Le droit à la vie privée à l'ère des TIC au Cameroun

Hervé Martial Tchabo Sontang

Édition électronique

URL : <http://journals.openedition.org/revdh/7975>

DOI : 10.4000/revdh.7975

ISSN : 2264-119X

Éditeur

Centre de recherches et d'études sur les droits fondamentaux

Référence électronique

Hervé Martial Tchabo Sontang, « 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 19 octobre 2020.

URL : <http://journals.openedition.org/revdh/7975> ; DOI : <https://doi.org/10.4000/revdh.7975>

Ce document a été généré automatiquement le 19 octobre 2020.

Tous droits réservés

Le droit à la vie privée à l'ère des TIC au Cameroun

Hervé Martial Tchabo Sontang

- 1 Larry PAGE, l'un des deux fondateurs de Google, aime bien faire remarquer que ce service de recherche sur le Web fait partie du quotidien d'un grand nombre de gens, au même titre que se brosser les dents¹. Cette affirmation illustre bien combien il est difficile de nos jours de mener une vie déconnectée des réseaux de communications électroniques. Les supports de l'environnement électronique, les technologies de l'information et de la communication (TIC)², ont envahi le quotidien de l'Homme. Être joignable, être disponible, signifient de nos jours être connecté à des réseaux de communications électroniques. Cette situation n'est pas sans impact sur l'humanité. De nombreuses études imputent d'ailleurs à cette relation, quelquefois intime, entre l'Homme et les TIC, des conséquences parfois dramatiques et inattendues comme la dégradation de la qualité des relations sociales ou le développement de nouvelles formes d'addictions³. Par ailleurs, et surtout si rien n'est fait, le concept de vie privée, pourtant si important pour l'équilibre des rapports sociaux⁴, deviendra vide de sens⁵.
- 2 Comme on peut l'entrevoir, la vie privée désigne la sphère d'intimité réservée à chaque individu et protégée contre les intrusions extérieures, qu'elles proviennent des autres individus ou même de l'État. En d'autres termes, c'est l'espace dans lequel l'organisation de la vie de chacun « ne regarde personne d'autre que lui et ses intimes »⁶. Ainsi, elle est un rempart, un sanctuaire pour tout individu, voire, une nécessité⁷. C'est évidemment parce qu'elle est fondamentale pour l'épanouissement de l'homme dans la société⁸ que sa protection est garantie au plan mondial par les textes internationaux, notamment le Pacte international relatif aux droits civils et politiques (PIDCP)⁹ qui, sans doute inspiré par l'article 12¹⁰ de la Déclaration Universelle des Droits de l'Homme, dispose de manière solennelle que : « nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes »¹¹. Sur le plan africain, l'on peut citer, bien que le Cameroun ne l'ait pas encore ratifiée, la Convention de l'Union Africaine sur la

cybersécurité et la protection des données personnelles¹² dont l'un des principaux objectifs, tels que déclinés dans son préambule, est de « *mettre en place, dans chaque État partie, un dispositif permettant de lutter contre les atteintes à la vie privée susceptibles d'être engendrées par la collecte, le traitement, la transmission, le stockage et l'usage des données à caractère personnel* ».

- 3 Sur le plan national, même si l'expression « *vie privée* » n'est pas expressément mentionnée dans la Constitution, on doit cependant reconnaître que le cadre de sa protection est bien fixé par les dispositions de la norme fondamentale en ce qu'elles protègent distinctement les différents aspects qui constituent le cadre d'exercice de la vie privée. C'est ainsi que son préambule¹³ pose clairement le principe de l'inviolabilité du domicile et du secret de la correspondance. Prenant le relais, la loi relative à la cybersécurité et la cybercriminalité pose que « *toute personne a droit au respect de sa vie privée* »¹⁴ et, pour assurer l'effectivité de ce droit, le Code pénal camerounais sanctionne, notamment sous les qualifications de diffamation¹⁵, de violation de domicile¹⁶ ou de violation du secret de la correspondance¹⁷, les atteintes à l'honneur et à la vie privée des individus.
- 4 Avec le développement des outils et réseaux de communications électroniques, la vigueur de ce dispositif protecteur semble prendre un coup. En effet, la révolution numérique¹⁸ qui marque l'époque contemporaine draine dans son sillage une métamorphose des mœurs, des usages et des pratiques sociales ne s'accommodant pas toujours avec le caractère fondamental de la vie privée et de ses attributs. Beaucoup d'outils et de procédés techniques permettent de nos jours aux tiers d'accéder, à distance, dans la sphère d'intimité d'autrui, de le suivre grâce aux méthodes de géolocalisation. Dans ce contexte¹⁹, il est évident que, si rien n'est fait, la distinction vie privée/vie publique²⁰, essentielle dans un État de droit²¹, court inévitablement le risque de devenir caduque²². Face à cette menace, il paraît nécessaire de se poser la question de savoir si, à l'ère des TIC, le droit à la vie privée a-t-il encore un contenu réel en droit camerounais, autrement dit, à l'ère des TIC, le droit à la vie privée bénéficie-t-il en droit camerounais d'une protection véritable ?
- 5 Pour bien comprendre et répondre à cette question il convient préalablement d'observer que, dans un contexte dominé par les TIC, le concept de vie privée a fait sa mue dans la mesure où la cloison entre l'espace privé et l'espace public s'est notablement effritée. Ainsi, la protection de la vie privée ne saurait plus se fonder sur une considération dépassée, opposant les lieux de vie privée à ceux de vie publique. On admet par exemple que sur le lieu du travail, lieu public en principe²³, le salarié continue à bénéficier d'un espace privé sur le disque dur de l'ordinateur mis à sa disposition par l'employeur pour les besoins de service²⁴. Aussi, les facilités avec lesquelles les TIC permettent de collecter des informations propres aux individus et de les traiter massivement ont fait comprendre qu'il ne s'agit plus seulement, au nom de la vie privée, de protéger ce qui relève strictement du domicile de l'individu, mais, aussi de préserver ce qui, bien que révélé ou connu publiquement²⁵, est cependant rattaché à une personne et constitue ainsi une donnée permettant de l'identifier, mieux, une donnée à caractère personnel.
- 6 Cette notion, donnée à caractère personnel, est fille de la révolution numérique car, spécialement « *développée en réponse à la menace que pouvaient représenter les technologies de l'information pour les libertés individuelles et sur la vie privée* »²⁶. C'est ainsi qu'elle est présentée comme « *le socle de la protection des personnes dans un univers complexe et*

numérique »²⁷. À travers elle, on regroupe toutes les données²⁸ et informations, et tous les éléments pouvant permettre d'identifier, directement ou indirectement, une personne physique²⁹. Plus précisément, une donnée à caractère personnel pourrait être définie 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 économique³⁰. Cette définition permet d'observer qu'en plus des informations nominatives qui permettent d'identifier directement un individu, rentrent aussi dans cette notion d'autres informations et données qui ne servent qu'indirectement à l'identification d'une personne. La notion de données à caractère personnel est donc plus large que celle d'informations nominatives.

- 7 S'il est évident, au regard des éléments qui précèdent, que la notion de vie privée dans sa conception classique et celle de données à caractère personnel se recoupent en ce qu'elles se rattachent à l'idée de la protection de l'individu dans ses rapports avec la société, force est de constater qu'elles ne se confondent pas. On peut à cet effet observer par exemple que certains aspects relevant du domaine de la vie privée, à l'instar du secret de la correspondance, échappent au qualificatif de donnée à caractère personnel ; en revanche, les éléments tels le nom, la voix³¹, l'image³² ou même l'adresse professionnelle³³ d'une personne, constituant des données à caractère personnel, ne rentreraient pas classiquement dans le giron de la vie privée. Cette nuance s'observe davantage au sujet d'une copie d'examen, assortie des annotations du correcteur, dont la nature de donnée à caractère personnel a été reconnue par la Cour de Justice de l'Union Européenne³⁴ sans qu'on puisse dire qu'il s'agit véritablement d'un élément de la vie privée au sens traditionnel³⁵. Ces exemples permettent de comprendre que la notion de donnée à caractère personnel présenterait un certain degré d'autonomie³⁶ par rapport à celle de vie privée prise dans son sens classique.
- 8 Cependant, pour bien comprendre le questionnement relatif à la vie privée, il faut intégrer dans le raisonnement le fait qu'elle n'a pas toujours eu la même place dans la société au fil des époques historiques. Les travaux de certains auteurs³⁷ montrent bien que la vie privée n'est pas une réalité naturelle et que ses contours se redéfinissent en permanence³⁸. Le rythme de ces redéfinitions épouse en général l'allure de la courbe des mutations sociales. On doit donc comprendre que la notion de vie privée de même que le régime de sa protection doivent épouser le contexte social dans lequel les citoyens vivent. Plus concrètement, la digitalisation qui marque profondément la vie sociale actuellement et qui entraîne la révolution numérique³⁹ impose aux pouvoirs publics un changement d'approche dans la régulation des rapports sociaux. C'est d'ailleurs l'idée qui a motivé l'adoption par le parlement sénégalais de la loi sur la protection des données personnelles dont l'exposé de motifs souligne qu'« avec le développement de l'informatique et de ses applications, le domaine traditionnel de la vie privée s'enrichit chaque jour de nouveaux éléments »⁴⁰.
- 9 Ce constat fait donc apparaître les données à caractère personnel comme une partie du principe de la vie privée qui englobe tout ce qui se rattache à l'identité personnelle, familiale d'une personne ainsi qu'à son image⁴¹. Dans sa conception actuelle donc, la vie privée intègre désormais toutes les informations⁴² pouvant permettre d'identifier un individu. Il s'agit simplement ainsi de tenir compte de « l'extension conceptuelle de la vie privée au numérique »⁴³. C'est par ailleurs cette manière de voir que préconise le Conseil

constitutionnel français lorsqu'il conclut que la protection des données à caractère personnel est une composante de la vie privée⁴⁴.

- 10 Dès lors, protéger la vie privée dans le contexte des TIC, c'est prendre des mesures juridiques appropriées pour éviter « *de voir des institutions, publiques ou privées, ou même des individus, utiliser des informations relatives à notre vie privée pour porter atteinte à nos libertés et à notre capacité d'auto-détermination* »⁴⁵. Cela revient donc, non seulement à préserver l'intimité de l'individu concerné, mais aussi, à sécuriser toutes les données qui permettent de l'identifier. C'est cette compréhension qui va servir de trame aux développements qui suivent.
- 11 Dans ce cadre, il est patent de constater que le droit positif camerounais n'ignore pas fondamentalement la problématique de la protection de la vie privée à l'ère des TIC dans la mesure où plusieurs textes portant globalement sur les différents aspects de l'économie numérique contiennent quelques règles relatives à la protection de la vie privée. Mais, la garantie que ces règles assurent à ce droit fondamental est bien limitée (I). À cela, se superpose un cadre de régulation inadéquat (II).

I Un droit objet d'une garantie limitée dans le contexte du numérique

- 12 Ayant vite perçu le risque que l'informatisation de la société pouvait faire courir à la vie privée et plus spécifiquement aux données à caractère personnel, l'ONU a défini un ensemble de principes devant encadrer le traitement des données à caractère personnel⁴⁶. Ces principes sont complétés par d'autres instruments juridiques. Sont ainsi notamment consacrés les principes de finalité⁴⁷, de loyauté et de transparence⁴⁸, de pertinence ou de proportionnalité⁴⁹, d'accès de rectification et d'opposition⁵⁰, de sécurité et de confidentialité⁵¹, de respect de la dignité de la personne concernée, de la limitation de la durée du traitement⁵², et bien d'autres. C'est donc à la lumière de ces principes essentiels que l'on peut dire que la garantie dont bénéficie la vie privée dans le contexte camerounais est limitée. En effet, même si certaines règles traduisent un effort du droit camerounais de garantir la jouissance effective de la vie privée à l'ère des TIC (A), il demeure que, pour le moment, certaines pratiques intrusives demeurent encore en dehors du droit (B).

A. L'effort de construction d'un régime préservant la vie privée

- 13 Si l'on peut quelquefois trouver dans l'arsenal juridique camerounais des règles et principes régissant certains usages des TIC en lien avec la vie privée, c'est néanmoins au prix d'un certain effort dans la mesure où ils ne sont pas tous recensés dans un texte en particulier, ce qui donne l'impression d'un cadre juridique, non seulement insuffisant, mais aussi dispersé, voire désintégré. En effet, chaque règle s'applique dans un cadre particulier. On peut ainsi distinguer les règles consacrées dans le cadre de la réglementation des communications électroniques (1) de celles posées en dehors du domaine des communications électroniques (2).

1) La prise en compte de la vie privée dans la réglementation des communications électroniques

- 14 Dans le cadre de la réglementation des communications électroniques, le droit positif camerounais, fortement marqué de l'empreinte des textes communautaires de la Communauté économique et monétaire de l'Afrique centrale (CEMAC), contient quelques règles visant directement ou indirectement la protection de la vie privée des utilisateurs des terminaux et des services de communications électroniques et des tiers. Ces règles sont contenues dans plusieurs textes d'origine communautaire⁵³ ou nationale⁵⁴. Elles forment un dispositif essentiellement guidé par les principes de droit communautaire de la confidentialité des communications effectuées au moyen des réseaux de communications électroniques accessibles au public et de la confidentialité des données relatives au trafic y afférent⁵⁵. Ils sont traduits en droit interne par les règles garantissant l'inviolabilité et le secret des communications électroniques, excepté dans les conditions légalement et réglementairement applicables⁵⁶. De même, sont institués le droit de recourir à l'anonymat, l'interdiction d'usurper de l'identité d'autrui, le droit du titulaire des données de donner son consentement ou de s'opposer à certains traitements.
- 15 Concernant le droit de recourir à l'anonymat, le régime mis en place par le législateur vise globalement à garantir la tranquillité des abonnés. D'une part, la tranquillité de l'émetteur qui souhaite être anonyme en exigeant alors de son opérateur la non-divulgaration⁵⁷ de son identificateur d'accès⁵⁸. Pour garantir ce privilège, la loi oblige les opérateurs des réseaux ouverts au public à offrir aux consommateurs, par un moyen simple et gratuit, la possibilité de masquer leurs numéros⁵⁹.
- 16 S'il est un droit pour l'abonné de ne pas révéler son identité aux autres utilisateurs du réseau, il reste cependant que le recours à l'anonymat ne doit pas servir de moyen pour des actes ou des fins illicites. Ce risque est réel et c'est pour le contenir que le législateur interdit la possibilité de communiquer sous anonymat dans certains cas⁶⁰. De même, pour garantir la tranquillité des autres abonnés, il est encore mis à la charge des opérateurs l'obligation de leur proposer des systèmes de blocage des appels secrets et des appels malveillants⁶¹, lesquels sont très souvent faits sous le couvert de l'anonymat.
- 17 Dans tous les cas, on doit observer qu'en cas de recours à l'anonymat, l'identité de l'appelant n'est masquée qu'à l'égard du destinataire de l'appel puisqu'en effet, tout abonné à un réseau de communication ouvert au public est obligatoirement identifié auprès de son opérateur comme l'exige l'article 55⁶² de la loi n° 2010/013 régissant les communications électroniques au Cameroun. Donc, en cas de nécessité, l'opérateur pourra techniquement, et devra juridiquement, lever l'anonymat pour permettre aux autorités compétentes de mener aisément leurs investigations. Par ces règles, le législateur essaie de prendre en compte tout à la fois, le droit à l'anonymat d'un abonné et le droit à la tranquillité des autres utilisateurs du réseau.
- 18 Ce droit à la tranquillité est complété par l'interdiction faite aux tiers d'usurper de l'identité d'autrui⁶³. Usurper l'identité d'autrui pourrait se comprendre comme le fait d'utiliser une ou plusieurs données de toute nature permettant d'identifier un tiers en vue soit de troubler sa tranquillité ou celle d'autrui, soit de porter atteinte à son honneur ou à sa considération. Il s'agit évidemment d'un acte d'intrusion dans la vie privée d'autrui. Sous cette qualification, il faut saisir la pratique, devenue très courante

et banalisée sur les réseaux sociaux, consistant à attribuer à certaines personnalités des propos qui ne leur reviennent pas exactement ou encore celle consistant à adopter un nom ou une photo de profil appartenant à un tiers, généralement bien connu du public. Toujours dans ce registre, doit être assimilée la pratique de *scamming* consistant à pirater les paramètres de connexion à la messagerie électronique d'un tiers pour envoyer des messages malsains à des fins d'extorsion de fonds aux correspondants dont les adresses sont contenues dans le répertoire de la messagerie piratée. Dans le contexte camerounais, certaines autorités publiques⁶⁴ ont été victimes d'usurpation d'identité sur le réseau social Facebook. Très souvent, les victimes ont dû commettre des communiqués pour dénoncer publiquement l'usurpation de leur identité par des individus mal intentionnés⁶⁵. En attendant que le juge pénal camerounais ait l'occasion de se prononcer sur ces faits qui, sans doute constitue une infraction⁶⁶, il convient de souligner, à titre de droit comparé, que le juge pénal français a déjà eu l'opportunité de sanctionner des comportements constitutifs d'usurpation d'identité sur Facebook⁶⁷.

- 19 Pour limiter les risques d'utilisation illicite des données nominatives d'autrui, il est érigé en infraction pénale le fait de conserver des données à caractère personnel dans une base de traitement au-delà du temps défini⁶⁸. Il n'en sera autrement que si les États, pour des raisons sécuritaires, demandent aux opérateurs de garder ces informations pour une durée maximale de deux (2) ans⁶⁹.
- 20 Pour illustrer le droit de consentement ou d'opposition, il convient de préciser que, le traitement des données concernant les utilisateurs des services de communications électroniques, autres que celles relatives au trafic, ne peut être fait que par des personnes habilitées et exclusivement dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée, après avoir été rendues anonymes ou après que l'utilisateur ait donné son consentement éclairé, qu'il peut retirer à tout moment⁷⁰. Le caractère exprès de ce consentement pourrait être très prochainement consacré⁷¹ de telle sorte que, comme l'a précisé le juge français, à titre de droit comparé, on ne puisse déduire de l'accessibilité d'une donnée à caractère personnel et de l'absence de plainte de son titulaire son consentement à son traitement, lequel demeure alors frauduleux⁷².
- 21 Ce droit ne s'impose pas seulement aux opérateurs des réseaux de communications électroniques. On doit bien comprendre que, par principe, la publication des données à caractère personnel ou l'allusion faite à la vie privée d'un tiers sur les réseaux sociaux ne devraient pas se faire sans le consentement de la personne concernée. Il est notamment contraire à la loi pénale camerounaise⁷³ le fait de publier, sans l'avis préalable des intéressés, des photos réalisées dans un contexte particulier et permettant aisément d'identifier des personnes⁷⁴. Le consentement donné pour un traitement précis ne vaut pas pour un autre type de traitement, c'est le principe de la finalité. De même, lorsque le consentement de la personne concernée n'est pas nécessaire pour la collecte des données, le traitement qui s'ensuit peut cependant nécessiter son accord préalable. C'est ainsi qu'un individu qui ne remet pas en cause la licéité de la vidéo réalisée dans un milieu public, peut cependant critiquer son utilisation ultérieure. Dans un cas similaire, et à titre de droit comparé, la Cour Européenne des Droits de l'Homme a conclu qu'il s'agissait, du point de vue de la protection des données, d'un détournement de finalité puisque les données avaient été captées dans un but de surveillance des voies publiques et étaient ensuite utilisées pour illustrer l'utilité de la vidéosurveillance⁷⁵.

- 22 Participe toujours du droit des utilisateurs au consentement la consécration du principe de l'*opt-in*⁷⁶ en matière de messagerie publicitaire. Ainsi, le prestataire des services de communications électroniques doit, en principe, préalablement recueillir le consentement du destinataire du message avant l'envoi.
- 23 Certains de ces principes sont repris par certains des textes en vigueur en dehors du domaine des communications électroniques.

2) Le souci de préserver la vie privée hors du domaine des communications électroniques

- 24 En passant en revue certains textes du droit camerounais, l'analyste peut observer que certains textes particuliers consacrent, dans le cadre de leur objet spécifique, des règles ayant directement ou indirectement pour souci de protéger la vie privée dans le cadre des opérations de traitement des informations relatives aux individus. Il en est ainsi notamment des textes qui régissent le secteur bancaire ou de ceux qui s'appliquent à l'enseignement supérieur.
- 25 Pour prendre l'exemple du secteur bancaire, il faut dire qu'il est l'un des secteurs les plus concernés par le traitement des données personnelles, ce dans la mesure où chaque transaction bancaire donne lieu à la collecte d'une pile d'informations présentant un caractère éminemment privé. La réglementation de ce secteur a d'ailleurs institué un ensemble de fichiers pour les collecter et les traiter suivant différentes finalités. L'un des instruments essentiels de cette démarche est la Centrale des Incidents de Paiements (CIP). Consacrée par l'article 210 du règlement du 04 avril 2003 sur les systèmes, moyens et incidents de paiement et est constituée de 4 fichiers⁷⁷. Les informations collectées et contenues dans ces différents fichiers ont évidemment un caractère personnel puisqu'elles sont relatives à l'identité des personnes et qu'elles contiennent des renseignements se rapportant à leur patrimoine et à certaines décisions de justice ayant en général un caractère pénal. Les opérations qui y sont réalisées constituent donc des traitements de données à caractère personnel. Partant, le texte qui organise leur fonctionnement prescrit un ensemble de précautions.
- 26 L'une des premières précautions, qui vise sans doute à garantir le principe de la confidentialité des données en évitant le risque de leur divulgation aux personnes non autorisées, est que les données sont collectées pour un but précis et elles ne peuvent être consultées que par des entités justifiant d'un intérêt légitime s'inscrivant dans la finalité indiquée. Ainsi, seuls les établissements assujettis, les juridictions, les autorités d'enquêtes et certaines administrations publiques dont la liste doit être limitativement établie peuvent consulter ces fichiers, en ligne ou par messagerie. Par ailleurs, la procédure de consultation est sécurisée⁷⁸. Ce souci de confidentialité est renforcé par le principe du secret bancaire⁷⁹ mis à la charge des établissements de crédits et leurs préposés⁸⁰.
- 27 Concernant les droits du titulaire des données traitées, notamment les droits d'accès et de rectification, il est prévu que les personnes physiques ou morales qui contestent l'exactitude des informations déclarées à la CIP qui les concernent, ont le droit de demander la rectification desdites informations auprès de l'établissement assujetti déclarant, lequel est tenu d'effectuer les rectifications nécessaires, s'il s'avère que les informations étaient inexacts, et d'en informer la CIP⁸¹. Une règle analogue est

consacrée, dans le contexte académique, au profit de l'étudiant relativement à la tenue de son dossier académique⁸².

- 28 Les personnes dont les données sont traitées ont en plus le droit de voir lesdites données effacées ou anonymisées au bout d'un délai prescrit. Pour le cas de la centrale des incidents de paiement, la durée de conservation légale est de 15 ans⁸³. Pour que toutes ces règles soient respectées, il faut évidemment soumettre les responsables de traitement à un contrôle strict. Un tel contrôle est illusoire si déjà la pratique qui donne lieu à la collecte des données ne fait l'objet d'aucun encadrement.

B. La subsistance des pratiques intrusives non encadrées

- 29 De plus en plus, on assiste dans la société camerounaise à l'implémentation des solutions technologiques mettant la vie privée et les données personnelles des citoyens en danger. Parmi ces nombreuses pratiques hautement intrusives, on peut citer l'usage de la vidéosurveillance et la collecte des données biométriques aux fins d'identification ou d'authentification.
- 30 Les nouveaux enjeux de gouvernance et de sécurité poussent nécessairement les pouvoirs publics à rechercher les meilleures solutions de transparence des processus démocratiques et d'anticipation sur les projets criminels. C'est dans ce contexte que la biométrie est très largement employée pour la sécurisation des titres identitaires⁸⁴ et que la vidéosurveillance est implémentée dans la plupart des villes stratégiques de la République du Cameroun⁸⁵.
- 31 La notion de biométrie désigne couramment la reconnaissance, l'identification et l'authentification d'une personne sur la base d'une caractéristique biologique⁸⁶ telle l'iris, la voix, ou l'empreinte digitale. Ainsi comprise, il y a lieu d'observer que son utilisation et ses différentes applications ne sont pas du domaine du monopole des pouvoirs publics. En effet, beaucoup d'entités privées, notamment des sociétés commerciales⁸⁷, exploitent cette technologie pour contrôler l'assiduité et la loyauté de leurs employés. Le marché de la biométrie, de même que celui de la vidéosurveillance est d'ailleurs désormais en pleine expansion au Cameroun à en juger au moins par la diversité des prestataires⁸⁸. L'implémentation de ces technologies aboutit inmanquablement à une collecte massive des données biologiques des citoyens. Chaque fois, en effet, qu'une empreinte digitale est collectée, que l'iris est filmé ou que la voix est enregistrée, les fichiers sont en général conservés dans des bases de données pour traitement. On ne peut d'ailleurs identifier un individu par ces moyens que si préalablement un échantillon est conservé dans les serveurs pour vérifier la conformité et valider l'identité ultérieure du titulaire.
- 32 Même si les données qu'elle permet de collecter ne sont pas de nature biologique, la vidéosurveillance est tout aussi menaçante pour la vie privée et les données personnelles des individus, notamment parce qu'elle permet de collecter des informations sur les individus et de retracer les parcours qu'ils suivent. En plus des programmes de surveillance urbaine tels qu'indiqués ci-dessus, la vidéosurveillance est une solution très implémentée à des fins sécuritaires dans les établissements bancaires et les supermarchés notamment. Si son utilité peut être aisément comprise, il est cependant clair qu'en l'absence d'un cadre juridique formel, le risque des dérives est réel. C'est pourquoi dans la plupart d'États de droit, son utilisation est soumise à une autorisation de l'autorité compétente et, faute d'avoir accompli une telle formalité,

s'agissant notamment du domaine des relations professionnelles, l'employeur ne saurait imposer l'utilisation du dispositif de vidéosurveillance à l'employé⁸⁹.

- 33 N'est pas véritablement éloignée de la problématique de la vidéosurveillance la pratique consistant à exiger de l'employé qu'il soit permanemment connecté pour répondre aux sollicitations du service même à domicile et pendant les périodes de repos ou de congés. C'est en effet une autre forme de surveillance et d'embrigadement du salarié grâce aux outils de communication en ligne. C'est pour lutter contre cette pratique intrusive et garantir aux salariés un équilibre entre le travail et la vie privée que la Belgique⁹⁰, à la suite de la France, a adopté une loi demandant aux entreprises de veiller à ce que les nouveaux moyens de communication ne portent pas atteinte au respect des temps de repos et de congés. C'est ce qu'on appelle parfois, à tort il faut bien l'avouer, le « droit à la déconnexion »⁹¹.
- 34 Curieusement, au Cameroun, le droit positif est aphasique sur ces questions. Il n'existe pas véritablement de règles qui encadrent la mise en œuvre et l'exploitation de ces solutions par les entités concernées, qu'elles soient publiques ou privées. Il est curieux de constater que l'autorité réglementaire qui prévoit des mécanismes de collecte des données à caractère personnel dans le cadre de la production des titres identitaires, n'ait, dans aucun des décrets en vigueur⁹², pris le soin d'indiquer précisément les principes qui gouverneront le traitement desdites données. Le simple fait de prévoir qu'un responsable aura la charge de « *veiller au respect strict des règles de professionnalisme, d'intégrité et d'éthique auxquelles est assujéti le personnel du Centre National de Production des Titres Identitaires* »⁹³ n'est pas suffisant. Il faut, pour combler ces manquements renforcer et mieux articuler le dispositif de régulation qui, pour l'instant, se révèle inadéquat.

II. Un droit relevant d'un cadre de régulation inadéquat

- 35 Il n'est pas abusif de dire qu'en l'état actuel du droit camerounais, la configuration du cadre de régulation des services numériques ne permet pas d'assurer avec efficacité la protection de la vie privée dans l'environnement électronique (A). À cela, s'ajoute le fait que certaines questions précises n'ont pas été expressément dévolues aux régulateurs, ce qui donne à leurs compétences cumulées un caractère limité (B).

A. L'inadéquation découlant de la configuration du cadre de régulation

- 36 En droit camerounais, les questions relatives à la protection de la vie privée dans le domaine des TIC relèvent, principalement, de la compétence de deux organes de régulation (1), ce qui n'est pas de nature à garantir l'efficacité du dispositif exposé à un risque de conflit de compétences (2).

1) L'intervention de deux organes de régulation

- 37 Dans sa configuration actuelle, l'environnement électronique est caractérisé par le déséquilibre des forces en faveur des opérateurs. Par diverses techniques échappant pour la plupart à la connaissance des utilisateurs, les professionnels s'assurent subtilement la collecte et le traitement massif des données des utilisateurs.

Ces procédés de traitement et leurs finalités ne sont pas généralement compatibles avec le caractère fondamental de la vie privée. Celle-ci étant un sanctuaire dont le principe de la protection est consacré, il est important qu'un gardien vigilant soit institué pour la préserver d'agressions extérieures. Ainsi, l'utilisateur ne pouvant seul assurer le respect de sa vie privée dans l'environnement électronique, il est nécessaire qu'un organe neutre, impartial, mais suffisamment efficace, soit mis en place pour encadrer les rapports entre les différentes parties prenantes et éviter au maximum qu'on aboutisse à la réification, déjà dénoncée⁹⁴, des données relatives à la vie privée des utilisateurs notamment. Il faut d'ailleurs souligner que c'est dans le cadre de la protection des données personnelles qu'en 1978, la première autorité administrative indépendante, la Commission Nationale Informatique et Libertés (CNIL), a été créée en France. Elle est, à ce jour, présentée comme « *la véritable pierre angulaire du régime de protection des données* »⁹⁵. Le caractère indépendant de cette commission, qui tient dans une certaine mesure au contexte de sa création⁹⁶, démontre bien que la question de la protection des données personnelles doit être régulée par une entité séparée de toutes les parties prenantes et autonome de l'État puisqu'il s'agit dans nombre de cas de protéger les citoyens contre l'État lui-même⁹⁷.

- 38 L'expérience de la CNIL en France a largement inspiré la définition, par l'Assemblée Générale de l'ONU, des Principes directeurs des Nations Unies pour la réglementation des fichiers informatisés contenant des données à caractère personnel. Le principe n° 8 précise que « *chaque législation devrait désigner l'autorité qui, en conformité avec le système juridique interne, est chargée de contrôler le respect des principes précités. Cette autorité devrait présenter des garanties d'impartialité, d'indépendance à l'égard des personnes ou organismes responsables des traitements et de leur mise en œuvre, et de compétence technique* ». De la formulation de ce principe, on comprend bien qu'un seul organe doit être chargé de cette mission. Par ailleurs, il est évident que c'est à l'État qu'incombe cette importante tâche de désigner ou d'instituer cette autorité. Il n'est donc pas question d'encourager les phénomènes d'autorégulation puisqu'ils ne peuvent garantir efficacement l'impartialité et l'indépendance de l'autorité conformément aux principes directeurs de l'ONU.
- 39 Certains États africains ont déjà bien compris ce principe essentiel de la société de l'information et l'ont mis en œuvre en adoptant des lois relatives à la protection des données à caractère personnel, lesquelles instituent, pour la plupart, un organisme chargé, de façon exclusive, de la protection de la vie privée dans le cadre des différents usages des TIC⁹⁸.
- 40 L'existence d'un tel organisme est évidemment déterminante pour la qualité du dispositif de protection des données personnelles et plus largement de la vie privée à l'heure du développement de l'économie numérique favorisée par les TIC. Le projet de Directive CEMAC sur le cadre juridique de la protection des données à caractère personnel le reconnaît expressément dans son préambule en ces termes : « *la mise en place d'un régime de protection des données à caractère personnel ne sera effective qu'avec la création d'une Autorité de contrôle qui devra assurer cette fonction de contrôle du bon respect de la législation et de la protection de la vie privée en général* »⁹⁹. Ce projet met lui aussi l'accent sur le caractère unique de l'organe de régulation envisagé lorsqu'il prévoit en son article 28 qu'« *il est institué une autorité administrative indépendante appelée l'Autorité de contrôle chargée du respect, sur le territoire national, des dispositions de la présente loi type ainsi que la protection à la vie privée en général* ». Même si ce texte est encore en l'état de

projet, et donc, pas encore obligatoire pour les États membres de la CEMAC, il traduit globalement la logique partagée en cette matière par diverses législations en vigueur dans de nombreux États et communautés d'États. Cette exigence est évidemment une condition d'efficacité du dispositif de régulation. Certes, il peut être nécessaire que, pour des domaines d'activités précis, des régulateurs sectoriels soient institués pour, relativement à leur champ spécial de compétence, réguler certains aspects de la vie privée en lien avec les usages qui sont faits des TIC ; mais il demeure constant que l'existence d'un organe unique, chargé d'assurer la cohérence de l'ensemble du dispositif de régulation et la mise en œuvre harmonisée des principes généraux est une nécessité impérieuse.

- 41 Dans le contexte camerounais cependant, cette nécessité d'un organe unique est ignorée ; et, dans le seul domaine des communications électroniques, deux organes ont été consacrés avec d'ailleurs des compétences définies dans une confusion laissant pressentir l'inefficacité du dispositif.

2) L'existence d'un risque de conflit de compétences entre les régulateurs

- 42 Malgré l'urgence de la question de la régulation des usages des TIC en lien avec la vie privée des citoyens, et les avancées déjà réalisées dans les autres États africains, on a encore l'impression que l'État camerounais « *hésite, tâtonne, jusqu'à donner le sentiment de se laisser déborder* »¹⁰⁰. En effet, en l'état actuel du droit camerounais, il existe une confusion née du fait que deux organes partagent les compétences en cette matière et au final, on a l'impression qu'aucun organe ne joue effectivement ce rôle.
- 43 On pouvait dans un premier temps penser que la fonction de la protection de la vie privée dans l'environnement électronique est assurée par l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC) dans la mesure où d'après le point j de l'article 5 du Décret du 10 avril 2012 qui organise son fonctionnement, elle a, entre autres, pour mission « *de veiller, dans l'usage des TIC, au respect de l'éthique, ainsi qu'à la protection de la propriété intellectuelle, des consommateurs, des bonnes mœurs et de la vie privée* ». Cependant, en regardant de près, on ne saurait dire que, par cette seule disposition, l'ANTIC doit être considérée comme l'organe régulateur du traitement des données à caractère personnel en droit camerounais. Il faut en effet relever qu'en dehors de cette formulation laconique, aucune disposition n'organise les modalités de mise en œuvre de cette mission.
- 44 Pour accentuer ce doute, les textes qui organisent le fonctionnement de l'Agence de Régulation des Télécommunications (ART) lui confient aussi une compétence en matière de protection des données personnelles. C'est ainsi que, de manière générale, les textes la chargent de la régulation, du contrôle et du suivi des activités des opérateurs et des fournisseurs de services des communications électroniques¹⁰¹. Dans ce contexte, elle est non seulement investie de la mission « *de garantir la protection des consommateurs* »¹⁰², mais surtout de réguler le dispositif d'identification des abonnés des terminaux de communications électroniques¹⁰³.
- 45 Même si à première vue, on peut observer que la compétence de cette agence est limitée au domaine des communications électroniques, on conviendra néanmoins que non seulement, c'est l'un des domaines où la problématique de la protection des données personnelles se pose avec acuité, mais aussi, cette mission entre en conflit avec celle dévolue à l'ANTIC chargée de veiller à ce que l'usage des TIC se fasse dans le

respect des « *bonnes mœurs et de la vie privée* »¹⁰⁴. Or, les communications électroniques, régulées par l'ART, procèdent bien de l'usage des TIC. Par ailleurs, le dispositif juridique en vigueur fait bien de l'ART le garant du respect par les prestataires de la vie privée des utilisateurs des réseaux de communications électroniques. À ce titre, l'ART peut sanctionner, soit d'office, soit à la demande d'une organisation professionnelle, d'une association agréée d'utilisateurs ou d'une personne physique ou morale, après constatation ou vérification, les manquements des prestataires à l'obligation de respecter les droits des utilisateurs, dont notamment la violation de leur droit à la vie privée¹⁰⁵. C'est en effet à ce titre que l'ART a, notamment le 22 mai 2014, pris des mesures visant à encadrer l'envoi des SMS non sollicités aux abonnés¹⁰⁶. Il s'agissait pour elle de contenir la propension de cette pratique intrusive affectionnée par les opérateurs et autres prestataires qui, non seulement perturbe la tranquillité des abonnés, mais aussi, procède du traitement de leurs données personnelles. Généralement qualifiée de *spamming*, l'encadrement de cette pratique et le contentieux en résultant sont pourtant officiellement de la compétence de l'ANTIC où il est prévu qu'elle est chargée « *de mettre en place des mécanismes pour régler des litiges d'une part, entre les opérateurs des TIC et, d'autre part, entre opérateurs et utilisateurs, pour les problèmes spécifiquement liés aux contenus et à la qualité de service (spamming, phishing, hacking)* »¹⁰⁷.

- 46 Finalement, on peut bien dire que, sur le plan textuel, ces deux Agences, ANTIC et ART, se partagent les compétences en matière de protection de la vie privée dans la société de l'information sans que l'on puisse véritablement comprendre comment leurs rôles s'articulent dans la pratique. En effet, les risques de conflits de compétence sont si évidents que l'harmonie nécessaire à l'ordre et à la sécurité juridiques est manifestement compromise en ce domaine. On ne peut dès lors que constater le caractère nocif de ce bicéphalisme et, partant, son inefficacité.
- 47 Si l'intention des autorités publiques camerounaises est de faire de l'ANTIC, en ce qu'elle est assure « *la promotion et le suivi de l'action des pouvoirs publics en matière de Technologies de l'Information et de la Communication (TIC)* »¹⁰⁸, l'autorité en charge du contrôle et de la régulation des usages des TIC en lien avec la vie privée, il faudrait alors que ce rôle soit mieux défini, suffisamment précisé et renforcé par un texte législatif. En effet, d'après la Constitution camerounaise, les questions relatives aux droits, garanties et obligations fondamentaux du citoyen et notamment « *la sauvegarde de la liberté et de la sécurité individuelles* » sont du domaine de la loi¹⁰⁹. Par ailleurs, il faudrait notamment instituer, au profit de cette agence, de manière claire, une obligation, à la charge de toute entité responsable d'un dispositif de traitement des données à caractère personnel, soit de déclarer toutes les opérations de traitement qu'elle fait desdites données, soit de solliciter son autorisation avant tout traitement, selon les cas. De même, il faudrait tenir compte de l'usage qui veut que les organismes de protection de la vie privée dans le contexte du numérique joue un rôle consultatif dont la mise en œuvre permet au pouvoir normatif compétent d'intégrer les exigences de protection des données personnelles dans les normes intéressant ces questions au moment même de leur rédaction¹¹⁰.
- 48 Quand bien-même ces dispositions seraient adoptées, on pourrait encore douter que, dans sa configuration actuelle et du fait de ses nombreuses missions variées¹¹¹, cette agence puisse effectivement et efficacement contrôler et réguler la question des données personnelles. En effet, en général, les autorités en charge de la protection de la vie privée dans l'environnement électronique ont pour unique et exclusive mission

cette protection¹¹². Autrement dit, elles se consacrent uniquement et exclusivement à la protection des données à caractère personnel¹¹³, dans tous ses aspects et non de façon limitée comme c'est actuellement le cas au Cameroun.

B.L'inadéquation liée au caractère limité des compétences cumulées par les régulateurs

- 49 Même s'il est vrai que c'est avec le développement des TIC et l'avènement de l'économie numérique que s'est aussi amplifiée la problématique de la protection des données à caractère personnel, force est de reconnaître que c'est souvent loin des réseaux de communications électroniques que des usages, nocifs pour ces données, prennent généralement corps et s'enracinent dans les mœurs. C'est notamment le lieu de préciser que les communications électroniques ne constituent pas les seuls usages dont sont susceptibles les TIC. Dans ce contexte, on ne peut prétendre réguler les données à caractère personnel, en ne mettant sous contrôle que les opérateurs de communications électroniques comme c'est un peu le cas actuellement en droit camerounais. Certes, il a été indiqué ci-dessus quelques principes qui se dégagent notamment de la réglementation bancaire et qui participeraient de la protection des données personnelles. Mais, non seulement, leur nombre est marginal, mais aussi, le contrôle de leur mise en œuvre ne relève spécialement de la compétence d'aucun organe précis. En général la COBAC qui assure la régulation du secteur bancaire dans son ensemble ne se soucie le plus souvent que de la santé financière de ses assujettis ; c'est ainsi que ses différents rapports ne font presque jamais allusion au traitement des données des clients. Par ailleurs, les textes concernés ne prévoient aucune sanction en cas de manquement des établissements assujettis ; ce qui permet de dire qu'au cas même où la COBAC décide de s'intéresser à cet aspect, en l'absence d'une réglementation générale prévoyant des sanctions à prononcer judiciairement, seules seront applicables aux établissements défaillants des sanctions disciplinaires.
- 50 Les textes qui régissent les principaux organes de régulation de l'économie numérique au Cameroun, l'ART et l'ANTIC, ne font pas de ces organismes des régulateurs généraux des questions des données personnelles. Ils sont, au mieux, des régulateurs sectoriels dans la mesure où leurs compétences ont des domaines bien définis. Il est donc évident que, les données à caractère personnel ne sont, dans le contexte camerounais, régulées que de manière très parcellaire.
- 51 Beaucoup d'opérations de traitement des données relatives aux individus ne font aujourd'hui l'objet d'aucun contrôle par l'un ou l'autre de ces régulateurs. À titre d'illustration, les textes ne précisent pas quelle est l'autorité chargée d'assurer le contrôle et la régulation du traitement des données collectées par les administrations en charge de la production des titres identitaires (CNI, Passeport, Carte de séjour, etc.) ?
- 114
- 52 Il faut impérativement un dispositif de régulation générale assis sur une réglementation générale et une autorité régulatrice dotée de pouvoirs généraux lui permettant d'intervenir chaque fois qu'il est question du traitement des données relatives à la vie privée. C'est en effet le lieu d'attirer l'attention des pouvoirs publics sur le danger de multiplier des organes en fonction des secteurs d'activités. Il est bien sûr à craindre qu'une telle approche, si elle était adoptée, aboutisse d'une part à une sorte de hiérarchisation des valeurs des données en fonction des secteurs et surtout le

risque que certains secteurs soient oubliés, d'autre part, une telle approche serait incapable de prendre suffisamment en compte les procédés de l'interconnexion et de l'interopérabilité des données et des bases qui les contiennent et qui structurent les *Big Data*¹¹⁵ qui caractérisent l'époque actuelle. Par l'interconnexion des bases de données, les données circulent, se reproduisent, se conservent, s'agrègent et se corrélient avec celles d'autres bases de données et échappent de ce fait au secteur d'activité d'origine et donc au régulateur sectoriel. Non seulement, les rapprochements de bases de données sont plus nuisibles pour les citoyens¹¹⁶ dont notamment le risque de perdre le contrôle sur les données collectées est plus grand¹¹⁷, mais aussi, elles mettent en lumière les limites de l'approche sectorielle de la régulation des données personnelles.

- 53 Donc, même si les régulateurs économiques sectoriels peuvent avoir un droit de regard sur le traitement que leurs assujettis font des données collectées, il y a impérativement lieu à la mise en place d'une autorité centrale chargée de veiller, de façon harmonieuse cohérente, sur la protection des données personnelles. Telle est un peu l'approche utilisée en droit de la concurrence où, bien que les régulateurs sectoriels soient investis d'une compétence en la matière dans leurs domaines économiques respectifs¹¹⁸, il existe une autorité centrale, la Commission Nationale de la Concurrence¹¹⁹, ayant une compétence générale sur le plan national.

Conclusion

- 54 La révolution numérique est généralement présentée comme un moteur de croissance économique et de développement social ; ce qui suppose qu'elle porte les valeurs humaines en son cœur. Mais, ses différentes applications montrent bien que l'homme et les données qui le caractérisent tendent à devenir des marchandises comme toute autre et, c'est dans une large mesure grâce au marché des données à caractère personnel que cette révolution avance. Certes, il faut bien qu'elle avance, mais surtout, que son but humaniste ne soit pas détourné. Pour ce, le législateur camerounais doit prendre conscience du défi qui l'interpelle pour, dans un premier temps, structurer et ordonner les règles éparses qui existent déjà et, dans un second temps, les renforcer tant sur le plan matériel que sur le plan institutionnel pour favoriser une conciliation adéquate entre les exigences relatives à la dignité humaine et les enjeux du développement numérique. On ne doit pas l'oublier, le vrai développement ne se sert pas de l'homme, mais vise son bien-être. C'est ainsi qu'il convient de souscrire à l'idée selon laquelle « *la protection des données personnelles est un marqueur des sociétés démocratiques contemporaines* »¹²⁰.

NOTES

1. D. Ichbiah, *Comment Google mangera le monde*, L'archipel, nouvelle édition, 2010.
2. D'après *Le Grand dictionnaire terminologique* de l'Office Québécois de la Langue Française, les TIC désignent l'« ensemble des technologies issues de la convergence de l'informatique et des techniques

évoluées du multimédia et des télécommunications, qui ont permis l'émergence de moyens de communication plus efficaces, en améliorant le traitement, la mise en mémoire, la diffusion et l'échange de l'information ». cf. Pdf en ligne.

3. Par exemple, « Une pathologie appelée nomophobie - de l'anglais 'no-mobile phobia' - et présenté comme une peur excessive d'être séparée de son téléphone portable est même en émergence selon un nombre non négligeable de psychiatres », B. Ajang, "Hyper-communication et hyper-connexion numérique : être hyper-vigilant aux excès ?", 23 juin 2017 [en ligne]. Par ailleurs « une étude récente aux États-Unis (3) mesure 40 % de la population adulte présentant une addiction à internet (aux emails, jeux en ligne, contenus interdits aux moins de 18 ans) ». Susan M. Snyder, Wen Li, Jennifer E. O'Brien, and Matthew O. Howard, "The Effect of U.S. University Students' Problematic Internet Use on Family Relationships : A Mixed-methods Investigation," Plos One, 11 décembre, 2015 [en ligne]

4. A. Vitalis, *L'incertaine révolution numérique*, 1 Londres, ISTE Éditions, 2016, p. 28. Par ailleurs pour cet auteur, la vie privée est « essentielle à la vie démocratique » *op. cit.*, p. 107.

5. C'est l'impression qui se dégage de ce questionnement : « La vie privée, une valeur fondamentale menacée ? », Y. Détraigne et A.-M. Escoffier, *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*, Rapport d'information n° 441 (2008-2009), fait au nom de la commission des lois du Sénat (France), déposé le 27 mai 2009 [en ligne].

6. G. Cornu (Dir.), *Vocabulaire juridique*, PUF, 9^{ème} édition mise à jour, 2011, p. 1064.

7. Comme l'écrivait Aristote, le « public » est le « royaume de la liberté » alors que le « privé » est le « royaume de la nécessité ». cf. Y. Estienne, "Un monde de verre : Facebook ou les paradoxes de la vie privée (sur)exposée", In *Actes du 15ème colloque CREIS-TERMINAL - Les libertés à l'épreuve de l'informatique Fichage et contrôle social* - juin 2010 [en ligne].

8. Comme le souligne un rapport au Sénat français, « La notion de vie privée est ainsi, dans une société démocratique, indissociable de l'existence de l'individu et de l'exercice des libertés : la société reconnaît à l'individu le droit de disposer d'un espace privé, distinct de la vie collective de la communauté », Y. Détraigne et A.-M. Escoffier, *op. cit.* [en ligne]

9. Ce Pacte est adopté par l'Assemblée Générale des Nations Unies dans sa Résolution 2200 a (XXI) du 16 décembre 1966 ; il est entré en vigueur le 23 mars 1976, conformément à l'article 49, pour toutes les dispositions à l'exception de celles de l'article 41 (Comité de droits de l'homme) ; et le 28 mars 1979 pour les dispositions de l'article 41, conformément au paragraphe 2 dudit article 41. Il a été ratifié par le Cameroun le 27 juin 1984.

10. Ce texte prévoit : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

11. Art. 17 PIDCP.

12. Cette Convention a été adoptée à Malabo, en Guinée Équatoriale, le du 27 juin 2014, lors de la vingt-troisième session ordinaire de la Conférence de l'Union. Cette Convention n'est pas encore entrée en vigueur à cause du nombre insuffisant des ratifications. En effet, d'après son article 36, elle « entre en vigueur trente (30) jours après la réception, par le Président de la Commission de l'Union africaine, du quinzième (15ème) instrument de ratification ou d'adhésion ». Or, à la date du 3 juin 2019, seuls cinq instruments de ratification sont déjà déposés. v. sur ce point la page dédiée à cette Convention sur le site web de l'Union Africaine.

13. Il faut préciser que d'après l'article 65 de la Constitution de la République du Cameroun, « le Préambule fait partie intégrante de la Constitution ».

14. Cf. art. 41, loi n° 2010-012 relative à la cybersécurité et la cybercriminalité.

15. Cf. art. 305 Code pénal, 12 juillet 2016 : « Est puni d'un emprisonnement de six (06) jours à six (06) mois et d'une amende de cinq mille (5 000) à deux millions (2 000 000) de francs ou de l'une de ces deux peines seulement, celui qui, par l'un des moyens prévus à l'article 152 du présent Code, porte atteinte à

l'honneur ou à la considération d'une personne en lui imputant directement ou non des faits dont il ne peut rapporter »

16. L'article 299 CP réprime la violation de domicile en ces termes : « (1) Est puni d'un emprisonnement de dix (10) jours à un (1) an et d'une amende de cinq mille (5.000) à cinquante mille (50.000) francs ou de l'une de ces deux peines seulement, celui qui s'introduit ou se maintient dans le domicile d'autrui contre son gré. (2) Les peines prévues à l'alinéa 1 ci-dessus sont doublées si l'infraction est commise pendant la nuit ou à l'aide des menaces, violences ou voies de fait. (3) La poursuite ne peut être exercée que sur plainte de la victime ».

17. L'article 300 CP réprime la violation de correspondance en ces termes : « (1) Est puni d'un emprisonnement de quinze (15) jours à un (1) an et d'une amende de cinq mille (5.000) à cent mille (100.000) francs ou de l'une de ces deux peines seulement, celui qui, sans l'autorisation du destinataire, supprime ou ouvre la correspondance d'autrui ».

18. L'Union Internationale des Télécommunications (UIT) définit la révolution numérique comme « le passage de notre société à l'ère de l'information et de la communication reposant sur une immatérialité grandissante des données diffusées à l'échelle mondiale [en ligne]

19. Ce contexte est caractérisé par un risque de confusion. Comme le souligne un auteur en effet, « le numérique permet, en effet, un maillage de la vie publique et privée d'une personne qui est extrêmement fin et qui remet en cause la séparation entre les différents compartiments de sa vie ». cf. É. GEFFRAY, « Comment assurer l'effectivité de la protection des droits à l'ère post-Snowden ? », in A. Grosjean (Dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1^{ère} édition, Larcier, Coll. Création Information Communication (CIC), 2015, p. 21.

20. « Dans une société libre, chaque individu a deux vies : sa vie publique et sa vie privée ». Cf. F. Terré, « La vie privée », in Tabatoni, *Société de l'information et vie privée*, Tome 3, PUF, 2002.

21. La vie privée garantit la possibilité de l'existence d'un espace public. Cf. A. Vitalis, *L'incertaine révolution numérique*, 1 Londres, ISTE Éditions, 2016, p. 28. Par ailleurs pour cet auteur, la vie privée est « essentielle à la vie démocratique » op. cit., p. 107.

22. Cf. M. Untersinger, *Anonymat sur internet, protéger sa vie privée*, 2^{ème} édition, Eyrolles, 2014. Pour cet auteur, « l'équilibre entre vie privée et vie publique tend à s'inverser : publier ne coûte rien, préserver sa vie privée requiert des efforts ».

23. Il a été jugé que l'activité professionnelle est « placée sur la scène publique » (Paris 16 mars 1966, D. 1966, 749), car elle participe à la vie de la cité et ne relève pas, semble-t-il, en soi de la vie privée (V. TGI Bayonne, réf., 29 mai 1976, JCP 1976, II, 18495, note R. Bonnais). Cf. F. Terré, « La vie privée », in P. Tabatoni, *Société de l'information et vie privée*, Tome 3, PUF, coll. Cahiers Académie sc. morales et politiques, 2002, p. 143.

24. Cass. Soc, Arrêt n° 4164 du 2 octobre 2001, 99-42.942, Société Nikon France SA C/ M. X, *Recueil Dalloz* 2001 p. 3148. Dans cet arrêt, la Cour de cassation décide que Le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; et que, par voie de conséquence, l'employeur ne peut prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur.

25. Le teint d'un individu par exemple.

26. Sur la question, Y. L. Kouahou, *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.

27. « La protection des données personnelles apparaît comme le socle de la protection des personnes dans un univers complexe et numérique ». Cf. I. Falque-Pierrotin, préface d'A. Debet, J. Massot et N. Metallinos (Dir), *Informatique et libertés, La protection des données à caractère personnel en droit français et européen*, Lextenso éditions, coll. Les intégrales, 2015.

28. « Une donnée est une description élémentaire, typiquement numérique, d'une réalité ». Cf. S. Abiteboul, "Sciences des données : de la logique du premier ordre à la Toile", Leçon inaugurale prononcée le jeudi 8 mars 2012. Chaire d'Informatique et sciences numériques.

29. Y. L. Kouahou, thèse précitée, n° 1291 : « La donnée peut se rapporter directement à la personne et c'est le cas des données manifestement personnelles. La donnée peut ne pas se rapporter directement à la personne, mais permettre l'identification de la personne en fonction des moyens d'identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ; ce sont les données indirectement personnelles ».

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

31. 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.

32. Selon la jurisprudence de la CJUE, l'image d'une personne enregistrée par une caméra constitue une « donnée à caractère personnel », au sens de l'article 2, sous a), de la directive 95/46, dans la mesure où elle permet d'identifier la personne concernée (voir, en ce sens, arrêt du 11 décembre 2014, Ryněš, C-212/13, EU :C:2014 :2428, point 22).

33. Dans son ordonnance de référé du 6 avril 2018, le TGI de Paris a considéré que les nom, prénom et coordonnées professionnelles d'un chirurgien-dentiste restaient des données personnelles. Le tribunal explique que « 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 », cf. TGI de Paris, ordonnance de référé du 6 avril 2018, Monsieur X. / Google France et Google LLC, <https://www.legalis.net/jurisprudences/tgi-de-paris-ordonnance-de-refere-du-6-avril-2018/>.

34. Dans un arrêt du 20 décembre 2017, la Cour de justice de l'UE a affirmé que « les réponses écrites fournies par un candidat lors d'un examen professionnel et les éventuelles annotations de l'examineur relatives à ces réponses constituent des données à caractère personnel, au sens de cette disposition ». À ce sujet, la juridiction européenne note que les réponses reflètent le niveau de connaissance et de compétence du candidat, ses processus de réflexion, son jugement et son esprit critique. Par ailleurs, la collecte des réponses a pour but d'évaluer la personne et ses capacités à exercer ce métier. Enfin, l'utilisation de ses données est susceptible d'avoir un effet sur les droits et intérêts de cette dernière. S'agissant des annotations de l'examineur aux réponses du candidat, elles constituent aussi des informations sur le candidat. Cf. CJUE, 2ème ch., arrêt du 20 décembre 2017, M. X. / Data Protection Commissioner [en ligne].

35. L'expression la plus appropriée pour contenir les notions de « vie privée » et de « données à caractère personnel » serait sans doute celle de « sphère privée ». Mais, en retenant juste la notion de « vie privée » dans le cadre de cette étude, l'idée est surtout, de mettre en exergue l'évolution conceptuelle de la notion de « vie privée ». Il faut en effet s'apercevoir qu'en fonction des périodes de l'histoire de l'humanité, cette notion n'a pas toujours eu le même contenu.

36. Cf. I. Falque-Pierrotin, *préc.* : « elle n'est plus seulement limitée à la protection de la vie privée, elle s'émancipe de ce seul objectif pour constituer un but en soi, une protection de la personne dans toute sa complexité, dans toutes ses dimensions, publiques et privées, personnelles ou professionnelles ».

37. Ph. Ariès et G. Duby, *Histoire de la vie privée* (5 volumes), éditions Le Seuil, 1999.

38. Y. Estienne, "Un monde de verre : Facebook ou les paradoxes de la vie privée (sur)exposée", In Actes du 15ème colloque CREIS-TERMINAL – Les libertés à l'épreuve de l'informatique Fiche et contrôle social – juin 2010 [en ligne].

39. E. Suzanne, " Révolution informationnelle et révolution numérique", 8 octobre 2010, [en ligne]. L'UIT définit la révolution numérique comme « le passage de notre société à l'ère de l'information et de la communication reposant sur une immatérialité grandissante des données diffusées à l'échelle mondiale » [en ligne].

40. Cf. Exposé de motifs de la loi sénégalaise n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel.
41. Cf. J.-F. Thery et I. Falque-Pierrotin, Internet et les réseaux numériques : étude adoptée par l'Assemblée générale du Conseil d'Etat le 2 juillet 1998, La Documentation française, 1998, p. 15.
42. Y. Poulet, J.-F. Henrotte, La protection des données (à caractère personnel) à l'heure de l'Internet, in Protection du consommateur, pratiques commerciales et T.I.C., collection Commission Université-Palais, volume 109, pp. 197-245. Cité par Y. Détraigne et A.-M. Escoffier, op. cit. : Les données personnelles sont des informations et « l'information représente pour ceux qui la détiennent un pouvoir vis-à-vis de ceux sur lesquels l'information est détenue. Celui qui détient l'information sur autrui peut adapter sa décision en fonction de la connaissance que l'information collectée et traitée lui donne d'autrui. Il prévoit son attitude et peut donc répondre à sa demande ou influencer celle-ci ».
43. Y. L. Kouahou, 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° 1152 et 1257 notamment.
44. Cf. I. Falque-Pierrotin, *préc.*
45. Y. Détraigne et A.-M. Escoffier, op. cit, [en ligne].
46. Il s'agit des 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.
47. Ce principe signifie que les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime, correspondant aux missions de l'établissement, responsable du traitement. Tout détournement de finalité est passible de sanctions pénales.
48. « La collecte, le traitement, la conservation des données personnelles et leur transmission éventuelle à des tiers doivent s'effectuer de manière loyale. Cela suppose que les données ne soient pas collectées et traitées à l'insu de la personne concernée et que les personnes soient informées de l'identité et du lieu d'établissement de la personne qui traite ces données, des finalités poursuivies, du caractère obligatoire ou facultatif du traitement des données, des destinataires des informations, ainsi que toute information nécessaire à l'exercice de leurs droits ». cf. P. Perez et J. Duchaine, La Commission Nationale de l'Informatique et des Libertés, Principes de la protection des données à caractère personnel, 2009 – actualisation : 2013 [pdf en ligne]
49. Il signifie que les données collectées, quantitativement et qualitativement, doivent être strictement nécessaires à la finalité du traitement. Ainsi, les données collectées ne doivent pas être excessives au regard des objectifs poursuivis.
50. Le titulaire des données objet du traitement doit toujours avoir la possibilité d'accéder ou de se faire communiquer toutes les informations le concernant contenues dans un fichier détenu par le responsable du traitement pour les faire rectifier ou supprimer lorsqu'elles sont erronées. De même, il 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.
51. Ce principe exige du responsable du traitement de prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation à des entités non autorisées. Il s'agit en principe d'une obligation de résultat.
52. Par principe, les données collectées dans le cadre d'un traitement ne doivent pas être conservées de façon indéfinie dans les fichiers informatiques. Le législateur doit toujours fixer une durée de conservation pour préserver le droit à l'oubli.
53. Il s'agit notamment 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 et de la Directive n° 09/08-UEAC-133-CM-18 harmonisant les régimes juridiques des activités électroniques dans les États membres de la CEMAC.

54. Il s'agit essentiellement de la loi n° 2010-012 du 21 décembre 2010 relative à la cybersécurité et la cybercriminalité au Cameroun ; de la loi n° 2010-013 du 21 décembre 2010 (telle que 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 ainsi que leurs règlements d'application.

55. 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.

56. Art. 51, loi n° 2010-013 régissant les communications électroniques.

57. Ne pas divulguer ses identifiants est pour tout citoyen un droit : l'anonymat. On peut en effet observer que ce droit, l'anonymat, « *s'inscrit dans le cadre des droits et des libertés fondamentaux de la personne 'humaine'* » dans la mesure où le droit au respect de l'intimité de la vie privée inclut nécessairement l'anonymat. Cf. E. A. Caprioli, « Anonymat et commerce électronique », in Les premières journées internationales du droit du commerce électronique, Actes du colloque de Nice des 23, 24 et 25 octobre 2000, coll. Actualités de droit de l'entreprise, Litec, 2002, p. 151. Dans la même lancée, il est soutenu que l'anonymat est « *l'ultime rempart de la liberté et de la vie privée* ». cf. E. Davio, « Anonymat et autonomie identitaire sur internet », in *Cahiers du C.R.I.D.*, (Sous la direction de Etienne Montero), *Droit des technologies de l'information, Regards prospectifs*, Bruxelles, Bruylant, 1999, p. 303 s.

58. Idem.

59. Art. 6, décret n° 2013/0399 PM du 27 février 2013 fixant les modalités de protection des consommateurs des services de communications électroniques

60. Il faut cependant relever que le recours à l'anonymat est simplement interdit dans certains cas notamment en cas d'émission des messages électroniques à des fins de prospection (L'article 48 de la loi n° 2010-012 relative à la cybersécurité et à la cybercriminalité).

61. Art. 6, al. 2 *in fine*, 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. Cette disposition est relayée en droit interne par l'article 9, alinéa 2 du décret n° 2013/0399 précité.

62. L'alinéa 1^{er} de ce texte dispose : « *Les opérateurs et exploitants des réseaux de communications électroniques ouverts au public, ainsi que les fournisseurs de services, sont tenus au moment de toute souscription, de procéder à l'identification des abonnés et des terminaux. Ils tiennent à jour des listes d'abonnés* ».

63. 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* ».

64. On peut citer, à titre d'illustration les cas de Monsieur Ferdinand Ngoh Ngoh (Secrétaire général de la Présidence de la République) ou de Charles Ndong (Directeur général de la CRTV). Cf. D. Mbouwe, « Cameroun : cybercriminalité sur facebook, voici les faux comptes de personnalités qui servent à arnaquer », [en ligne, consulté le 07 novembre 2011].

65. Voir par exemple, l'un des cas les plus récents, le communiqué du 26 juillet 2017 signé de Monsieur Louis Paul Motazé, MINEPAT, dans lequel il précise n'avoir « *jamais possédé de compte Facebook et met en garde tous ceux qui seraient tentés ou sont déjà entrés en communication avec ces faux profils* ». On pourra encore citer le communiqué du 26 septembre 2015 signé de son directeur de cabinet des services du Premier Ministre dénonçant l'usurpation de l'identité de ce dernier ; ou encore le communiqué du 16 février 2016 dénonçant l'usurpation de l'identité du Monsieur Basile Atangana Kouna, Ministre de l'eau et de l'énergie, sur le réseau Facebook.

66. Notamment, sur le fondement de l'alinéa 4 de l'article 74 de la loi n° 2010/012 relative à la cybersécurité et à la cybercriminalité dispose : « (4) Est puni d'un emprisonnement de six (06) mois à deux (02) ans et d'une amende de 1.000.000 (un million) à 5.000.000 (cinq millions) F CFA ou de l'une de ces deux peines seulement, le fait de collecter par des moyens illicites, des données nominatives d'une personne en vue de porter atteinte à son intimité et à sa considération ».

67. Cf. TGI, Paris, 17^{ème} chambre correctionnelle, jugement du 24 mars 2015, V. P. et F. Z. / A. S. et K. G.
68. Cf. Art. 74 ; al. 7 loi n° 2010/012 précitée : « *Est puni d'un emprisonnement de six (06) mois à deux (02) ans et d'une amende de 5.000.000 (cinq millions) à 50.000.000 (cinquante millions) F CFA, ou de l'une de ces deux peines seulement, celui qui conserve des informations sous une forme nominative ou chiffrée au-delà de la durée légale indiquée dans la demande d'avis ou la déclaration préalable à la mise en œuvre du traitement automatisé* ».
69. Art. 16, Directive CEMAC n° 07-08 précitée.
70. Art. 17, Directive CEMAC n° 07-08 précitée.
71. Il ressort du projet de directive CEMAC relative à la protection des données à caractère personnel que « 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 ».
72. Cour d'appel de Paris, Pôle 4 – Ch. 11, arrêt du 15 septembre 2017, M. X. / Weezevent.
73. Art. 74, al. 1, loi n° 2010-012 précité : « *Est puni d'un emprisonnement de un (01) à deux (02) ans et d'une amende de 1.000.000 (un million) à 5.000.000 (cinq millions) F CFA, quiconque, au moyen d'un procédé quelconque porte atteinte à l'intimité de la vie privée d'autrui en fixant, enregistrant ou transmettant, sans le consentement de leur auteur, les données électroniques ayant un caractère privé ou confidentiel* ».
74. Quelques illustrations : filmer quelqu'un dans un lieu réservé sans son opposition vaut-il autorisation de diffusion sur des réseaux sociaux ? Enregistrer les moments intimes passés avec un ami et avec son consentement vaut-il autorisation de publication de la vidéo ? Pour la cour de cassation française, et en application des articles 226-1 1° et 226-2 du Code pénal français, « *n'est pas pénalement réprimé le fait de diffuser, sans son accord, l'image d'une personne réalisée dans un lieu privé avec son consentement* », donc, seul le consentement initial à être photographié doit être pris en compte. Cf. Cass. Crim., Arrêt n° 780 du 16 mars 2016 (15-82.676).
75. cf. A. Debet, J. Massot et N. Metallinos (Dir), *op. cit.*, n° 280.
76. Cf. art. 7, al 1^{er}, loi 2010/021 du 21 décembre 2010 régissant le commerce électronique : « *Est interdite, la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique ou morale qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen* ».
77. Ces quatre fichiers sont : le Fichier des Comptes Bancaires, en abrégé « FCB » ; le Fichier des Incidents de Paiement sur Chèques et sur Cartes de Paiement, en abrégé « FIPCCP » ; le Fichier des Effets Impayés, en abrégé « FEI » et le Fichier des Chèques et Cartes Irréguliers, en abrégé « FCCI ». cf. art. 3, al. 1, Décision du Conseil National du Crédit du 23 janvier 2013 relative au dispositif de centralisation et de diffusion des incidents de paiement au Cameroun.
78. Art. 6, Conseil National du Crédit - Décision du 23 janvier 2013 relative au dispositif de centralisation et de diffusion des incidents de paiement au Cameroun.
79. Cf. La loi n° 2003/004 du 21 avril 2003 relative au secret bancaire.
80. Sur le régime du secret bancaire en droit camerounais, voir notamment H. M. TCHABO SONTANG, « Le régime juridique du secret bancaire en droit positif camerounais », *Juridis périodique*, n° 81, janvier-mars 2010, pp. 47-60.
81. Art. 13 Décision du 23 janvier 2013 précitée.
82. Art. 11, al. 3, Arrêté MINESUP du 11 septembre 2008 portant statut commun des étudiants des Institutions Universitaires publiques du Cameroun. Ce texte prévoit que « *l'étudiant jouit du droit d'accès à son dossier académique personnel ; il peut notamment exiger de l'Administration Universitaire, la clarification, la rectification, la mise à jour, le complément ou le retrait des informations qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte, l'utilisation, la communication ou la conservation est interdite par les lois et règlements en vigueur* ».
83. Art. 5, décision de 23 janvier 2013 précitée.

84. L'article 2 du décret n° 2016/375 Décret du 04 août 2016 fixant les caractéristiques et les modalités d'établissement et de délivrance de la Carte Nationale d'Identité précise bien que la carte nationale d'identité « *est informatisée, biométrique, personnelle et contient une puce électronique* ». Pour sa part, l'article 84 de la loi n° 2012-001 du 19 avril 2012 portant code électoral souligne que la carte électorale est « *biométrique* ».

85. Ledit projet, mis en œuvre depuis janvier 2014 à Yaoundé, la capitale, dans le cadre de sa phase pilote, prévoit l'installation de 1500 caméras et relais de communication dans les 10 chefs-lieux de région ainsi que dans 7 autres zones stratégiques frontalières, notamment dans la région de l'Extrême-Nord en proie aux assauts de la secte islamiste Boko Haram, [Cf. en ligne, consulté le 10 janvier 2018].

86. Cf. E. Wery, « Une société implante des puces RFID sous la peau de ses employés », *Droit et technologies.org*, [publié en ligne le 10/02/2017].

87. Le site internet d'un prestataire permet d'avoir un aperçu des sociétés utilisant de telles technologies : [en ligne, consulté le 10 janvier 2018].

88. Voir une liste non exhaustive à cette adresse, consultée le 10 janvier 2018.

89. En France notamment, la Cour de cassation française a eu à juger que le licenciement d'un salarié pour refus d'utiliser son badge doit être considéré comme sans cause réelle et sérieuse, à défaut de déclaration à la CNIL du traitement automatisé de données à caractère personnel concernant le système de badge dès son installation. Voir Cass soc. 06 avril 2004, RJS 06 /04 n° 787.

90. Loi du 26 mars 2018 relative au renforcement de la croissance économique et de la cohésion sociale assignent un objectif aux entreprises.

91. E. Wery, « Le droit à la déconnexion adopté en Belgique », *Droit et technologies.org*, publié le 19 avril 2018.

92. Ce constat se vérifie notamment avec le Décret n° 2016/375 du 04 août 2016 fixant les caractéristiques et les modalités d'établissement et de délivrance de la Carte Nationale d'Identité et le Décret n° 2016/374 fixant l'organisation, le fonctionnement et les attributions du Centre National de Production des Titres Identitaires.

93. Art. 4, al. 1 Décret n° 2016/374 fixant l'organisation, le fonctionnement et les attributions du Centre National de Production des Titres Identitaires.

94. Cf. Ph. MALAURIE et L. AYNÈS, *Droit des personnes, la protection des mineurs et des majeurs*, 8^{ème} édition, LGDJ, Lextenso éditions, Coll Droit civil, 2015, n° 5.

95. A. Debet, J. Massot et N. Metallinos (Dir), *op. cit.*, n° 8.

96. Il faut souligner que la loi française, informatique et libertés, qui crée la CNIL, est adoptée en France dans un contexte de méfiance vis-à-vis d'un projet gouvernemental qui visait à centraliser tous les fichiers de traitement des données personnelles des français, « le projet SAFARI ». À la suite de la révélation de ce projet par un article de Philippe Boucher publié dans *Le Monde* du 21 mars 1974 : « SAFARI ou la chasse aux Français », le Premier ministre, Pierre MESSMER, nomma une commission chargée de proposer des mesures pour garantir le respect de la vie privée et des libertés face au développement de l'informatique. Le fruit de ces travaux conduisit à l'adoption de la loi du 6 janvier 1978 dite Informatique et libertés qui encadre et régule les opérations relatives aux traitements automatisés. Cf. A. Debet, J. Massot et N. Metallinos (Dir), *op. cit.*, n° 7 et 8.

Le ministère de l'Intérieur comptait ainsi centraliser l'ensemble des renseignements collectés sur le territoire français. L'opinion publique fut alertée. Et, grâce à cet article, les pouvoirs publics furent contraints de réagir.

97. Des études mettent bien en exergue l'idée selon laquelle, à l'origine, la question de la protection de la vie privée participait avant de tout de la protection de l'individu contre les dérives totalitaires de l'État : « Au lendemain de la Révolution, Benjamin Constant montre que, contre la « *liberté des Anciens* » qui pensent que l'homme n'est libre que par sa participation active

au pouvoir collectif, la « *liberté des Modernes* » se conçoit comme la préservation des droits de l'individu et de sa sphère privée face aux immixtions de la puissance publique ». cf. Y. Détraigne et A.-M. Escoffier, *op. cit.* [en ligne].

98. À titre d'illustration : l'article 5 de la loi sénégalaise n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel a mis en place la Commission des Données personnelles (CDP) ; au Gabon, c'est la loi n° 001-2011 du 25 septembre 2011 relative à la protection des données à caractère personnel qui crée, en son article 15, la « Commission nationale pour la protection des données à caractère personnel » en abrégé « CNPDCP » ; au Bénin, l'article 19 de la loi n° 2009-09 du 27 avril 2009 portant protection des données à caractère personnel en République du Bénin a institué la « Commission Nationale de l'Informatique et des Libertés » (CNIL) ; au Burkina-Faso, l'article 26 de la loi n° 010-2004 du 20 avril 2004 portant protection des données à caractère personnel a institué la Commission de l'informatique et des libertés (CIL).

99. Cf. Préambule Directive CEMAC relatif à la protection des données à caractère personnel.

100. cf. S. Enlart et O. Charbonnier, *Société digitale, comment rester humain ?*, Dunod, 2018, p. 6.

101. Art. 36, al. 1, Loi n° 2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun telle que modifiée par la loi 2015-06 du 20 avril 2015.

102. Art. 36, al. 2, Loi n° 2010/013 du 21 décembre 2010 précitée.

103. Cf. Décret n° 2015/3759 Fixant les modalités d'identification des abonnés et des équipements terminaux des réseaux de communications électroniques.

104. Cf. art. 5, j, Décret n° 2012/180 du 10 avril 2012 portant organisation et fonctionnement de l'ANTIC.

105. Cf. art. 21, Décret N° 2013/0399 PM du 27 février 2013 fixant les modalités de protection des consommateurs des services de communications électroniques.

106. Décision n° 086 du 22 mai 2014 fixant les conditions et modalités de lancement par les opérateurs des offres promotionnelles de services des communications électroniques et Décision n° 087 du 22 mai 2014 prescrivant aux opérateurs les modalités d'encadrement des jeux et d'envoi des SMS indésirés par voie téléphonique.

107. Cf. article 5, i) du Décret n° 2012/180 du 10 avril 2012 portant organisation et fonctionnement de l'ANTIC.

108. Cf. art. 4-a, Décret n° 2012-180 du 10 avril 2012 portant organisation et fonctionnement de l'Agence Nationale des Technologies de l'Information et de la Communication.

109. Cf. art. 26 de la Constitution camerounaise.

110. À titre d'illustration l'art. 33 de la loi gabonaise n° 001-2011 du 25 septembre 2011 relative à la protection des données à caractère personnel dispose en son alinéa 4 que la Commission nationale pour la protection des données à caractère personnel « a) est consultée sur tout projet de loi ou décret relatif à la protection des personnes à l'égard des traitements automatisés ; b) propose au Gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques ». Voir aussi, l'article 37, j) de la loi burkinabé n° 010-2004 du 27 avril 2004 portant protection des données à caractère personnel et l'article 16, alinéa 2, f) de la loi sénégalaise n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel.

111. Les nombreuses missions de l'ANTIC sont, entre autres : assurer la veille technologique, administrer et gérer le nom de domaine .cm, assurer la régularité et l'effectivité des audits de sécurité, etc. (art. 6, décret n° 2012/180 précitée).

112. Cf. notamment l'article 15 de la loi gabonaise n° 001-2011 du 25 septembre 2011 relative à la protection des données à caractère personnel et l'article 5 de la loi sénégalaise n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel

113. Pour le cas du Gabon, voir l'article 33 de la loi n° 001-2011 du 25 septembre 2011 relative à la protection des données à caractère personnel ; pour le cas du Sénégal, la Commission des

Données personnelles (CDP) est exclusivement chargée « de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi » (art. 5 loi sénégalaise n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel ; l'article 16 de cette loi énumère dans le détail les composantes de cette mission générale).

114. Le Décret n° 2016-374 du 04 août 2016 fixant l'organisation, le fonctionnement et les attributions du Centre National de Production des Titres Identitaires ne prévoit rien en ce sens.

115. Par l'expression « *Big data* », traduite littéralement par les expressions « *grosses données* », mégadonnées (recommandé), ou encore « *données massives* », on désigne des ensembles de données devenus si volumineux qu'ils dépassent l'intuition et les capacités humaines d'analyse et même celles des outils informatiques classiques de gestion de base de données ou de l'information. Cf. « *Big data* », Wikipédia.

116. Comme l'observe le Conseil d'État français, si toutes les données collectées auprès d'un individu « restaient disséminées auprès des personnes qui les ont recueillies, les risques pour la vie privée seraient sans doute limités », Conseil d'État, *Le numérique et les droits fondamentaux*, Étude annuelle 2014, La Documentation française, 2015.

117. La donnée collectée par l'entreprise X est immédiatement transférée à l'entreprise Y sans que le titulaire de ladite donnée en ait eu connaissance.

118. À titre d'illustration, l'autorité nationale de régulation des communications électroniques a, d'après l'article 5 du Règlement N° 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, entre autres pouvoirs de « *veiller à ce que les actions et les pratiques des opérateurs n'aient pas pour effet d'empêcher, de restreindre ou de fausser la concurrence sur le marché national et/ou sous-régional des communications électroniques* » et de « *sanctionner les manquements des opérateurs à leurs obligations ainsi que les actions et pratiques anticoncurrentielles, dans les conditions précisées à l'article 9 du présent règlement* ».

119. Décret du 13 septembre 2013 fixant la composition, l'organisation et les modalités de fonctionnement de la commission nationale de la concurrence.

120. I. FALQUE-PIERROTIN, *op. cit.*

RÉSUMÉS

La nécessité de protéger la vie privée s'éprouve comme un besoin profond tant pour l'individu pris isolément que pour la société dans son ensemble. Il faut dire que la vie privée se présente comme la condition première à l'exercice des libertés fondamentales en société. Si ce qui précède sonne comme une évidence, il y a cependant lieu de relever que le droit à la vie privée se trouve, du fait de l'invasion du numérique dans les rapports humains, un peu malmené. Tel est notamment le cas en droit camerounais où il apparaît que le cadre juridique des usages des TIC n'est pas suffisamment outillé et nécessite d'être toiletté, complété et réajusté.

The need to protect privacy is felt as a profound need for both the individual in isolation and the society as a whole. It must be said that privacy is the first condition for the exercise of fundamental freedoms in society. While the above sounds obvious, it should be noted that the right to privacy is somewhat abused as a result of the invasion of digital in human relationships.

This is notably the case in Cameroonian law where it appears that the legal framework for ICT uses is not sufficiently equipped and requires grooming, completion and readjusting.

INDEX

Mots-clés : vie privée, données à caractère personnel, TIC, droit camerounais

Keywords : privacy, personal data, ICT, cameroonian Law

AUTEUR

HERVÉ MARTIAL TCHABO SONTANG

Hervé Martial Tchabo Sontang est Maître-assistant, FSJP, à l'université de Dschang. Il est membre de l'Unité de Recherche en Droit, Institutions et Intégration Communautaire (URDIIC) et chercheur dans le domaine du droit du numérique.