée due à l'inaction

Tandis que le rôle du fournisseur d'accès internet se limite à assurer le transfert des données dans l'instantanéité et sans possibilité de contrôler le contenu de ce qui transite par son service, le fournisseur d'hébergement effectue une prestation durable de stockage d'informations que la domiciliation sur son serveur rend disponibles et accessibles aux personnes désireuses de les consulter¹⁰³. Le fournisseur d'hébergement assure donc le stockage des signaux, d'écrits, d'images, de sponsor de messages de toute nature fournis par les destinataires de ces services. L'article 34 alinéa 1 de la loi de 2010 sur la cybersécurité et la cybercriminalité a retenu la responsabilité de l'hébergeur dans des conditions bien précises. Néanmoins la loi n'indique pas la procédure à suivre en cas de dénonciation du contenu illicite auprès du fournisseur d'hébergement. En effet l'hébergeur peut être tenu responsable pour son inaction. En effet l'article 34 alinéa 1 de la loi de 2010 sur la cybersécurité et la cybercriminalité fait obligation au fournisseur d'hébergement de retirer le contenu illicite dès le moment qu'il a connaissance des faits. En général, les fournisseurs d'hébergement disposent de moyens techniques pour faire cesser les atteintes ou pour supprimer les contenus illicites. La responsabilité de l'hébergeur est engagée par la simple non-exécution de l'obligation de retrait¹⁰⁴. La victime du contenu illicite a la possibilité de se baser sur l'article 1382 du Code civil et partant mettre en branle la responsabilité délictuelle du fournisseur d'hébergement. À noter que la responsabilité de

¹⁰² Voir art 40 alinéa 1 de la loi de 2010 sur la cybersécurité et la cybercriminalité au Cameroun.

¹⁰³ A. kchaou, La responsabilité civile et internet, thèse, Université Jean Moulin Lyon 3, 2022, p 255.

¹⁰⁴ En effet il faut le souligner que l'hébergeur est face à un dilemme au nom de quoi et en vertu de quelle autorité doit-il juger du caractère fautif ou non de telle ou telle information ? En vertu de quelle autorité devrait-il s'ériger en juge chargé de déterminer si un contenu est ou non fautif et dommageable ?.



l'hébergeur n'est pas liée à celle de l'auteur principal. Pour être engagée, elle ne requiert pas que les conditions de la responsabilité de l'auteur principal soient réunies. Lorsque l'hébergeur et le responsable principal sont tous deux attirés en justice, la voie est naturellement ouverte à une condamnation in solidum. Par conséquent, la victime peut toujours choisir de s'adresser à l'hébergeur pour réparer le préjudice subi après l'expiration du délai, ou de s'adresser à l'auteur principal pour la totalité du préjudice. Il y a donc deux responsabilités, celle de l'utilisateur mettant un contenu illicite sur Internet, et celle de l'hébergeur n'ayant pas retiré ce contenu dans des délais jugés acceptables. La mise en cause des émetteurs de contenus litigieux sur Internet s'avère particulièrement délicate, du fait de la structure technique décentralisée d'Internet et de son caractère international. Pour cela, le recours contre l'hébergeur paraît le plus praticable. Quant à la responsabilité pénale, l'hébergeur peut être poursuivi en tant que complice¹⁰⁵. Ainsi la complicité de l'hébergeur se matérialise par la fourniture de moyens lorsque ce dernier ne réagit pas promptement à retirer le contenu illicite. L'élément moral de la complicité apparaît à travers l'inaction de l'hébergeur alors qu'il a connaissance du caractère illicite du contenu¹⁰⁶. Le raisonnement est le suivant en maintenant le lien de téléchargement actif et en conservant le fichier sur ses serveurs, l'hébergeur fournit à l'internaute en question le moyen de commettre l'infraction. L'intention coupable est la connaissance du caractère illicite du contenu suite à la dénonciation.

En outre la responsabilité de l'hébergeur peut être engagée par le fait que plusieurs indices ou circonstances laissent apparaître de tels faits ou propos, ou contenus illicites. Il s'agit du cas où l'hébergeur a un doute sur l'illicéité du contenu en tenant compte des circonstances de création celui-ci. La responsabilité des hébergeurs peut être engagée en raison des sites hébergés lorsque l'hébergeur sait à l'avance les thèmes qui y seront abordés, soit lorsque par les services qu'il propose, il est évident qu'il connaît le contenu des sites hébergés. Dans ce cas, il ne peut pas

¹⁰⁵ Ce point de vue fait l'objet de débat car certains auteurs réfutent la qualité de complice à l'hébergeur parce qu'il ne peut y avoir complicité que si l'aide ou la fourniture de moyens est soit antérieure soit concomitante à la commission de l'infraction. Concernant l'hébergeur l'aide est postérieure et l'élément moral apparaît après la dénonciation du contenu illicite, comment est-il possible de parler de complicité de l'hébergeur alors que l'infraction est déjà réalisée et que l'hébergeur ne connaît le caractère illicite du contenu qu'après dénonciation ? En fait il faut préciser que l'hébergeur peut être considéré comme complice si et seulement si il refuse de retirer le contenu illicite dénoncé par un tiers et si l'infraction en question constitue une infraction continue. En effet l'inaction du prestataire de stockage dument informé de leur perpétration en permet le prolongement. Voir E.Dreyer, *Droit de la communication*, 2^{ème} édition, LexisNexis, 2022, p58, F. Picard, « Quelle est la responsabilité des hébergeurs face aux contenus illicites », disponible sur [www, Haas avocat .com](http://www.haasavocat.com), consulté le 6 mai 2025.

¹⁰⁶ Dans l'affaire U.E.J.F. contre Costes, du 10 juillet 199749, le Tribunal de Grande Instance de Paris décide que si la responsabilité de l'hébergeur doit être engagée pénalement, elle ne le sera que sur le terrain de la complicité.



opposer un défaut de connaissance des contenus¹⁰⁷. Dans le cas où le prestataire de stockage des données a eu connaissance initialement de l'illicéité des informations stockées, sa participation matérielle est évidente et sa conscience de fournir le moyen de la diffusion des informations illicites en fait pas l'ombre d'aucun doute, il peut donc être puni comme coauteur de l'infraction¹⁰⁸.

B- L'implication constante des fournisseurs de contenus

Les fournisseurs de contenus constituent la cheville ouvrière de la création des contenus. Ils sont le pilier de la conception, de la production, la mise à jour bref de la mise à disposition des contenus. Il arrive donc que la publication des contenus sur internet soit diffamatoire, haineux etc provoquant moult dommages posant ainsi le problème de la réparation de ceux-ci. En effet la responsabilité des contenus publiés sur internet crée un casse-tête juridique où s'entremêlent professionnels et amateurs, voire simples utilisateurs d'internet. En effet celui qui met un contenu illicite sur internet afin d'élargir sa distribution pourra être attaqué pour contrefaçon ou atteinte aux droits subjectifs. Cependant avec la particularité d'internet, il est possible que l'auteur des faits ne soit pas identifiable ou alors insolvable ou enfin du fait du caractère transnational d'internet, cette personne peut se retrouver dans des pays où le système judiciaire est largement déficient. Pour mettre un terme à la précarisation de dédommagement de la victime, le législateur a mis sur pied une responsabilité pénale en cascade pour les professionnels de communication audiovisuelle, électronique et en matière de presse (1) tandis que les non professionnels restent assujettis à la responsabilité de droit commun (2).

1- Une responsabilité en cascade pour les professionnels de la communication

L'identification des éditeurs de contenu dans le cyber espace est cruciale dans le cadre des investigations judiciaires sur les réseaux numériques. Parler d'éditeurs de contenu revient de primer à abord à les identifier et présenter les règles applicables en matière de responsabilité des éditeurs de contenus. On entend par éditeur de contenu ou encore fournisseur de contenus, une personne physique ou morale qui à titre professionnel ou non, édite et met en ligne de l'information au sens le plus large du terme à destination des internautes en la publiant sur son

¹⁰⁷ Voir arrêt rendu par la cour de cassation le 8 décembre 1998 qui concerne en l'espèce un service télématique de messagerie qui initie ce raisonnement. En l'espèce le créateur d'un service télématique de messagerie dénommé « 3615 renouveau » était poursuivi suite à des diffusions de deux messages anonymes sur son forum créé dans le but d'échanger des opinions religieuses et politiques des divers mouvements de la droite chrétienne, la cour de cassation a estimé que en mettant à disposition un tel service l'hébergeur savait à l'avance les thèmes qui seront abordés et par conséquent ne pouvait pas ignorer une connaissance de leur caractère illicite des faits ou propos.

¹⁰⁸ A. de Carlo, La responsabilité de l'hébergeur internet vis-à-vis des tiers, mémoire de master, de la faculté libre de droit, d'économie et de gestion, 2008, p 98 et suivantes.



site internet¹⁰⁹. En d'autres termes l'éditeur de contenu fait paraître sous sa responsabilité des contenus dont il a la maîtrise éditoriale, la connaissance et l'initiative de leur publication¹¹⁰. Il ne faut pas confondre l'éditeur de contenus avec l'internaute ou apporteur de contenus qui fournit directement l'information. Ce dernier poste une réaction sur un forum et ne fait pas partie de la chaîne de diffusion de l'information en ligne¹¹¹. L'éditeur de contenus est astreint à l'obligation d'identification qui diffère de l'éditeur professionnel de celle de l'éditeur non professionnel.

Concernant l'éditeur professionnel l'article 37 de la loi de 2010 sur la cyber sécurité et la cybercriminalité leur impose de mettre à la disposition du public leur nom, prénom, domicile, numéro de téléphone, le numéro d'inscription au registre de commerce et du crédit mobilier, leur dénomination sociale, leur siège social s'ils sont des personnes physiques, leur inscription au RCCM, leur capital social, l'adresse de leur siège social s'il s'agit des personnes morales, le nom du directeur ou codirecteur de la publication et le cas échéant celui du responsable de la rédaction. Quant aux éditeurs non professionnels la loi leur impose de mettre à la disposition du public leur nom, leur dénomination ou la raison sociale et l'adresse du prestataire¹¹². Cette obligation d'identification vise à lever l'anonymat des véritables responsables de contenus illicites et par conséquent engager facilement leur responsabilité pénale et civile.

En matière de presse et de communication audiovisuelle, électronique, la responsabilité pénale obéit à un système dérogatoire du droit commun dit de la responsabilité en cascade ou responsabilité éditoriale. Ce régime de responsabilité est prévu par la loi de 1990 sur la communication sociale au Cameroun en son article 74 qui énumère une série de personnes successives qui peuvent être déclarées coupables. Il se caractérise par le fait que la responsabilité pénale est transmise de manière successive à différentes personnes en fonction de leur rôle dans la commission de l'infraction. La responsabilité n'est pas directement imputée à l'auteur initial de l'infraction mais à une série de personnes successives. Ce mécanisme de responsabilité se fonde sur une présomption de connaissance des contenus mis en ligne envers le directeur de publication et qui découle sur une présomption de responsabilité. Il incombe donc au directeur de publication de surveiller et de contrôler le contenu diffusé¹¹³.

¹⁰⁹ P. Assane Touré, *Le traitement de la cybercriminalité devant le juge l'exemple du Sénégal*, Harmattan, 2014, p434

¹¹⁰ *Ibid.*

¹¹¹ J Bossann « Le droit pénal confronté à la diversité des intermédiaires de l'internet » *RSC*, 2013, p 295-312.

¹¹² Voir article 38alinéa1 de la loi de 2010 relative à la cybersécurité et la cybercriminalité

¹¹³ M. Cahen « La responsabilité du directeur de la publication : même en cas d'externalisation ? » disponible sur <https://www.murielle-cahen.com>, consulté 22 septembre 2025.



On cite en premier lieu les directeurs de publication ou éditeurs ainsi que les auteurs, à défaut des personnes visées ci-dessus, les imprimeurs, les distributeurs, les directeurs des entreprises d'enregistrement ou de diffusion, et à défaut de celles-ci, les afficheurs, les colporteurs et les vendeurs à la criée. Cependant cette transposition de la responsabilité en cascade à l'environnement numérique s'avère difficile car les acteurs de l'internet sont multiples, complexes et peuvent exercer en mêmes temps plusieurs fonctions¹¹⁴ d'où l'application combinée de différents régimes de responsabilité pénale dans le cyberespace¹¹⁵ comme au Sénégal¹¹⁶ ou en France.

2- L'internaute ou l'utilisateur de services

L'internet est devenu un haut lieu de commission de délits du fait des multiples avantages qu'il procure. On peut citer à cet effet les propos diffamatoires, les contenus haineux, les *fake news*, les contenus à caractère pédophile, etc qui sont légions sur la toile.

En effet, les réseaux sociaux sont le théâtre de vifs échanges heurtant parfois la vie privée d'autres utilisateurs. L'émergence de l'internet a multiplié, voire augmenté le nombre des délits et le législateur s'est donc précipité pour règlementer cet espace de communication et d'échanges en faisant un espace de droit par l'implémentation d'un régime de responsabilité.

Parler de la responsabilité de l'utilisateur de services revient à identifier le cadre dans lequel l'infraction a été perpétrée. Cette préoccupation se pose avec acuité notamment avec l'avènement des services du *web 2.0*¹¹⁷ qui permettent à l'internaute de passer du rôle passif de récepteur d'informations à celui plus actif de créateur de contenus¹¹⁸. Contrairement au *web 1.0* qui offrait des pages statiques, conçues, mises en ligne et modifiées par des initiés, le *web 2.0* donne la possibilité à tous de créer et de diffuser des contenus. Cette nouvelle donne pose la question des responsabilités des acteurs du web. Il apparaît donc opportun de sérier le rôle joué dans le cyber espace et le statut des acteurs de l'internet pour déterminer les responsabilités liés aux contenus illicites postés. Plusieurs cas de figure se présentent à savoir l'hypothèse où

¹¹⁴ La tentation est grande d'assimiler par exemple l'hébergeur à un directeur de publication responsable des contenus qu'il héberge dans son serveur,

¹¹⁵ P. Auvert « L'application du droit de presse au réseau internet », *JCP*, 1999, p 262. Il est évident que la responsabilité éditoriale s'applique à la fonction d'édition de contenus et la responsabilité de droit commun s'applique pour toutes les autres fonctions exercées dans le cyberespace notamment les fonctions d'intermédiaire technique.

¹¹⁶ P. Asana, *op cit*, p148 et ss.

¹¹⁷ Z. karambiri, « Les responsabilités liées aux contenus postés dans les blogs », *revue de droit des technologies de l'information*, no 36, 2009, p 29.

¹¹⁸ *Ibid*.



l'internaute met à la disposition du public des contenus illicites, le cas des forums de discussion et le cas des sites web et des blogs.

L'explosion de l'internet a mis l'internaute dans le statut de producteur d'informations. Ce changement de paradigme dans la création de contenus constitue un renouveau de la liberté d'expression qui augure de nombreux risques d'abus dans l'exercice de cette liberté. Cette nouvelle donne pose nécessairement la question des responsabilités des acteurs du cyberspace. La question est de savoir à quel titre l'internaute individuel devra assumer sa responsabilité du fait des contenus ? A ce titre la responsabilité de droit commun sera mise en jeu. Il sera responsable pleinement des contenus qu'il poste par sa propre initiative¹¹⁹.

S'agissant des forums de discussion, en l'absence de lois spécifiques règlementant les forums de discussion, la jurisprudence française a institué deux hypothèses qui peuvent se présenter : soit que le forum de discussion fait l'objet d'une modération a priori. Dans ce cas le directeur de publication a eu connaissance du contenu du message illicite avant sa communication au public d'où la condition de la fixation préalable¹²⁰. Par conséquent la responsabilité en cascade ou éditoriale sera mise en jeu. Par contre si le message litigieux n'a pas fait l'objet d'une fixation préalable à sa communication au public seul l'auteur dudit message sera tenu seul responsable¹²¹. En effet la modération¹²² permet à l'exploitant du forum de discussion de prendre connaissance du contenu du message avant sa communication au public d'où l'existence d'une fixation préalable. Celle-ci conduit inexorablement à l'applicabilité de la responsabilité en cascade.

S'agissant des sites web, la jurisprudence répressive française admet plus facilement la mise en œuvre de la fixation préalable. Un arrêt de la cour de cassation française du 10 mai 2005¹²³ a

¹¹⁹ Voir à ce propos les articles 43, 74 alinéa1, 74 alinéa8 de la loi de 2010 relative à la cybersécurité et la cybercriminalité, l'art 22 de la charte de protection des enfants en ligne au Cameroun.

¹²⁰ Le tribunal de grande instance de Paris a fait une stricte application de l'article 93-3 de la loi du 29 juillet 1982 en relaxant le concepteur et producteur d'un site accompagné d'un forum de discussion poursuivi en raison des propos diffamatoires et injurieux contenus dans des messages échangés entre les internautes. Il a été jugé qu'il ne pouvait être poursuivi en qualité de directeur de publication que si le message incriminé avait fait l'objet d'une fixation préalable à sa diffusion publique.

¹²¹ Voir dans ce sens, CA Paris, 28 janvier 2009, Dr. Pénal, 2009, no 26, Obs Mouysset.

¹²² La modération se traduit par l'utilisation d'outils spécifiques mettant en œuvre une lutte contre les contenus illicites. On cite par exemple l'utilisation d'outils de filtrage encouragée par les pouvoirs publics, la mise en place volontaire de filtrage automatique et d'outils d'implication du public par le biais d'outils de signalement, ici le public devient actif dans la lutte contre les contenus illicites et enfin l'utilisation d'outils contractuels d'autorégulation par les réseaux sociaux (il est fréquent de trouver dans les conditions générales d'utilisation des réseaux sociaux une liste exposant les types de contenus qu'il est interdit de publier sur la plateforme) Voir M. Saingra, la régulation des contenus illicites sur les réseaux sociaux, mémoire de master, université de Montpellier, 2020, p 45 et ss.

¹²³ Cass.crim 10 mai 2005, bull, crim,2005, no 144



jugé que les propos injurieux diffusés sur le site internet d'un syndicat à l'encontre d'un fonctionnaire public avaient nécessairement fait l'objet d'une fixation préalable avant leur communication au public. La haute juridiction a donc engagé une responsabilité éditoriale à l'encontre du secrétaire général du syndicat en tant que représentant légal dudit syndicat et partant ayant la qualité du directeur de publication du site.

S'agissant des blogs, le régime de la responsabilité en cascade est susceptible de s'appliquer au blogueur lorsque ce dernier surveille le contenu des messages avant que ceux-ci ne soient mis en ligne. L'éditeur du blog pourrait donc être considéré comme un directeur de publication car en contrôlant le message, en le diffusant, le blogueur en revendique le contenu¹²⁴. Toutefois, en tant qu'éditeur de blog, le blogueur peut être tenu responsable des commentaires ajoutés par les autres internautes. Ils sont donc tenus de mettre en place une politique stricte de retrait du contenu mis sur leur blog par des tiers afin que leur responsabilité civile ne soit pas engagée¹²⁵.

Cependant, dans les espaces interactifs, c'est-à-dire des messages envoyés par un internaute à un service de communication en public en ligne et mis par ce service à la disposition du public dans un espace de contributions personnelles, la responsabilité éditoriale ne peut pas être retenue car l'animateur du blog ou du forum n'a pas effectivement eu connaissance du message avant sa publication ou sa mise en ligne. Néanmoins, il peut être tenu responsable si dès le moment où il a eu connaissance, il n'a pas agi promptement pour retirer ce message. Par conséquent la responsabilité pénale des directeurs de publication s'apparente à celle des hébergeurs d'où la teneur de la loi du 12 juin 2009 dite loi Hadopi.

¹²⁴ Trib correctionnel, Arras, 20 janvier 2006 voir [http //foruminternet.org/specialisteillejuridique](http://foruminternet.org/specialisteillejuridique).

¹²⁵ Face au non retrait des commentaires incitant à la haine et à la violence contre un groupe de personnes, un blogueur français a été poursuivi devant la cour d'appel de Nîmes. Cette dernière a énoncé que le blogueur a pris l'initiative de créer un service de communication en public et a laissé les commentaires illicites encore visibles. Il a donc été reconnu coupable en qualité de producteur d'un site en ligne et tenu responsable du fait d'autrui. Pour engager sa responsabilité du fait d'autrui, la cour s'est fondée sur le fait que le blogueur a rendu public son blog personnel, il a donc autorisé des personnes à publier des commentaires. De ce fait, Il aurait l'obligation de contrôler ces derniers. . De plus, le blogueur avait toléré des commentaires haineux et s'est abstenu en les laissant sans rétractation six semaines après leur publication. Pour cela, sa responsabilité du fait de ces commentaires a été engagée. Il faut relever qu'en l'espèce, le blogueur est une personnalité politique. Selon la cour, cette qualité attire des commentaires ayant une teneur politique, par essence polémique. Ce blogueur est donc obligé de faire preuve de vigilance concernant les commentaires publiés et de renforcer la surveillance sur son blog. La qualité du blogueur influence sa fonction professionnelle et, par conséquent, sa responsabilité. . Le blogueur peut également exercer un contrôle a priori.



En conclusion

Publier un contenu illicite dans un pays peut en quelques secondes provoquer des dommages dans le monde entier. Bien plus la possibilité qu'offre internet de donner à chacun de publier sur ce réseau augmente significativement le nombre d'auteurs potentiels de dommages et par ricochet le nombre de victimes d'où la nécessité d'appréhender l'internet par le droit de la responsabilité. En effet parler de la responsabilité des acteurs dans le cyberspace est tributaire de l'exigence d'un contenu illicite d'une part et d'autre part du rôle exercé par les différents intervenants dans le cyberspace. Mais il faut le souligner le numérique est un espace complexe où de multiples acteurs aux fonctions diverses interagissent et s'influencent mutuellement créant un environnement dynamique et en constante évolution. Le cyber espace attire de nombreux personnes de mauvaise moralité à cause des avantages qu'il procure à savoir ses caractères transnational, volatil, et anonyme. Mais il est naïf de s'imaginer que ces comportements illégaux et dommageables commis dans le cyberspace resteront impunis. Le droit des Etats a entamé un assainissement en déterminant les responsabilités résultant d'une information à caractère délictueux et la faute reste donc le fondement de la responsabilité dans le cyberspace mais demeure limitée. Il importe d'aller plus loin et de se donner des moyens de mettre sur pied une normativité appropriée à cet environnement virtuel. Les paradigmes étatistes qui président à toutes les réflexions sur la normativité en général et le droit de la responsabilité en particulier paraissent insuffisants pour rendre compte de la globalité de cet espace. Il est plus jamais essentiel d'une part d'identifier les valeurs et préceptes proclamés dans les textes internationaux qui vont présider à la répartition des responsabilités dans les environnements électroniques. D'autre part tous les acteurs du cyberspace doivent déterminer de manière proactive des principes de répartition de responsabilités équitables qui ne sauraient être en marge des principes universels reconnus sans toutefois attendre que les règles viennent de l'Etat et enfin l'insignifiance des frontières entre les différentes branches du droit d'où de nouvelles pistes permettant d'appréhender et d'agir sur la normativité d'internet.