International Multilingual Journal of Science and Technology (IMJST)
ISSN: 2528-9810
Vol. 6 Issue 10, October - 2021

La Protection Des Données Personnelles Du Cyberconsommateur Par Le Droit Des Technologies De L'information Et De La Communication De La Cemac

MAJILO Linda Judith
mofolaure@yahoo.fr

RÉSUMÉ

La multiplication des activités électroniques au sein des États membres de la CEMAC a favorisé l'institution d'une autorité de régulation dont l'une des plus prestigieuses missions est la protection des droits des consommateurs. En effet, Les questions relatives à la protection des données personnelles à l'ère du numérique occupent désormais une place importante dans le droit des activités économiques au sein de la CEMAC. L'environnement juridique des affaires de la CEMAC s'est alors acclimaté pour encadrer les réalités juridiques liées aux activités économiques dématérialisées. Si la volonté du législateur communautaire de faire des techniques de communication électroniques un socle du développement est visible à travers l'institution d'un marché numérique dans lequel prime la protection des droits et la liberté des consommateurs, il faut encore relever sa hardiesse à travailler pour la sauvegarde de l'économie numérique par des règles qui protègent les données personnelles des consommateurs des services électroniques. Ces règles protectrices ont été définies par le législateur dans le but d'amoindrir les risques que l'informatisation pouvait faire courir à la vie privée et aux données à caractère personnel du consommateur. Ainsi, un ensemble de principes devant encadrer le traitement des données à caractère personnel a été consacré. Ces principes confèrent au consommateur certains droits. Le droit de la CEMAC concernant les technologies de l'information et de la communication témoigne ainsi sa volonté de protéger les usagers des technologies du numérique.

Mots clés : protection, consommateur, données personnelles, CEMAC.

ABSTRACT

The proliferation of electronic activities within CEMAC member states has encouraged the establishment of a regulatory authority, one of whose most prestigious missions is the protection of consumer rights. Indeed, questions relating to the protection of personal data in the digital age now occupy an important place in the law of economic activities within CEMAC. CEMAC's legal business environment was then acclimatized to frame the legal realities related to dematerialized economic activities. We still need to raise the freedom to work hard to safeguard the digital economy through rules that protect the personal data of consumers of electronic services. These protective rules have been defined by respecting the personal character of the consumer. Thus, a set of principles that should govern the processing of personal data has been established. These principles give the consumer certain rights. CEMAC's law relating to information and communication technologies thus testifies to its desire to protect users of digital technologies.

Keywords: protection, consumer, personal data, CEMAC.

La révolution [1] du numérique a entraîné une explosion des activités réalisées à partir des terminaux et des équipements électroniques. De nombreux investisseurs offrent des services électroniques accessibles en permanence et sous plusieurs formes, que ce soit pour satisfaire la demande ou la susciter[2]. Cette transaction appelée

[1] Les activités numériques se traduisent par la forte consommation des équipements électroniques et informatiques, mais aussi par l'accroissement, au cours des dernières années, des activités électroniques et l'expérimentation de diverses formes de commerce électronique dans l'espace de la CEMAC. On assiste alors à la forme : (*business-to-business e-commerce* ou B2B), il est question des entreprises physiques qui s'offrent des services à travers des plateformes numériques (banque électronique (*e-banking*), paiement électronique (*e-payment*)) ; (*business-to-consumer e-commerce* ou B2C), qui traduit le commerce électronique de détail entre commerçants et consommateurs. Ici, le commerçant offre des biens et des services au consommateur à partir d'un site Web professionnel ; (*consumer-to-consumer e-commerce* ou C2C), est le commerce électronique consommateur à consommateur en ligne, qui permet au consommateur, à partir d'une page Web de vendre des biens personnels sans avoir l'intention de s'installer définitivement comme un cybercommerçant.

[2] Isabelle de Lamberterie, *Le contrat électronique*, conférence organisée par le Programme international de coopération scientifique (CRDP/CECOJI), Montréal, 19 décembre 2003, p. 3, [En ligne], [www.lex-electronica.org/files/sites/103/9-2_lamberterie_2.pdf] (2

commerce électronique a bouleversé le monde. En effet, la doctrine affirme que le commerce électronique se caractérise par trois «i »[3]. À cet effet, on a en premier l'immatérialité, qui signifie que les échanges sur Internet sont très souvent dématérialisés. En deuxième lieu, l'interactivité, qui permet au consommateur de naviguer sur le site web à l'aide des liens hypertexte. Troisièmement, l'internationalité marque le fait que, le commerce électronique est sans frontières physique. Autrement dit, le consommateur peut acquérir un bien ou un service dans tous les quatre coins du monde sans déplacement physique. En effet, le commerce électronique, dont le mécanisme évacue la notion de distance dans l'exercice des activités économiques, représente un enjeu économique important[4]. Grace à son insensibilité à l'égard des frontières physique pour l'accomplissement des actes commerciales et aux avantages que revêt le commerce électronique, « *le trafic d'Internet double tous les cent jours*»[5] et fait de lui un outil très porteur du développement dans l'espace CEMAC [6] . Le consommateur peut communiquer avec des entreprises dans l'autre bout du monde, consulter leur site web, voir la marchandise et examiner ses caractéristiques comme dans un supermarché réel.

Toutefois, le développement du commerce électronique bien qu'ayant des avantages indéniables, n'est pas sans risque pour le cyberconsommateur. En effet, chaque connexion laisse forcément des traces, ce qui rend le consommateur transparent [7] . Le développement du commerce électronique permet de tracer un profil de plus en plus complet de chaque consommateur [8] . En fait, le consommateur lors d'achats d'article en ligne, communique ses données à caractère personnel. Ces données acquièrent très souvent « une valeur marchande » [9] . Les données personnelles sont alors devenues des marchandises dont les professionnels assurent la vente[10]. Source de convoitise, les données personnelles constituent une ressource précieuse pour les entreprises [11] . Ainsi, tandis que le volume de données à caractère personnel explose avec le développement du numérique, la dignité humaine tend à s'affaiblir. Cet affaiblissement est dû aux mauvais traitements et aux nombreux détournements que les professionnels infligent à ces données. La notion de donnée à caractère personnel est née de l'évolution des techniques d'information et de communication et notamment du numérique. Elle est spécialement « *développée en réponse à la menace que pouvaient représenter les technologies de l'information pour les libertés individuelles et sur la vie privée* »[12] surtout que, le succès du commerce électronique dépend, aussi, de la confiance qu'ont les consommateurs vis-à-vis de la protection accordée aux données à caractère personnel qu'ils transmettent» [13] . D'après l'article 2 de la Directive CEMAC [14] , les données personnelles sont **«** *Toute information relative à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs facteurs propres à son identité physique, physiologique, mentale, économique, culturelle ou sociale ».*

mai 2019). Pour cette dernière, les acteurs désignent « non seulement les fournisseurs, prestataires ou vendeurs mais aussi les destinataires de ces offres de fournitures ou de prestations ou les acheteurs potentiels, sans oublier ce que nous appellerons les "tiers" aux contrats qui sont concernés par l'opération contractuelle à un titre ou à un autre. »

[3] HUET (J.), « La problématique juridique du commerce électronique », Acte de colloque annuel de l'association droit et commerce, R.J.C.,2001, p.19.

[4] Voir D. Fenouillet« Commerce électronique et droit de la consommation : une rencontre incertaine », *R.D.C.* 2004.955.

[5] BOCHURBERG (L.), Internet et commerce électronique : Site web. Contrats. Responsabilités. Contentieux, Paris, DELMAS, 2ème édition, 2001, p. 11.

[6] L'utilisation du numérique dans les échanges commerciaux dans l'espace communautaire a permis d'accroître les activités économiques et l'amélioration du flux économique des revenus au profit des administrations publiques. La multiplication des activités électroniques grâce à Internet permettra également de relever le niveau de l'économie des États membres de la CEMAC.

[7] POUJOL (N.-M.), « Les libertés de l'individu face aux nouvelles technologies de l'information », Cahier français, n°296, 2000, p. 60.

[8] DELEURY (E.) et GOUBAU (D.), Le droit des personnes physiques, Québec-Canada, Les éditions Yvon Blais Inc, 1994, p. 149.

[9] TROUSSEAU (M.-P.F.) et HAAS (G.), *Internet et protection des données personnelles*, Paris, Litec, 2000, p. 111.

[10] GARNIER (F.), « Solutions concrètes pour un business éthique sur Internet », p.2, Disponible sur : http://www.droit-technologie.org.

[11] LAIME (M.), « Allons-nous devoir vendre nos données personnelles », disponible sur : http://www.uzine.net.

[12] V. KOUAHOU (Y.L.), *La mise en œuvre de la société de l'information au Cameroun : enjeux et perspectives au regard de l'évolution française et européenne*, Thèse de doctorat en droit privé, option nouvelles technologies et droit, Université de Montpellier 1, 2010, n° 1258. Cité par TCHABO SONTANG (H. M.), « Le droit à la vie privée à l'ère des TIC au Cameroun », *La Revue des droits de l'homme* [En ligne], 17 | 2020, mis en ligne le 13 janvier 2020, consulté le 10 juin 2021. URL : http://journals.openedition.org/revdh/7975 ; DOI : https://doi.org/10.4000/revdh.7975.

[13] LOUVEAUX (S.), « Le commerce électronique et la vie privée », in. Le droit des affaires en évolution, BRUYLANT, BRUXELLES, 1999, p. 183.

[14] Art. 2 de la Directive Harmonisation de la Protection des Consommateurs au sein de la CEMAC.

Compte tenu de leur sensibilité, les données à caractère personnel sont soumises à de strictes exigences[15], Ainsi, pour mieux concevoir le traitement des données à caractère personnel, il nous semble judicieux d'élucider dans un premier temps la notion équivoque de données personnelles (I) et d'envisager dans un second temps la protection efficace des données : de la collecte au traitement (II).

I : LA NOTION ÉQUIVOQUE DE DONNÉES PERSONNELLES

Toute donnée connectée produite par une activité humaine peut servir de base à la reconstitution d'informations plus précises et préjudiciables à l'intimité de la personne. Ainsi, la protection est envisagée selon la typologie des données (A). Cependant, les obstacles à la protection des données personnelles (B) ne sont pas minimes.

A- LA TYPOLOGIE DES DONNÉES

Les données sont définies à l'article 4 (41) de la loi camerounaise relative à la Cybersécurité et à la Cybercriminalité comme une « *représentation de faits, d'informations ou de notions sous une forme susceptible d'être traitée par un équipement terminal, y compris un programme permettant à ce dernier d'exécuter une fonction* »[16]. On peut distinguer deux grands types de données personnelles : les données d'identification (1) et les données délicates (2).

1. Les données d'identification

On peut scinder les données d'indentification en deux sous-groupes : on peut avoir d'une part, les données d'identification directe et d'autre part les données d'identification indirecte. L'mage, fixe ou animée, constitue une donnée nominative[17]. Il s'agit également des données biologiques » [18] et des données alphanumériques. Il est en effet question de toute application mémorisant les noms et prénoms les éléments tels le nom, la voix[19], l'image ou même l'adresse professionnelle d'une personne physique sauf lorsque les informations ne portent atteinte ni directement, ni indirectement à l'identité humaine, aux droits de l'homme, à la vie privée ou aux libertés individuelles ou publiques[20]. Dans son ordonnance de référé du 6 avril 2018, le TGI de Paris a observé que les noms, prénom et coordonnées professionnelles d'un chirurgien-dentiste restaient des données personnelles. D'après le juge, « *la circonstance que de telles données soient relatives, comme en l'espèce, à l'activité professionnelle de la personne en question est donc sans incidence sur cette qualification, dès lors qu'elle est désignée ou rendue identifiable, la notion n'étant pas restreinte, contrairement à ce que soutient la défenderesse, aux seules informations relatives à la vie privée* »[21]. Ce principe conduit à exclure du champ de la loi le « traitement automatisé du fichier des ouvrages d'une bibliothèque [22]. Les données directes à caractère personnel sont donc toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image relative à une personne physique identifiée ou identifiable directement par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique. Il s'agit concrètement de « toute information se rapportant à une personne physique identifiée ou identifiable » directement ou indirectement, notamment par un identifiant, « tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité´ physique, physiologique, génétique, psychique, économique, culturelle ou sociale ». Il est question de toutes les informations quelle que soit leur origine ou leur forme et qui permettent directement ou indirectement d'identifier une personne physique ou la rendent identifiable, à l'exception des informations liées à la vie publique ou considérées comme telle par la loi». Cette approche des données personnelles est justifiée par l'évolution technologique où tous les faits et gestes, notamment les achats en ligne, les clics, la consultation de sites internet ou même l'envoi de message ou l'utilisation des réseaux sociaux ou du GPS demeurent des pistes potentielles d'identification de l'utilisateur par les entreprises[23]. En dehors des informations nominatives qui permettent d'identifier directement un individu, d'autres informations baptisées données d'identification indirecte permettent l'identification indirecte d'un individu. Le concept de données à caractère personnel ne se résout donc pas aux informations nominatives. Le

[15] Le professionnel a des obligations : que ce soit au moment même de la transaction où il a l'obligation de sécuriser les données et d'informer le client qui doit consentir de façon expresse à leur conservation, ou au-delà de la transaction où il doit observer les principes liés à leur durée de conservation.

[16] Cf. Art. 4 (41) de la loi N° 2010/012 du 21 décembre 2010 relative à la Cybersécurité et à la Cybercriminalité au Cameroun.

[17] Ainsi, l'image d'une personne enregistrée par une caméra constitue une donnée à caractère personnel dans la mesure où elle permet d'identifier la personne concernée. Voir dans ce sens, l'article 2, sous a), de la directive 95/46, dans la mesure où elle permet d'identifier la personne concernée.

[18] COULIBALY(J.-C.), Cours de droit civil des personnes, 2015. [En ligne] www.ivoire-juriste.com (consulté le 10 septembre 2018).

[19] Logiquement, pour la CEDH, la voix est bien une donnée à caractère personnel. cf. CEDH, 25 décembre 2001, n° 44787/98, *P.G. et J.H. c. Royaume-Uni*, § 59.

[20] FRAYSSINET (J.), Informatique, fichiers et libertés, Litec, 1992, n° 104.

[21] Cf. TGI de Paris, ordonnance de référé du 6 avril 2018, Monsieur X. / Google France et Google LLC.

[22] FRAYSSINET (J.) *op. cit.*

[23] CHALTIEL (F.), « La protection des données personnelles. À propos de l'entrée en vigueur du règlement général de protection des données », LPA, n°111, 4 juin 2018, p. 6.

législateur communautaire renchérie cette position lorsqu'il définit la donnée à caractère personnel comme :*« toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique*[24]. La protection des données à caractère personnel apparait alors comme « *le socle de la protection des personnes dans un univers complexe et numérique* »[25].

Le numéro d'identification est aussi une donnée d'identification indirecte. Le numéro d'identification des étudiants est exclusivement utilisé pour leur immatriculation auprès des organismes de sécurité sociale et des mutuelles agissant comme centres payeurs de la scolarité. Ainsi, imposer étudiants un numéro d'identification personnel, parait légitime car, il aurait pour objectif de permettre aux technologies de l'information d'avoir un accès rapide aux profils et préférences humains, tels les modes d'apprentissage, les capacités physiques, cognitives et les préférences culturelles[26]. La biométrie est également une donnée d'identification indirecte. Elle permet l'identification et l'authentification d'un individu à travers ses caractéristiques biologiques. La biométrie, encore qualifiée de données génétiques[27] telles l'iris, la voix, ou l'empreinte digitale présente une importance extrême vue son objet et nécessite une protection de plus en plus sérieuse avec l'émergence de l'informatique et du commerce électronique. Les empreintes digitales constituent des données indirectement nominatives. Le recours à ce procédé d'identification de la personne, par biométrie[28], doit être légitime. Il doit également tenir compte de la finalité et de la proportionnalité[29]. Il est admis que : « *la prise de l'empreinte digitale est, dans l'inconscient collectif, ressentie comme une intrusion particulièrement indiscrète dans l'intimité de la personne* »[30]. Les pratiques intrusives mettent à mal le développement du commerce électronique. Or le commerce électronique apparait comme le meilleur moyen devant permettre aux pays membres de la CEMAC à accéder au développement. Pour y arriver, un climat de confiance doit pouvoir Reigner. En effet, la loi doit garantir aux consommateurs une meilleure protection de leur données à caractère personnel, qu'il s'agisse des données classiques ou des données délicates.

2. Les données délicates

L'un des défis majeurs que devra relever la CEMAC dans les années à venir sera de protéger au mieux les données personnelles que recueillent les professionnels, en vue d'éviter que des tiers ne se les procurent par des moyens illégaux, en exploitant par exemple les failles informatiques ou logistiques relatives à la sécurité de ces données. Certaines données sont en effet extrêmement délicates. Il s'agit des données dites sensibles. Ces données sont celles qui révèlent l'origine raciale ou éthique, les opinions politiques, les convictions religieuses ou philosophique, l'appartenance syndicale ainsi que les données relatives à la vie sexuelle. Il est question des données plus intimes. C'est pourquoi elles nécessitent un régime plus protecteur. Dans cette catégorie, figurent également les données relatives à la santé[31]ou des données médicales[32], qui doivent tout particulièrement être protégées, et ce d'autant plus qu'elles transitent par un nombre important de réseaux et de systèmes informatiques. On peut cependant sécuriser les fichiers informatiques par une technique de cryptage [33] qui pourrait garantir leur confidentialité. Aussi, le professionnel est tenu d'une obligation de précaution et d'information, il doit fournir des dispositifs de contrôle parental, il doit utiliser un dispositif permettant d'éviter l'accès des mineurs à des contenus illicites. À cet effet, le droit pénal camerounais puni d'un emprisonnement allant d'un an à cinq ans et d'une amende de 20 000 à 1000 000 celui qui excite, favorise ou facilite la débauche ou la corruption d'une personne mineure de vingt et un ans[34]. Ces peines étant doublées lorsque la personne mineure est âgée de moins de seize ans. L'article 27

[24] Cf. art. 1 Projet de Directive CEMAC relative à la protection des données à caractère personnel.

[25] Cf. FALQUE-PIERROTIN (I.), préface de DEBET (A.), MASSOT (J.) et METALLINOS (N.) (Dir), *Informatique et libertés, La protection des données à caractère personnel en droit français et européen*, Lextenso éditions, coll. Les intégrales, 2015. Cité par TCHABO SONTANG (H. M.), « Le droit à la vie privée à l'ère des TIC au Cameroun », *La Revue des droits de l'homme* [En ligne], 17 | 2020, mis en ligne le 13 janvier 2020, consulté le 10 juin 2021. URL : http://journals.openedition.org/revdh/7975 ; DOI : https://doi.org/10.4000/revdh.7975.

[26] MANDARD (S.), Internet va-t-il démanteler l'école?, Le Monde Intéractif, 26 septembre 2001, p. I.

[27] MALAUZAT (M.-I.), Le droit face aux pouvoirs des données génétiques, Paris, Presses Universitaires D'Aix-Marseille.2000, p. 191.

[28] Guerrier (Cl.), Protection des données personnelles et applications biométriques en Europe : CCE, juill.-août 2003, Chron. 19

[29] CNIL, Délibération n° 93-073 du 7 septembre 1993 : CNIL, 14° rapport 1993, Dc. fr. 1994, p. 125

[30] V. CNIL, Voix, image et protection des données personnelles, Doc. fr. 1996136infra n° 108, p. 22.

[31] de BROUWER (F.), « Protection des données à caractère personnel : un nouveau cadre légal Belge », *R.D.A.I.* [31] TAVERNIER (S.-V.), « La C.N.I.L et la protection des données médicales nominatives », *Gaz.Pal*.,1999,, n°2,1999, p.181.
2ème sem., p. 1153.

[33] D'après l'article 4. (28), le cryptage est définit comme : l' « *utilisation de codes ou signaux non usuels permettant la conservation des informations à transmettre en des signaux incompréhensibles par les tiers* ».

[34] Cf. Art. 344 du Code pénal camerounais.

de la loi camerounaise sur la cybercriminalité, renchéri en indiquant que les professionnels dont l'activité est d'offrir un accès à des systèmes d'information sont tenues d'informer les parents du danger encouru dans l'utilisation des systèmes d'information non sécurisés notamment pour les particuliers ; de la nécessité d'installer des dispositifs de contrôle parental ; des risques particuliers de violation de sécurité, notamment la famille générique des virus et de l'existence de moyens techniques permettant de restreindre l'accès au mineurs et de leur proposer au moins l'un de ces moyens, notamment l'utilisation des systèmes d'exploitation les plus récents [35] . Les correspondances et images érotiques, pornographiques, les réseaux pédophiles sur Internet dans le but de protéger l'intégrité physique ou morale des mineurs[36]. Internet étant un « lieu public », la diffusion de messages à destination d'un public non déterminé pourrait favoriser la corruption[37] ou les propositions sexuelles faites à un mineur[38]. Malgré toutes ces exigences, des obstacles persistent.

B- LES OBSTACLES À LA PROTECTION DES DONNÉES PERSONNELLES

Les risques liés aux procédés utilisés (1) et les risques dus à l'ignorance du consommateur (2) constituent des obstacles à la protection des données à caractère personnel.

1. Les risques liés aux procédés utilisés

Le législateur a encadré un certain nombre de procédés tels que : les cookies, le spamming et la commercialisation des données qui ne sont pas sans conséquence sur les données personnelles du consommateur dans la mesure où ils peuvent dans certains cas supprimer la confidentialité des échanges et ouvrir la voie à la cybercriminalité.

Les cookies [39] sont des « petits programmes espions» [40] . Les cookies sont une technique de collecte sur le web, ce sont de petits fichiers émis par le serveur consulté et enregistrés sur le disque dur du consommateur, qui permettent au responsable du serveur d'enregistrer les précédentes consultations, par ce consommateur, de son site. Ces fichiers dénommés cookies s'installent sur le disque dur du consommateur à l'occasion de la consultation de certains sites. Ils permettent de tracer le consommateur ; endroits où il navigue sur l'écran, ils permettent d'avoir des informations sur ses habitudes de navigation. Les données de connexion de chaque consommateur permettent à son fournisseur d'accès de suivre pas à pas son activité sur Internet, qu'il s'agisse des sites visités, de la date et de l'heure de ces visites, des documents téléchargés, de la participation à un espace de discussion, ou du courrier électronique reçu et envoyé. Ces données peuvent être conservées par le fournisseur d'accès et sont souvent utilisées par ce dernier pour procéder à une analyse du comportement de ses clients. Par ailleurs, le commerce électronique ne peut véritablement se dérouler sans l'usage des cookies car, il est légitime que le consommateur en ligne puisse accéder à tous les services commerciaux du site malgré son refus à l'installation de cookies[41].Toutefois, du fait de leur caractère sensible à l'égard des consommateurs, le législateur a encadré l'usage des cookies ainsi que le contenu des publicités, c'est-à-dire les produits et services pouvant faire ou non l'objet d'une publicité par voie électronique. En effet, les cookies ne sont pas toujours réfutables, ils ont aussi des avantages indéniables. Les cookies sont générés pour faciliter la navigation sur internet, l'accès aux sites échapper à la répétition des informations.

Les cookies ne doivent pas être utilisés à l'insu du consommateur. La collecte n'est loyale que si elle est faite avec l'accord [42] du consommateur. Le consommateur doit donner un consentement éclairé, qu'il peut retirer à tout moment[43]. Toutefois, le recueil du consentement préalable à l'installation d'un cookie n'est pas obligatoire si les cookies facilitent la communication par voie électronique ou s'ils sont nécessaires à la fourniture d'un service de communication en ligne.

Le législateur CEMAC dispose d'un arsenal juridique suffisant pour interdire certaines pratiques contestables. Ces règles sont contenues dans plusieurs textes d'origine communautaire [44] nationale[45]. Elles forment un dispositif essentiellement

[35] Art. 27 de la loi N° 2010/012 du 21 décembre 2010 relative à la Cybersécurité et à la Cybercriminalité au Cameroun.
[36] CRAMIER (P), Prévention, répression des infractions sexuelles et protection des mineurs, légipresse, Mars 1999, n° 159, p. 25
[37] LASSERRE CAPDEVILLE (J.), « Infractions commises à l'encontre de mineurs par l'intermédiaire d'Internet », Gaz. Pal., n° 250, 6 septembre 2012, p. 12.
[38]CA Colmar, 29 mai 2012, n°12/00737, Min. pub. c/ M. S.
[39] PANSIER (F-J.) et JEZ (E.), *L'initiation à l'Internet juridique*, Paris, Litec, 1998, p.72.
[40] PANSIER (F-J.) et JEZ (E.), *L'initiation à l'Internet juridique*, Paris, Litec, 1998, p.72.
[41] Les cookies ne sont pas à confondre avec les spams et les spywares.
[42] Cf. art. 7 (1), de la Loi-type relative à la protection des données personnelles.
[43] Art. 7, de la Directive n° 07/08-UEAC-133-CM-18 fixant le Cadre juridique de la protection des droits des utilisateurs de réseaux et de services de communications électroniques.
[44] Cf. Directive n° 07/08-UEAC-133-CM-18 Fixant le Cadre juridique de la protection des droits des utilisateurs de réseaux et de services de communications électroniques ; Directive n° 09/08-UEAC-133-CM-18 harmonisant les régimes juridiques des activités électroniques dans les États membres de la CEMAC.
[45] On peut avoir comme exemple : la loi n° 2010-012 du 21 décembre 2010 relative à la cybersécurité et la cybercriminalité au Cameroun ; la loi n° 2010-013 du 21

guidé par les principes de droit communautaire de la confidentialité des données relatives au trafic des communications effectuées au moyen des réseaux de communications électroniques[46]. Il s'agit des règles garantissant l'inviolabilité et le secret des communications électroniques. C'est l'interdiction faite aux tiers d'usurper de l'identité d'autrui[47]. Ainsi, l'utilisation des cookies est légitime et utile si le consommateur a été régulièrement informé et s'il a eu la possibilité de les refuser ou de les accepter. il doit alors être en mesure de faire jouer ses droits et en particulier son droit d'opposition. Ces données doivent également être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs. Une collecte des données à l'insu des intéressés et sans déclaration de traitement peut être qualifié de moyens frauduleux[48], déloyaux, ou illicites. Une telle pratique excepté les cas légaux et réglementaires[49] s'oppose naturellement au principe de collecte loyale des données. Cette pratique est punie[50]. La cybercriminalité est également réprimée.

La cybercriminalité peut être appréhendée comme tout comportement illégal ou contraire à l'éthique ou non autorisé, qui concerne un traitement automatique de données et/ou de transmissions de données[51]. C'est l'utilisation frauduleuse de l'informatique[52]. Elle doit enduire tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent. Le cyberespace[53] peut être un instrument actif qui favorise la commission de l'infraction. En effet, Internet a fait fleurir une multitude d'infractions liées à la circulation de l'information telle que les délits de presse[54] et de diffamation, la violation du droit d'auteur[55], les violations de vie privée et du secret des correspondances[56]. Pourtant, la loi interdit toute intrusion[57] dans la vie privée[58] du consommateur. L'émergence des réseaux informatiques transnationaux a conduit à la naissance des pirates informatiques ou des hackers. Elle a permis aux délinquants[59] d'entrer dans le champ d'incrimination des infractions liées au cyberespace. Ces délinquants qualifiés «hacker» ou « pirate » sont des personnes qui tentent de s'introduire dans les systèmes informatiques, en particulier pour obtenir des renseignements secrets ou confidentiels qui y sont placés. Il s'agit de tous ceux qui utilisent les TIC à des fins contraires à la loi. C'est à dire un criminel informatique qui exploite les failles dans une procédure d'accès pour casser un système informatique, qui viole l'intégrité de ce système en dérobant, altérant ou détruisant l'information, ou qui copie frauduleusement des logiciels». En effet, un détournement issu de la publicité électronique est particulièrement redoutable pour collecter des données personnelles, en parfaite illégalité, et susceptibles de causer un préjudice financier consistant pour le consommateur. Il s'agit en fait du phishing ou hameçonnage. Cette pratique de cybercriminalité qui consiste à envoyer une multitude de mails aux consommateurs d'une banque par exemple dans lesquels ces derniers sont invités à renseigner des données personnelles, notamment de nature bancaire, sous prétexte d'une mise à jour de celles-ci, ou suite à une prétendue perte des données. De plus, le consommateur n'est pas à l'abri d'un vol, d'une perte de sa carte bancaire. Cela pourrait permettre une utilisation frauduleuse de son moyen de paiement sur Internet. Le cyberespace, à l'image des récents scandales pédophiles en Europe est devenu le domaine privilégié de la délinquance. Cette cybercriminalité est multiforme et amène donc à envisager la protection des données personnelles

décembre 2010 (modifiée par la loi 2015-06 du 20 avril 2015) régissant les communications électroniques au Cameroun et de la L. n° 2010-021 du 21 décembre 2010 régissant le commerce électronique au Cameroun.

[46] Cf. Art. 3, Directive n° 07/08-UEAC-133-CM-18 fixant le Cadre juridique de la protection des droits des utilisateurs de réseaux et de services de communications électroniques.

[47] Ainsi, d'après l'alinéa 2 de l'article 48 de la loi n° 2010-012 précitée, « *l'émission des messages électroniques en usurpant l'identité d'autrui est interdite* ».

[48] Cour d'appel de Paris, Pôle 4 – Ch. 11, arrêt du 15 septembre 2017, M. X. / Weezevent.

[49] Art. 51, loi n° 2010-013 régissant les communications électroniques.

[50] C.Cass, ch. Crim 3 nov 1987.

[51] ALTERMAN (H.) et A. BLOCH (A.), La Fraude Informatique Paris, *Gaz. Palais*, 3 sep. 1988 p. 530.

[52] V. Les articles 3 à 33 de la Loi-type portant sur la lutte contre la cybercriminalité dans les Etats Membres de la CEEAC/CEMAC.

[53] JORDON (T.), *Cyberpower. The Culture and Policies of Cyberspace and the Internet* Londres, Routledge, 1999, pp. 20-58.

[54] JASSERME (S.), *La Diffamation sur Internet : Aspects Spécifiques au Réseau.* Mémoire de DESS, Université Paris II), 2001.

[55] TGI Paris, 14 août 1996,D., 1996, p. 490, note GAUTHIER (P.-Y.).

[56] TGI Privas, 3 septembre 1997, Expertises, n° 213, p. 79 note FRAYSSINET (J.).

[57] Cf. Art. 4, (51) qui définit l'intrusion par intérêt comme : l' « *accès intentionnel et sans droit dans un réseau de communications électroniques ou dans un système d'information, dans le but soit de nuire soit de tirer un bénéfice économique, financier, industriel, sécuritaire ou de souveraineté* »

[58] L'alinéa 2 de l'article 48 de la loi n° 2010-012 précitée, dispose à cet effet que : « *l'émission des messages électroniques en usurpant l'identité d'autrui est interdite* ».

[59] Le mot « délinquant » renvoie étymologiquement au terme latin «delinquere» signifiant commettre une faute. En droit pénal, le délinquant est défini comme l'auteur d'une infraction pénale, qui peut faire l'objet d'une poursuite de ce chef. le délinquant informatique serait la personne qui commet un délit informatique. Voir dans ce sens, LUCAS (A.), Le Droit de l'Informatique (PUF), [1987] n° 413.

dans plusieurs domaines notamment le paiement électronique, la télésanté et le commerce électronique. Toutefois, le recourt à la cryptologie[60] ou le téléchargement de logiciels ayant vocation à protéger la vie privée, tels que les firewalls devrait être une réponse efficace pour protéger la confidentialité des échanges et de la vie privée. La cybercriminalité n'est pas la seule menace à la protection des données à caractère personnel, il existe également des risques liés à l'ignorance du consommateur.

2. Les risques dus à l'ignorance du consommateur

L'encadrement juridique des activités économiques dans la CEMAC s'articule progressivement avec les avancées technologiques. Ayant perçu le risque que l'informatisation de la société pouvait faire courir à la vie privée et plus spécifiquement aux données à caractère personnel, et conscient de ce que l'usage commercial des moyens électroniques au préjudice des droits du consommateur peut entamer la confiance des clients et conduire à des pertes économiques importantes, un ensemble de principes[61] devant encadrer le traitement des données à caractère personnel a été défini. Il s'agit spécialement des principes d'accès de rectification et d'opposition de finalité, de loyauté et de transparence, de pertinence ou de proportionnalité, de sécurité et de confidentialité [62], de la limitation de la durée du traitement. Toutefois, très peu sont les consommateurs qui ont connaissance de l'existence de ces droits à leurs profits. Ainsi, la méconnaissance de leurs droits par les consommateurs peut sans doute découler du défaut d'information. Pareillement, la méconnaissance de la technologie constitue également une menace à la protection des données du cyberconsommateur.

La méconnaissance des droits par les consommateurs et la difficulté de leur mise en œuvre restent une grande menace à la protection des données à caractère personnelles. Les carences de l'État dans son rôle de protection des libertés peuvent également être à l'origine de la méconnaissance de ces droits. En effet, l'information des consommateurs a essentiellement pour objectif de développer une prise de conscience des risques qui pèsent sur leur vie privée. L'État entant que garant des libertés individuelles devrait mettre en place un certain nombre de procédés d'information, tant à destination des citoyens que des pouvoirs publics. Ces informations doivent permettre au consommateur de prendre conscience des menaces importantes qui pèsent sur sa vie privée. Ces informations ne concernent pas seulement les consommateurs, mais aussi les entreprises qui collectent et exploitent des données personnelles. Afin que ceux-ci prennent conscience des atteintes aux libertés publiques, l'État ne doit pas se limiter à consacrer des normes comme le droit d'accès, le droit d'opposition. Il doit s'assurer de la connaissance de ces droits par le biais des médias. Ainsi, par le biais de ces derniers les pouvoirs publics pourront alerter les consommateurs dans le but de favoriser une prise de conscience des menaces pesant sur leur vie privée, et leur donner les moyens de s'y opposer, en exigeant tout naturellement que la réglementation en vigueur soit respectée.

Dans la pratique, malgré les recommandations de la loi[63], plusieurs sites collectent les données à l'insu des consommateurs, ils n'indiquent pas comment le droit d'accès aux informations nominatives peut être exercé et n'indiquent pas clairement l'adresse où l'on peut joindre le responsable de la mise en œuvre des traitements informatiques liés à ces sites. Très souvent, le consommateur ignore que la loi dispose d'un certain nombre de droits à son profit. Certains sites s'efforcent à informer les consommateurs sur le fait que leurs données personnelles peuvent être amenées à être vendues, mais ne les signalent pas qu'il est possible de s'y opposer, et même quand ils indiquent que le consommateur a un droit d'opposition, ils ne dévoilent pas très souvent les conditions de cession de ces données et ne donnent aucune information sur l'usage qui est fait des cookies[64]. Par ailleurs, lorsque ces droits sont connus par certains consommateurs qui peuvent en bénéficier, ces derniers tombent sur la difficulté de leur mise en œuvre. Aussi, la mise en œuvre de ces droits est, en pratique, extrêmement délicate, ceci est dû à la complexité des procédures, et les consommateurs qui connaissent le régime juridique applicable risquent de se heurter à la complexité des procédures et des techniques utilisées.

La complexité des techniques est aussi au cœur des atteintes au respect de la vie privée et plus particulièrement aux données à caractère personnel. Les programmations des logiciels et les constituants physiques des ordinateurs sont trop complexes pour que le consommateur puisse comprendre le fonctionnement. Dans la pratique, en profitant du fait que les consommateurs ignorent [65] tout du

[60] Il s'agit d'une politique prenant convenablement en compte les conflits d'intérêts entre les besoins des consommateurs et la nécessité de pouvoir prévenir et réprimer les actes criminels.

[61] Il est question des Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel.

[62] Cf. art. 22 et 23, 15 et 14 de la Loi-type relative à la protection des données personnelles.

[63] Art. 24 de la Loi n° 2010/012 du 21 décembre 2010 relative à la Cyber sécurité et à la Cybercriminalité au Cameroun.

[64] Aucun site ne précise si ces cookies permettent par la suite de créer des fichiers contenant des informations nominatives sur les personnes qui se connectent à ces sites.

[65] On peut illustrer comme exemple l'affaire société Intel. En effet, la société Intel, premier fabricant au monde de microprocesseurs, avait installé des numéros

fonctionnement de ces procédés, les professionnels rusés les utilisent pour dérober les données personnelles du consommateur. Ces procédés contiennent parfois des logiciels espions [66] qui envoient, à l'insu des consommateurs, des informations sur leur utilisation du logiciel à leur concepteur, lui permettant d'optimiser les bases de données commerciales et d'établir des profils. Il existe pourtant des logiciels spécialisés pouvant permettre aux consommateurs de protéger leurs données personnelles face aux traitements invisibles. Ces logiciels nommés « firewalls »[67] sont des logiciels qui filtrent les données qui quittent de l'ordinateur du consommateur vers les sites avec lesquels il est en relation. Ainsi, lorsqu'un consommateur est connecté à un réseau, ses données partent de son ordinateur vers le réseau et les professionnels peuvent en effet surveiller leurs clients grâce à ces données de connexion. Conscient de ce que, le professionnel utilise très souvent, abusivement les données à caractère personnel du consommateur, le législateur a encadré la collecte des données. À cet égard, la collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est interdite. Ainsi, toute collecte de données effectuée à l'insu du consommateur est illégale. Aussi, la loi prévoit un droit d'opposition au profit de ce dernier. De plus, certains logiciels de navigation[68] ont été modifiés afin de permettre au consommateur en ligne de refuser *a priori* l'enregistrement de tout cookie depuis les pages web de certains sites[69].

Il ne devrait pas être possible d'inscrire une information sur le disque dur d'un consommateur sans qu'il en soit averti, sans qu'il puisse s'y opposer et sans qu'il puisse en connaître la teneur de manière intelligible [70]. En effet, effacer les cookies reste la solution la plus indiqué pour la protection des données à caractère personnel du consommateur. D'autres solutions peuvent se montrer encore plus raisonnables au consommateur, comme l'anonymisation des données. Toutefois, comment arriver à une telle protection si le consommateur n'a ni la maitrise de la technique, ni la connaissance de ce qui est fait de ses données ? On devrait alors faire appel aux pouvoirs publics et aux associations de défense de la vie privée. En effet, L'information des pouvoirs publics est le plus souvent menée au moyen de pétitions. Quant aux actions entreprises par les associations de défense de la vie privée, on pourrait suivre l'exemple des Etats-Unis, où les associations de protection de la vie privée travaillent en collaboration avec les pouvoirs publics, formulent des propositions de réglementation, et sont admises à plaider devant les tribunaux, en leur nom propre, selon le procédé de la class action. Ces informations pourront aussi découler des études universitaires, des colloques et des medias ayant pour objectifs d'une part, de signaler les atteintes commises à l'encontre de la vie privée des personnes, et, d'autre part, de donner un certain nombre de conseils pratiques à destination des usagers des systèmes de communication, plus particulièrement les consommateurs, en vue de les aider à échapper au fichage organisé par les professionnels. Il semble que ces mesures puissent aboutir à une protection efficace des données.

II : LA PROTECTION EFFICACE DES DONNÉES : DE LA COLLECTE AU TRAITEMENT

L'utilisation de l'internet est génératrice de traces invisibles ou visibles, phénomène dont les consommateurs ont plus ou moins conscience. Ce repérage continue lors de tout accès à un site. Ainsi, toute navigation génère une collecte considérable de données à caractère personnel. Il importe donc d'attirer l'attention des consommateurs sur leur sensibilité. Ainsi, vu leur caractère sensible, la collecte des données personnelles (A) et le traitement des données personnelles (B) doivent s'effectuer dans un cadre bien règlementé.

A- LA COLLECTE DES DONNÉES PERSONNELLES

Les entreprises commerciales profitent très souvent de l'absence de frontière physique qui est l'une des caractéristiques du commerce électronique, pour créer un paradis de données[71]. À cet égard, plusieurs types de collectes (1) à partir des sites Web permettent à ces entreprises de diversifier et de multiplier leur clientèle dans l'espace communautaire voire même à l'échelle mondial. Cependant, les conditions de collecte des données (2) doivent être respectées.

1. Les types de collecte

Le traçage électronique s'effectue avec les données résultant de l'utilisation des protocoles de communication permettant la communication entre ordinateurs sur l'internet. Le consommateur, en navigant, laisse indubitablement des traces telles que son adresse IP, la marque du navigateur, son identité d'abonné, l'heure de début et de fin de connexion, les sites visités. Ces traces permettent au professionnel de suivre le consommateur lors de tout accès à un site. Ce traçage se fait au moyen de cookies qui

d'identification sur les processeurs Pentium III qui ont été commercialisés en 1998 et 1999. Lorsque les consommateurs se connectaient à Internet, ce processeur transmettaient, à leur insu, des informations à Intel, telles que les dates de leurs connexions au réseau, les sites visités, le numéro d'identification ayant pour objet de permettre un classement des données ainsi collectées.

[66] Il s'agit des logiciels espions spyware ou espiogiciel.

[67] Signifie murs de feu.

[68] On peut illustrer comme exemple : Internet Explorer et Netscape.

[69] Il s'agit le plus souvent des sites de messagerie à distance, qui sont les sites les plus visités.

[70] V. Rapport "Internet et les réseaux numériques", p.11.

[71] LUCAS (A.), J.DEVEZE (J.), et FRAYSSINET (J.), *Droit de l'informatique et de l'Internet*, Paris, P.U.F., p. 14.

permettent une collecte considérable de données personnelles du consommateur. Cette collecte peut être faite sur deux formes : la collecte directe et la collecte indirecte.

La collecte directe est celle qui s'effectue directement auprès du consommateur. Qu'il s'agisse des informations recueillies par voie de questionnaire, des applications en milieu scolaire et des applications de recherche scientifique, ou des forums de discussion, En effet, en communiquant des informations à l'occasion des réponses aux questionnaires en ligne par exemple, les participants laissent des traces, les traitements « invisibles » permettent de manière très efficace, d'en collecter d'autres et même à leur insu. De même, les opinions exprimées par les internautes, à l'occasion de leur participation à des forums, peuvent être collectées. Le plus souvent, communiquer des données personnelles ouvre l'accès à de nombreux logiciels ou de services gratuits sur Internet. En contrepartie, les prestataires de services se donnent le droit de les utiliser à d'autres fins en détournant de ce fait leur finalité. Lors des forums de discussion par exemple, les adresses électroniques des participants peuvent à l'aide de logiciels spécialisés, être téléchargées vers une base de données commerciale. Cette base de données qui pourra être utilisée à des fins commerciales permettra au professionnel de bâtir une liste de clients potentiels, qui seront ensuite sollicités par l'envoi de messages électroniques vers leurs adresses. Cette intrusion lui permettra de connaître l'opinion de chacun sur tel ou tel produit. Ces téléchargements qui s'effectuent en général à l'insu des personnes concernées constituent un détournement de finalité dans la mesure où, dans le cas d'espèce, les participants ont pour objectif de participer à des débats, et non d'alimenter des bases de données commerciales. C'est pourquoi la loi recommande que les internautes soient avertis par les responsables des risques de captation des données et fait de l'anonymat un moyen efficace.

La collecte indirecte des données peut être considérée comme celle où les données qui ne sont pas recueillie immédiatement auprès de la personne concernée. La collecte indirecte des données, qui ne se fait pas directement auprès des consommateurs pose le problème de l'information de ces derniers notamment lorsqu'une entreprise achète des données personnelles du cyberconsommateur auprès d'une autre, pour faire la prospection commerciale. En matière de collecte indirecte, l'information est examinée dans les hypothèses d'extension de finalité et se consume, en général, par des obligations très strictes d'information. En effet, deux méthodes de collecte indirecte soulèvent des difficultés particulières: l'extraction de fichiers par extension de finalité et le traçage électronique. C'est-à-dire le principe de finalité.

Le principe de finalité constitue une des pierres angulaires des dispositifs de protection des données personnelles. À cet effet, les données à caractère personnel faisant l'objet d'un traitement automatisé doivent être enregistrées pour des finalités déterminées et légitimes et ne doivent pas être utilisées de manière incompatible avec ces finalités. Ainsi, lorsque le responsable envisage transférer ou vendre un fichier comportant des données à caractère personnel, il doit nécessairement informer le consommateur, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois. Autrement dit, le responsable du traitement ne doit procurer les mêmes informations que si ces données avaient été directement collectées auprès du consommateur.

Par extension de finalité, on peut entendre le prolongement de la finalité du fichier de base. Ces autorisations s'accompagnent de l'exigence de garanties supplémentaires. Il a été par exemple admis que : si le responsable du traitement a l'intention d'effectuer, un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été obtenues, il doit préalablement donner à la personne concernée des informations au sujet de cette autre finalité [72]. En principe, les données à caractère personnel sont collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités. Néanmoins, un traitement ultérieur de données à des fins est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus à cet effet : il s'agit en effet des dispositions relatives à la durée de conservation des données, lesquelles ne peuvent être conservées au-delà de la durée initialement prévue.

2. Les conditions de collecte des données

La collecte loyale des données à caractère personnel est soumise à l'obligation préalable d'information et au recueil du consentement. Le droit à l'information est le droit que possède le cyberconsommateur d'obtenir du cybercommerçant des informations satisfaisantes et pertinentes concernant l'utilisation de ses données personnelles. L'article 12 de la Loi-type CEEAC consacre le droit à l'information et le contenu de celui-ci. À cet égard, le professionnel doit informer au préalable le consommateur sur la nature des données concernée par le traitement ; les finalités du traitement des données [73] ; le caractère obligatoire ou facultatif de leur réponse , les conséquences du défaut de réponse ce qui lui permet de décider de répondre ou non en toute connaissance de cause, le nom de la personne physique ou morale bénéficiaire des données, ou de celui qui dispose du droit d'accès et

[72] Art. 14 § 4 RGPD.

[73] Lorsque les données sont collectées pour l'exécution d'un contrat et pour des opérations de prospection, le responsable du traitement doit indiquer clairement ces deux finalités.

son domicile, le nom et prénom du responsable du traitement ou sa dénomination sociale et le cas échéant, son représentant et son domicile, leur droit d'accès aux données les concernant, leur droit de revenir, à tout moment, sur l'acceptation du traitement ; leur droit de s'opposer au traitement de leur donnée ; la durée de conservation des données ; une description sommaire des mesures mises en œuvre pour garantir la sécurité des données[74] ; le pays vers lequel le responsable du traitement entend, le cas échéant, transférer lesdits données. Le professionnel doit en outre informer le consommateur *du danger encouru dans l'utilisation des systèmes d'information non sécurisés notamment pour les particuliers ; de la nécessité d'installer des dispositifs de contrôle parental ; des risques particuliers de violations de sécurité, notamment la famille générique des virus ; de l'existence de moyens techniques permettant de restreindre l'accès à certains services et de leur proposer au moins l'un de ces moyens, notamment l'utilisation des systèmes d'exploitation les plus récents, les outils antivirus et contre les logiciels espions et trompeurs, l'activation des pare-feux personnels, de systèmes de détection d'intrusions et l'activation des mises à jour automatiques*[75]. Ainsi, l'exigence d'une information complète de la personne concernée assure la transparence des transactions. Cette information englobe les droits des personnes concernées à savoir, le droit d'accès, le droit de revenir sur l'acceptation du traitement et le droit d'opposition. L'information doit porter sur l'existence de procédé de collecte automatique de données ainsi que les mesures de sécurité garantissant l'authenticité du site, l'intégrité et la confidentialité [76] des informations transmises sur le réseau. Dès lors, le professionnel doit informer au préalable le consommateur par n'importe quel moyen laissant une trace écrite. Ainsi, la notification peut s'effectuer par lettre recommandé avec accusé de réception ou par n'importe quel moyen laissant une trace écrite. En pratique, les responsables du traitement utilisent des procédés techniques pour informer le consommateur. Ce dernier peut cliquer sur la fenêtre « données personnelles» et voir s'afficher à l'écran la politique du responsable des traitements dans la protection des données à caractère personnel. Cette fenêtre doit apparaître soit dans la page d'accueil, soit au début du document électronique pour que l'information soit facilement accessible à l'utilisateur. Le consommateur doit être informé au moment même de la collecte des informations, au plus tard lors de l'enregistrement. De plus, le consommateur doit être informé des finalités pour lesquelles ses données seront utilisées. Il en est de même si le professionnel qui traite ces données envisage de les transmettre à des tiers. Le but de l'octroi d'un droit d'information est donc d'assurer la transparence lors de la collecte des données et de permettre aux personnes concernées d'exprimer leur opposition ou leur consentement.

Le consentement suppose que toute personne connaissant l'utilisation possible de ses données, consente effectivement à cette utilisation. Le consentement est « *toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel accepte que ses données à caractère personnel fassent l'objet d'un traitement* »[77]. Ainsi, les données à caractère personnel ne peuvent être traitées que si le consommateur « *a donné son consentement explicite écrit, que ce soit sur support papier, support électronique ou tout autre support équivalent* »[78]. Le consentement est le socle de la protection des données à caractère personnel Le défaut de consentement ne devrait pas permettre l'utilisation des données personnelles. Le consentement est alors présenté comme la pierre angulaire du procédé de traitement des données des personnes. «Il devrait être aussi simple de retirer son consentement que de le donner» [79]. Autrement dit, le consommateur a également le droit de révoquer son consentement. C'est dire que le consentement peut être retiré à tout moment et sans frais[80] par le consommateur.

La place le consentement est au cœur du droit au respect des données à caractère personnel, son rôle aujourd'hui, ne doit pas être surestimé. Le Consentement doit être suffisamment éclairé ce qui suppose qu'au préalable, le consommateur doit avoir été informé. Cette information devant lui permettre de savoir à quoi serviront les données et quels types de traitements seront réalisés. Il doit être obtenu de façon directe et loyale. Le professionnel doit concevoir un formulaire du genre « j'accepte » ou « j'autorise » pour faciliter l'opération. Le consentement est perçu comme l'élément clé de la protection des données,

[74] Cette information permettra à la personne concernée d'évaluer si ses données sont en toute sécurité.

[75] L'article 27 consacre le droit à l'information. Il dispose à cet effet que : « *Les personnes morales dont l'activité est d'offrir un accès à des systèmes d'information sont tenues d'informer les usagers* ».

[76] La confidentialité des communications acheminées à travers les réseaux de communications électroniques et les systèmes d'information y compris les données relatives au trafic, est assurée par les opérateurs et exploitants des réseaux de communications électroniques et des systèmes d'information.

[77] Cf. Art. 1er pt. 5 de la Loi-type relative à la protection des données personnelles.

[78] Cf. Art. 6, al. 1 (a) de la Loi-type relative à la protection des données personnelles.

[79] Parlement européen, Commission des libertés civiles, de la justice et des affaires intérieures, Projet de rapport sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), 16 janvier 2013.

[80] Cf. Art. 6 al. 1 (a) de la Loi-type relative à la protection des données personnelles.

puisqu'il s'agit du meilleur moyen pour que les consommateurs puissent contrôler les activités de traitement de leurs données. Il doit être exprès ce qui signifie qu'il doit résulter d'un acte positif. Le consentement doit être suffisamment clair surtout lorsqu'il s'agit des données sensibles. Toutefois, la réalité témoigne que la demande de consentement est peu respectée. En effet, plusieurs sites Web utilisent des cookies et seulement, quelques un de ses sites en informent les visiteurs. Il s'ajoute à tout cela les modalités d'information. L'information doit être fournie d'une façon pratique et efficace. Or, ce n'est pas toujours le cas dans la pratique. En effet, l'obligation d'information et l'exigence du consentement paraissent être des obligations gênantes pour le domaine du commerce électronique y compris sur Internet [81] car, on remarque que la demande de consentement et l'obligation d'information sont pour le professionnel, des obligations lourdes, coûteuses et complexes à mettre en œuvre surtout lorsqu'il s'agit du traitement des données personnelles.

B- LE TRAITEMENT DES DONNÉES PERSONNELLES

Le cyberespace permet au professionnel de créer un paradis de données [82]. Ainsi, les fichiers [83] que professionnel construit pour ses potentiels clients constitue un traitement[84]. Le traitement des données personnelles peut être considéré comme toutes les opérations réalisées d'une façon automatisée ou manuelle par une personne physique ou morale, et qui ont pour but notamment la collecte, l'enregistrement, l'organisation, la conservation, la modification, l'utilisation, l'exploitation, l'expédition, la distribution, la diffusion ou la destruction ou la consultation des données personnelles, ainsi que toutes les opérations relatives à l'exploitation de bases des données, des index, des répertoires, des fichiers ou l'interconnexion. La loi sur la protection des données à caractère personnel tend à assurer une transparence en matière de traitement des données à caractère personnel. Elle confère au cyberconsommateur des droits permettant de vérifier ce qu'il advient de ses données personnelles. Il est alors question d'étudier dans un premier temps les droits du consommateur (1) et dans un second temps les commandements de la protection des données personnelles (2).

1. LES DROITS DU CONSOMMATEUR

Si la volonté du législateur communautaire de faire des techniques de communications électroniques[85] un socle du développement est perceptible à travers l'institution législative d'un marché numérique dans lequel la garantie des droits et la liberté des activités sont assurées, il faut encore relever sa hardiesse à travailler pour la sauvegarde de l'économie numérique par des règles qui protègent les consommateurs des services électroniques. Ces règles protectrices ont été définit par le législateur dans le but d'amoindrir les risques que l'informatisation pouvait faire courir aux données à caractère personnel du consommateur. Ainsi, un ensemble de principes[86] devant encadrer le traitement des données à caractère personnel a été consacré. Ces principes confèrent au consommateur certains droits : il s'agit du droit d'accès et de communication, du droit de rectification et d'opposition.

Le droit d'accès est un droit exercé par la personne concernée, ses héritiers ou son tuteur. C'est le droit de consulter toutes ses données à caractère personnel, le droit de les corriger, compléter, rectifier, mettre à jour, modifier, clarifier ou effacer lorsqu'elles s'avèrent inexactes, équivoques, ou que leur traitement est prohibé. Ainsi, tout consommateur a le droit d'obtenir du détenteur du fichier des informations sur le but, la base juridique, les catégories de données personnelles recueillies, l'identité des personnes ayant participé à la constitution du fichier et celle des destinataires des données. Le droit d'accès suppose également le droit d'obtenir une copie des données dans une langue claire et conforme au contenu des enregistrements, et sous une forme intelligible lorsqu'elles sont traitées à l'aide de procédés automatisés. Le consommateur, ses héritiers ou son tuteur selon le cas, peuvent demander par écrit ou par n'importe quel moyen laissant trace écrite l'obtention de copie des données à caractère personnel. Toutefois, le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique. En cas de

[81] LUCAS (A.), J.DEVEZE et FRAYSSINET (J.), *Droit de l'informatique et de l'Internet*, Paris, P.U.F., 1994, p.136.

[82] LUCAS (A.), J.DEVEZE (J.), et FRAYSSINET (J.), *Droit de l'informatique et de l'Internet*, Paris, P.U.F., p. 14.

[83] Un fichier est définit par l'article 6 de la loi 2004 comme étant « *Ensemble de D.C.P. structuré etregroupé susceptible d'être consulté selon des critères déterminés et permettant d'identifier une personne déterminée* ».

[84] GUINCHARD (S.), M. HARICHAUX (M.) de TOURDONNET (R.), *Internet pour le droit : connexion-recherche-* droit, Paris, 2ème éd., MONTCHRESTIEN, E.J.A., 2001, p.176. , p. 170

[85] Les communications électroniques sont définies à l'article premier du Règlement no 21/08-UEAC-133-CM-18 du 19 décembre 2008 relatif à l'harmonisation des réglementations et des politiques de régulation des communications électroniques au sein des États membres de la CEMAC (ci-après « Règlement no 21/08-UEAC-133-CM-18 ») comme les « émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électronique ».

[86] Cf. Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, Adoptés le 14 décembre 1990 par l'Assemblée générale des Nations Unies dans sa résolution 45-95 du 14 décembre 1990.

contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées[87]. Dans la pratique, le droit d'accès aux données personnelles reste largement ignoré ce qui peut en partie expliquer sa faible mise en œuvre et son efficacité pratique limitée. Cependant, le consommateur ne peut préalablement renoncer au droit d'accès car, il constitue la pierre angulaire de la protection des données» [88] dans la mesure où il permet une maîtrise du consommateur sur ses données. Ainsi, tout consommateur doit pouvoir obtenir communication de ses données qui doivent être conforme au contenue des enregistrements[89]. Le droit d'accès s'exerce sur toutes les données à caractère personnel. Toutefois, des limites à ce droit sont envisageables. Tel est le cas lorsque le traitement des données à caractère personnel est effectué à des fins scientifiques et à condition que ces données n'affectent la vie privée du consommateur que d'une façon limitée. Une autre limite est possible si le motif recherché par la limitation du droit d'accès est la protection du consommateur lui-même ou des tiers. Cependant, il est à craindre que ces exceptions soient utilisées pour empêcher le droit d'accès.

Le droit d'opposition renforce la maîtrise du consommateur sur ses données à caractère personnel. En pratique, le consommateur exprime son opposition soit en marquant la case à cocher soit en décochant cette case[90]. Le consommateur a le droit de s'opposer, pour des motifs légitimes, à ce que des données le concernant soient enregistrées dans un fichier informatique, sauf si celui-ci présente un caractère obligatoire. Le droit d'opposition suppose que le consommateur sache au moins qu'un fichier contenant les données personnelles existe à son sujet et qu'il peut connaître l'identité de celui qui le tient. Autrement dit, pour pouvoir s'opposer à ce que ses données soient traitées, il faut au préalable que le consommateur ait été informé lors du traitement en cours. Le droit d'opposition est donc le complément du droit à l'information. Ainsi, le consommateur, ses héritiers ou son tuteur, a le droit de s'opposer à tout moment au traitement des données à caractère personnel le concernant pour des raisons légitimes[91] sauf dans le cas où le traitement est prévu par la loi ou exigé par la nature de l'obligation. Toutefois, l'exercice du droit d'opposition est subordonné à l'existence de raisons légitimes. De plus, le consentement du consommateur n'est pas requis lorsque la collecte implique des efforts disproportionnés ou s'il s'avère manifestement que la collecte n'affecte pas ses intérêts légitimes, ou lorsque la personne concernée est décédée. On peut néanmoins admettre que la collecte des données, en elle-même, n'affecte pas vraiment la dignité du consommateur. Ce sont, en fait, les opérations postérieures à la collecte qui sont dangereuses.

Le droit d'accès ne trouve toute son efficacité que si la personne concernée pourrait rectifier ses données. En effet, le droit de rectification permet au consommateur, ses héritiers ou son tuteur, de demander au professionnel de rectifier les données à caractère personnel le concernant, les compléter, les modifier, les clarifier, les mettre à jour, les effacer lorsqu'elles s'avèrent erronées, incomplètes, ou ambiguës, ou demander leur destruction lorsque leur collecte ou leur utilisation a été effectuée en violation de la loi. Ainsi, le responsable du traitement et le sous-traitant doivent corriger, compléter, modifier, ou mettre à jour les fichiers dont ils disposent, et effacer les données à caractère personnel de ces fichiers s'ils ont eu connaissance de l'inexactitude ou de l'insuffisance de ces données. Ces droits ont pour objectif de protéger le consommateur contre des immixtions dans sa vie privée. Le droit de rectification permet au consommateur d'assurer une maîtrise complète sur ses données personnelles. Mais, ce droit est assorti d'une multitude d'inconvénients. En effet, le droit de rectification se présente comme une consécration législative sans débouché. Ceci est dû à la difficulté lié à sa mise en œuvre puisqu'il constitue la boucle des droits du consommateur. Autrement dit, le droit de rectification est dépendant de l'exercice des autres droits[92]. Ainsi, si l'un d'entre eux fait défaut, la rectification des données devient impossible. Quant au droit d'opposition, il va à l'encontre des promoteurs du commerce électronique et reste malaisément applicable pour les sites dont la législation ne consacre pas en raison du caractère transfrontalier du commerce électronique[93]. Afin de protéger la dignité du consommateur, le législateur a établi plusieurs commandements devant assurer la protection des données personnelles.

2. Les commandements de la protection des données personnelles

La nécessité de posséder des clients potentiels, et de connaître leurs comportements, conduit très souvent le professionnel à collecter des données personnelles. Ces atteintes au droit au respect de la

[87] Cf. Art.39 II de la loi française Informatique et Liberté tel que modifiée par la loi de 6 août 2004.
[88] MARTIN (D.), « La directive 95/46/CE (protection des données) et sa transposition en droit français », Gaz.Pal., 1998, p.608.
[89] GUINCHARD (S.), HARICHAUX (M.) et de TOURDONNET (R.), Internet pour le droit : connexion-recherche- droit, Paris, 2ème éd., MONTCHRESTIEN, E.J.A.,2001, p.176.
[90] LUCAS (A), DEVEZE (J.), FRAYSSINET (J.), *Droit de l'informatique et de l'Internet*, Paris, P.U.F., 1994 p.117.
[91] Les raisons légitimes signifient que ces raisons ne doivent pas être contraires à la loi et aux bonnes mœurs.
[92] En effet, le consommateur ne pourrait rectifier ses données s'il n'est informé de leurs existences. Il ne pourrait non plus rectifier s'il n'a le droit d'accès à ces données ou s'il n'a droit de s'y opposer.
[93] LUCAS (A), DEVEZE (J.), FRAYSSINET (J.), *op.cit*.p.119.

privée dans le domaine commercial ont fait l'objet d'une règlementation particulièrement approfondie. En conséquence, plusieurs principes émanent de la loi-type relative à la protection des données personnelles : il s'agit des principes luttant contre l'utilisation abusive des données et des principes étroitement liés à la collecte et au traitement des données à caractère personnel qui apparaissent comme des obligations du responsable du traitement.

D'après le principe de loyauté, la collecte, l'enregistrement, l'utilisation et la transmission des données à caractère personnel du consommateur doivent se faire de bonne foi. Autrement dit, le traitement des données à caractère personnel, quelle que soit son origine ou sa forme, ne doit pas porter atteinte aux droits des consommateurs. Le principe de la loyauté dans la collecte des données signifie que les données collectées doivent être indispensables à l'opération. À cet effet, la collecte ne doit pas se faire à l'insu du consommateur [94]. Toutefois, dans la pratique, aussi bien des commerçants que des fournisseurs de contenus et services électroniques recourent aux cookies, pour jauger les potentiels clients. Ces cookies[95], qualifiées de « témoins » de la navigation des internautes permettent au professionnel de passer au crible de métriques le nombre de connexions, d'amis, de followers, de messages envoyés ou reçus, nombre de fois où le profil du client aura été consulté, de pages ou sites web sur lesquelles son nom apparaît[96]. Ainsi, pour collecter des données personnelles, la plupart des professionnelles à l'insu des consommateurs utilisent essentiellement les cookies qui apparaissent alors comme des « petits programmes espions» [97], très efficaces pour atteindre la clientèle. Or, la donnée est une partie constitutive de la personne et ne peut être cédée sans son consentement.

Le principe de finalité signifie que l'utilisation des données personnelles du consommateur doit être strictement limitée à une finalité explicitement déterminée au préalable. À cet effet, le collecteur des données personnelles doit exposer les objectifs qu'il désire atteindre par la collecte. La collecte des données doit avoir une finalité licite, déterminée et explicite. La collecte, l'enregistrement et l'utilisation des données personnelles sont strictement limités à ce qui est nécessaire pour atteindre des buts expressément fixés d'avance par le professionnel. Ceci signifie que, la finalité doit non seulement être déterminée et explicite, c'est-à-dire non équivoque, mais aussi, elle doit être licite, c'est-à-dire conforme à la loi en vigueur et aux bonnes mœurs. Le caractère explicite et déterminée de la finalité signifie que le professionnel ne doit pas transmettre les données du consommateur à d'autres personnels sauf si ces derniers en ont besoin dans le cadre de la réalisation des mêmes buts et ne les utiliseront que de manière compatible. Toutefois, les données personnelles du consommateur peuvent être utilisées à des fins autres que celles affirmées lors de la collecte s'il a donné son consentement ou si le traitement est nécessaire à la sauvegarde d'un intérêt vital[98].

D'après le principe de sécurité des données à caractère personnel, tout responsable qui effectue le traitement des données à caractère personnel est tenue à l'égard du consommateur de prendre toute les précautions nécessaires pour assurer la sécurité de ses données et empêcher les tiers de procéder à leur modification, à leur altération ou à leur consultation sans l'autorisation de celui-ci. Autrement dit, le responsable du traitement doit prendre toutes les précautions utiles afin de garantir la confidentialité des données et d'empêcher leur déformation, endommagement, ou communication à un tiers non autorisé. Le principe de sécurité des données vise à assurer l'intégrité et la confidentialité des données lors de leur conservation. Ainsi, le responsable du traitement doit prendre des précautions qui consiste à empêcher que les équipements et les installations utilisés dans le traitement des données à caractère personnel soient placés dans des conditions ou des lieux permettant à des personnes non autorisées d'y accéder ; empêcher que les supports des données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée ; empêcher l'introduction non autorisée de toute donnée dans le système d'information, ainsi que toute prise de connaissance, tout effacement ou toute radiation des données enregistrées ; garantir que puisse être vérifiée a posteriori l'identité des personnes ayant eu accès au système d'information ; empêcher que les données puissent être lues, copiées, modifiées, effacées ou radiées, lors de leur communication où du transport de leur support ; sauvegarder les données par la constitution de copie de réserve sécurisées. L'obligation de sécurité intervient avant toute divulgation des données. Pour assurer une protection complète des données lors de leur conservation, il faudrait réglementer aussi la durée de leur conservation. C'est ce que la doctrine appelle le droit à l'oubli[99].

Le droit à l'oubli[100] peut être vu comme le droit de suppression, le droit de suite. C'est le droit qu'a le

[94] BOYER (J.), « L'Internet et la protection des données personnelles et de la vie privée », *Cahier Français*, n° 295, p.74.
[95] PANSIER (F-J.) et JEZ (E.), *L'initiation à l'Internet juridique*, Paris, Litec, 1998, p.72.
[96] GILLE (L.), « La donnée au cœur du numérique : questions », pages 28 & 32.
[97] PANSIER (F-J.) et JEZ (E.), *L'initiation à l'Internet juridique*, Paris, Litec, 1998, p.72.
[98] V. Art. 41 de la Loi-type relative à la protection des données personnelles.
[99] LIDON (R.), La création prétorienne en matière de droit de la personnalité et son incidence sur la notion de famille, Paris, *DALLOZ*, 1974, p.25.
[100] Dans l'arrêt du 13 mai 2014, la CJUE a posé que l'exploitant d'un moteur de recherche « *est obligé de supprimer de la liste des résultats, affichée à la suite d'une*

consommateur d'exiger que ses données personnelles soient supprimées de toute base de données, c'est à dire le droit de voir ses données oubliées après un certain temps. C'est dire qu'après la durée de traitement, les informations doivent être rendues anonymes [101]. Les données doivent être conservées jusqu'à l'accomplissement de la finalité déclarée par le responsable du traitement. Une fois cette finalité accomplie, les données perdent leur raison d'être et doivent être détruites.

D'après le principe de légitimité, le traitement des données personnelles n'est possible que s'il existe une raison suffisamment légitime pour le justifier. Autrement dit, le traitement des données peut être légitimé s'il existe un intérêt justifié à condition que le traitement desdites données n'affecte la vie privée que de façon infime. Ce principe recommande la licitée dans le traitement des données.

Le principe de nécessité et de proportionnalité implique que les données personnelles doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées[102]. Le traitement doit se limiter aux données pour lesquelles il existe un rapport direct avec la finalité initiale du traitement. Ces données doivent non seulement être utiles, mais aussi nécessaires pour celui qui les traite.

D'après le principe de sécurité et de confidentialité, les données personnelles doivent être traitées de manière confidentielle et être stockées à des lieux et sur du matériel sûrs. Ce principe met en relief le secret professionnel. C'est dire que les données personnelles ne doivent pas être divulguées[103]. En cas de non-respect de ce principe, la responsabilité du professionnel peut être engagée.

Le principe d'exactitude des données : les données traitées doivent être correctes et actuelles. Si ce n'est pas le cas, les données personnelles doivent être rectifiées ou bien effacées. La loi protège également contre toute décision négative prise automatiquement par ordinateur, dont le consommateur peut faire l'objet sans pouvoir faire valoir son point de vue personnel.

Le principe de transparence : le responsable du traitement doit fournir au consommateur des informations nécessaires relatives aux traitements auxquels sont soumises ses données et doit assurer à ce dernier la possibilité d'un contrôle personnel. Le responsable du traitement doit renseigner le consommateur sur l'usage qui sera fait de ses données personnelles.

Le principe de renforcement de la protection des données sensibles et de surveillance : Le traitement les données génétiques, d'informations relatives aux opinions et convictions ou qui ont un lien avec la santé et la vie sexuelle, est interdit hormis les cas expressément prévus par la loi.

L'interdiction du spamming : Il s'agit de l'utilisation des données personnelles à des fins commerciales. En effet, le marketing direct à l'aide des moyens de communication modernes (SMS, e-mail, etc.) est interdit sauf si le consentement du consommateur a été obtenu.

En résumé, on peut affirmer que le droit des technologies de la CEMAC protège les consommateurs. Toutefois il existe encore des failles qu'il faudrait combler.

---

recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne ( ) et ce ( ) même lorsque leur publication en elle-même sur lesdites pages est licite ». Elle ajoute qu'il convient « *d'examiner si la personne concernée a un droit à ce que l'information en question ( ) ne soit plus ( ) liée à son nom* », notamment si l'information paraît inadéquate, pas ou plus pertinente ou excessive au regard des finalités du traitement, et que cette personne doit pouvoir « *demander que l'information en question ne soit plus mise à la disposition du grand public* ». L'arrêt précise cependant que « *tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir ( ) accès à l'information* » (CJUE, 13 mai 2014, affaire C-131/12).

[101] TROUSSEAU (M.-P.F.)- et HAAS (G.), op.cit., *Internet et protection des données personnelles*, Paris, Litec, 2000, p. 56.

[102] Cf. art. 4, al. 1(c), de la Loi-type relative à la protection des données personnelles.

[103] Cf. Art. 14 de la Loi-type relative à la protection des données personnelles.