Global Scientific JOURNALS

GSJ: Volume 8, Issue 5, May 2020, Online: ISSN 2320-9186
www.globalscientificjournal.com

DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL DES INTERNAUTES EN RDC.

PROTECTION OF PERSONAL DATA OF INTERNET USERS IN THE DEMOCRATIC REPUBLIC OF THE CONGO (DRC)

[1]YENDE R. Grevisse, [2]MADAWA K. Zéphyrin, [3]MBAKWIRAVYO M. Osée, [4]KASIMWANDE K. William, [5]KAKULE L. Thierry et [6]MAHASANO M. Emmanuel.

[1, 2, 3, 4] Département de Sciences Informatique et de Gestion (Facultés Africaines Bakhita), B.P.63 Butembo, Nord Kivu, RD Congo.

[5] Département de Sciences Informatique et de Gestion (Institut Supérieur de Commerce), B.P.178 Beni, Nord Kivu, RD Congo.

[6] Département de droit Public (Université Catholique du Graben), B.P.29 Butembo, Nord Kivu, RD Congo.

RESUME

L'Informatique et Internet en particulier deviennent un moyen de plus en plus indispensable, quasi utilisable dans tous les domaines (communications, commerce, relations sociales, etc.). La grande masse d'information qui circule sur Internet favorise grandement la collecte de données à l'insu de l'utilisateur, leur divulgation à des tiers et le croisement de ces données constitue une possibilité fructueuse pour de potentielles atteintes à la vie privée des utilisateurs. Cet article traite du sujet de la protection des données personnelles dans ses relations avec les TIC dans la société Congolaise. La finalité de la présente étude est la construction d'une approche critique et communicationnelle portant sur un cadre juridique convenable soumis, d'une part, aux évolutions techniques et, d'autre part, à la nécessaire conciliation entre statut et l'utilisation de ces données personnelles par des internautes Congolais. Cette construction s'appuie sur des enquêtes de travaux scientifiques déjà menés ou en cours, comportant des risques apparents et dissimulés dus à l'extraordinaire essor des techniques informatiques.

Mots-clés : Cadre juridique, Protection, Vie privée, Données à caractère personnel, NTIC, Internet, Internaute congolais, RDC…

ABSTRACT

Computer Sciences and the Internet in particular are becoming an increasingly essential means, almost usable in all fields (communications, commerce, social relations, etc.). The large mass of information circulating on the Internet greatly favors the collection of data without the knowledge of the user, its disclosure to third parties and the crossing of this data constitutes a fruitful possibility for potential invasions of the privacy of users. . This article deals with the subject of the protection of personal data in its relations with ICT in Congolese society. The purpose of this study is the construction of a critical and communicational approach relating to a suitable legal framework subject, on the one hand, to technical developments and, on the other hand, to the necessary reconciliation between status and the use of this personal data by Congolese internet users. This construction is

based on investigations of scientific work already carried out or in progress, involving apparent and hidden risks due to the extraordinary development of computer techniques.

Keywords: Legal framework, Protection, Privacy, Personal data, NICT, Internet, Congolese Internet user, DRC…

INTRODUCTION

Depuis que l'internet s'est réformé, passant d'un réseau essentiellement scientifique à l'étonnant moyen de communication, le cadre juridique et la prolifération des modes d'atteinte à l'intégrité des internautes protégeant l'interception des données personnelles doit faire face à des nouvelles épreuves. Toutefois, attribuons le mérite aux divergentes rénovations concourus dans le domaine informatique depuis 20 ans, grâce à certaines pratiques adoptées, qui ont réussi à faire face aux différentes attaques du domaine privé ou du domaine public.

Actuellement, on collecte et on traite des volumes de données de plus en plus considérables sur chacun de nous. Néanmoins, nous sommes aussi acteurs de ces agissements. Il peut s'agir d'informations tout à fait insignifiantes et anodines, mais qui, combinées entre elles et avec d'autres renseignements, peuvent être hautement révélatrices et donner lieu à une menace pour notre vie privée. Les nouveaux outils informatiques apparus ces dernières années, comme les réseaux sociaux ou l'informatique en nuage, nous sont devenus précieux dans notre vie quotidienne et facilitent amplement notre travail, cependant ils peuvent autant présenter des risques pour la protection des données. D'une manière globale, l'internet pose deux types de complications : d'abord, celles qui sont les conséquences liées à l'univers du réseau lui-même telle que l'application d'une loi nationale à un phénomène qui est transfrontalier et/ou la difficulté de connaître l'authentique identité des intermédiaires (en raison de l'abstraction des échanges, des possibilités d'alias et autres « enseignes virtuelles »). Et l'on retrouve inévitablement ces difficultés lorsqu'il s'agit de faire respecter la législation sur la protection des données à caractère personnel.

En ce qui concerne l'application territoriale des lois, la première réponse juridique à la technique fut la création de nouvelles normes, évidemment internationales afin de pallier les éventuelles lacunes d'application des lois nationales dans le cadre des pratiques émergentes des réseaux informatiques. [10] Ainsi, le 24 octobre 1995, l'Union européenne a adopté une directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[18]. Ce texte est complété par une directive spécifique du 15 décembre 1997 visant à assurer un niveau équivalent de protection du droit à la vie privée quant au traitement de données à caractère personnel dans le secteur des télécommunications. A cela s'ajoute la loi du 6 janvier 1978, laquelle rappelle les droits du citoyen qui sont essentiels à la protection de sa vie privée (droit de communication des informations, droit d'accès direct à ces informations, droit de rectification, droit d'opposition, droit à l'oubli des informations collectées).

En République Démocratique du Congo, Ces directives, n'ont toujours pas été transposées dans leur droit interne alors même que le système congolais semble plus protecteur et très scrupuleux en cas de délit. Cependant, si l'État congolais constitue le produit d'une évolution historique dans l'organisation de sa communauté, il est également la figure à même de produire un ordre social dont l'objet est de réguler ce qui précisément ne peut être régulé par la sphère privée. En effet, les données personnelles sont des informations qui permettent d'identifier distinctement, de manière directe ou indirecte, une personne physique. Il s'agit donc de données qui portent sur des éléments qui déterminent une personne, et qui sont ainsi susceptibles d'affecter la vie privée de celle-ci.

Dès lors, ces données étant ainsi considérées, on peut interpréter que la requête d'une certaine protection de ces données se heurte à une autre exigence, celle consistant à les mettre à la disposition de l'État dans une certaine mesure, afin que les autorités publiques puissent garantir efficacement le maintien de la sécurité. Et même si ces considérations ne sont pas nécessairement inconciliables, il est

clair que l'on soit en présence de deux actions dont la disposition exclusive est bien différente puisque l'une privilégie l'intérêt de la personne tandis que l'autre tend à suspendre cet intérêt au profit d'un intérêt sans doute plus général tenant à la sécurité. Cette notion de sécurité peut, en plus, être largement entendue et recouvrir la sécurité des individus comme celle de l'État congolais lui-même. On voit bien qu'il est tout à fait possible de décliner sous plusieurs angles l'étude sur les données personnelles compte tenu de l'ampleur des enjeux, mais aussi de la relative incertitude autour des discours et des concepts concernant cette problématique[12].

La finalité de cette recherche est la construction d'une approche critique et communicationnelle portant sur un cadre juridique convenable soumis, d'une part, aux évolutions techniques et, d'autre part, à la nécessaire conciliation entre statut et l'utilisation de ces données personnelles au sein de la société congolaise. Cette construction s'appuie sur des enquêtes de travaux scientifiques déjà menés ou en cours, comportant des risques apparents et dissimulés dus à l'extraordinaire essor des techniques informatiques. […] Dans cette perspective, nous présenterons la complexité de la protection des données personnelles basée sur ses aspects constitutifs et à l'altérité apportée par l'emploi généralisé des systèmes informatisés combinée à la digitalisation des données. C'est pourquoi, qu'il est plus enthousiasmant de focaliser nos interrogations sur la dynamique systémique en matière de traitement des données personnelles, tout en examinant l'impact des exigences sécuritaires, en tenant compte de l'espace congolais. A la fin de la présente étude, nous proposerons également un cadre règlementaire pouvant être adopté dans la législation congolaise pour une application adéquate des divers traitements de données à caractère personnel en RDC.

I. REGARD SUR LE DOMAINE A CARACTERE PRIVE

I.1. CONTEXTE DE LA SPHERE PRIVEE

Les notions liées à la vie privée peuvent péniblement être engagées sans s'intéresser aux divergentes significations du terme *« personnel ou individuel »*. En effet, ce mot semble être considéré comme recouvrant un certain nombre de concepts liés suivant leur culture et leur point de vue, cependant, il désigne communément, ce qui est relatif au droit à la vie privée (*right of privacy)* ou la protection de la vie privée (*privacy protection).*

La mention du concept de « *vie privée ou privacy »,* éveille chez tout un chacun un ensemble de problématiques liées à la vie quotidienne ou à la perception de procédés techniques liées à un certain contexte professionnel. Ainsi, la capacité à cacher un certain nombre de choses sur soi au public en général, à des collègues, à des connaissances, relève nécessairement du droit à la vie privée. Ces choses telles que la notion de surveillance des activités d'un individu, l'enregistrement ou le traitement d'informations le concernant, le fait d'entrer en communication avec lui sur la base des résultats d'un tel traitement sont autant d'actions en lien étroit avec la notion de la sphère privée. Le concept semble donc composite et par conséquent difficile à cerner. Néanmoins, certains auteurs ont proposé des définitions très restreintes dont on peut se demander si elles correspondent vraiment à cette vision naïve et intuitive de la vie privée :

— En 1967, **Alan Westin** définit ainsi le terme « *privacy* » [1], comme « *un droit d'un individu à déterminer par quel moyen, à quel moment et quel type d'informations le concernant, doit être communiqué aux autres* »

— En 2006, **Günter Müller**[16], adopte un point de vue assez similaire mais plus abstrait en définissant ainsi le terme « *privacy* », comme *« une possibilité de contrôler la distribution et l'utilisation des données personnelles*».

Ces deux auteurs précédemment cités, paraissent limiter la notion de vie privée à une diffusion maîtrisée d'informations et donc, à une question de gestion des flux d'informations se rapportant à soi. Cependant, d'autres auteurs, en l'occurrence de **Sara Baase** propose dans son livre

« *The gift of fire* » [37], une acception légèrement divergente et plus parlante, suivant laquelle le mot « *privacy »* peut signifier indistinctement :

— L'absence d'intrusion ;
— Le contrôle des informations nous concernant ;
— L'absence de surveillance.

Ceci posé, nous pouvons dorénavant théoriser certaines définitions liées à la vie privée à partir des éléments déjà recueillis, afin de faire référence par la suite à des concepts clairs et distincts ; Plutôt que d'utiliser le terme de « *vie privée* » qui, peut s'avérer assez vague à cause même de son caractère intuitif. Saisissons ainsi :

— **Sphère privée-** La sphère privée d'un individu est l'ensemble des informations se rapportant à lui-même, qu'il considère comme sensibles et donc dignes d'être protégées. Cette sphère est personnelle (*l'individu est le propriétaire des informations qu'elle contient*), personnalisable (*l'individu décide des informations qu'elle contient*), dynamique (*les informations peuvent y être ajoutées ou en être retirées*) et dépendante du contexte (*les informations qu'elle contient peuvent, en nature et en nombre, dépendre du temps, des activités de l'individu ou d'autres paramètres*). De manière brève, la sphère privée encapsule donc toutes les informations, explicitement représentées ou non, qui nous concernent et que nous souhaitons protéger pour quelque motif que ce soit.

— **Droit à la vie privée -** Le droit à la vie privée d'un individu est sa prétention aux caractères personnel, personnalisable, dynamique et contextuel de sa sphère privée ainsi qu'au contrôle de la diffusion, de l'utilisation et de la conservation des informations contenues dans sa sphère privée, quelles que soient la représentation de ces informations et la localisation de cette représentation. De manière succincte, le droit à la vie privée la notion de propriété des données, fortement liée à celle du contrôle.

— **Protection de la vie privée-** La protection de la vie privée est l'ensemble des mesures techniques visant à assurer le respect du droit à la vie privée.

I.2. CONTEXTE DES DONNEES A CARACTERE PERSONNEL

[35] Les données à caractère personnel, sont tous types d'informations qui se rapportent à une personne physique, c'est-à-dire à un individu, et qui permettent de distinguer celui-ci, directement ou indirectement, d'un ensemble de personnes… Il peut s'agir d'un simple numéro d'identification (téléphonique) ou de caractéristiques identitaires, qu'elles soient physiques, économiques ou sociales. A cela s'ajoute également des enregistrements audio ou vidéo qui peuvent aussi constituer des données à caractère personnel dès lors que la personne qui en est l'objet peut être identifiée. Par contre, le traitement des données, fait référence à toute forme d'opération entièrement ou partiellement automatisée, mais aussi manuelle, qui peut être appliquée à des données personnelles, à condition qu'elle soit méthodique et que ses résultats soient consignés systématiquement, telle que la collecte, le tri, la consultation, la diffusion et la destruction de données qui sont autant d'exemples d'opérations de traitement des données. Ce qui appartient au responsable du traitement des données personnelles de signaler les opérations dont elles font l'objet. Toutefois, Certaines catégories de données nécessitent une attention particulière, car leur traitement peut avoir des répercussions sur le droit à la vie privée. Ces informations dites « sensibles » bénéficient d'un plus haut degré de protection. Il s'agit des informations telles que :

— celles qui révèlent l'origine raciale ou ethnique ;
— les opinions politiques ;
— les convictions religieuses ou philosophiques ;
— l'appartenance syndicale ;
— les informations sur la santé ou sur la vie sexuelle.

Ici, on peut constater que Le règlement de la Com35mission Européenne n° 45/2001[] s'applique à la fois aux informations consignées sur papier qu'à celles traitées par des moyens électroniques ; et préconise que les données à caractère personnel soient uniquement rassemblées à des fins légitimes et ne doivent pas être conservées au-delà de la période nécessaire à l'objet de leur collecte, sauf pour des finalités historiques et archivables.

A titre illustratif, les données à caractère personnel peuvent être votre nom, votre date de naissance, votre photo, votre adresse électronique, votre numéro téléphonique ou encore le numéro d'une pièce d'identité. Le traitement de ces données doit être justifié par une finalité précise et doit répondre à une nécessité (par exemple l'exécution d'un contrat ou d'une autre obligation juridique) ou recueillir l'approbation de la personne concernée. Les données qui font l'objet de l'opération doivent être actualisées et leur nombre ou leur importance ne doit pas être excessifs par rapport à l'objectif poursuivi. Celui-ci doit d'ailleurs être fixé préalablement à l'opération de collecte des données et ne peut pas être modifié par la suite, sauf si des règles internes permettent cette modification. En outre, les données à caractère personnel doivent être mises à jour autant que nécessaire et le responsable du traitement doit y veiller, de même qu'il doit permettre aux personnes concernées d'accéder à leurs données au moment opportun. Ainsi, pour éviter toute confusion, au moment de la collecte des données, le responsable du traitement doit communiquer les informations suivantes à la personne concernée :

- l'identité du responsable du traitement ;
- la finalité de ce traitement ;
- les tiers éventuels auxquelles les données seront divulguées et les éventuels transferts de données envisagés ;
- la possibilité pour la personne concernée d'accéder à ses données, de les rectifier, de les verrouiller, d'en demander l'effacement et de s'opposer à leur traitement.

II. PROTECTION DES DONNEES A CARACTERE PERSONNEL

Cette partie sera principalement consacrée à tous les éléments ayant traits au protectorat des données à caractère personnel des internautes sur Internet. Nous essaierons de caractériser comment cet aspect distinctif est traité de manière étendue, nous analyserons également quelques-unes des nombreuses propositions techniques s'y rapportant et le mettrons en lien avec les domaines applicatifs déjà identifiés pour la protection de la sphère privée en général.

II.1. LES 6 AXES DE LA PROTECTION DES DONNEES PERSONNELLES

L'analyse des textes légaux et réglementaires (ainsi que des recommandations que l'on peut couramment observer dans les chartes d'utilisation de systèmes informatiques) nous a permis de classer en six axes les éléments constitutifs des réglementations en matière de protection des données personnelles. Cette classification vient compléter, de manière transversale, les « critères communs » fixés par la norme ISO/IEC 15408-2, publiée en 1999, décomposant la protection des données personnelles en quatre critères techniques évaluables que doit respecter un système[20] :

- La possibilité pour l'utilisateur d'agir de manière anonyme, de manière qu'aucun autre utilisateur ne puisse l'identifier ;
- La possibilité d'agir sous un pseudonyme, interdisant l'identification directe par les autres utilisateurs mais permettant tout de même de relier l'utilisateur à ses actions ;
- L'impossibilité pour les autres utilisateurs d'établir des corrélations entre les différentes activités de l'utilisateur ;
- La non-observabilité, interdisant aux autres utilisateurs de pouvoir décider si une action est en cours.

Ces « critères » expriment les conditions que doit respecter un système pour garantir la protection de la vie privée de ses utilisateurs, sans toutefois caractériser cette protection elle-même. Nous proposons une classification qui identifie six axes, suivant lesquels une autorité (comme un système législatif) peut émettre des exigences sur la protection des données personnelles. À la différence de l'ISO/IEC, qui a par essence un rôle normatif, nous ne présageons pas de l'étendue de ces exigences, mais exclusivement de leur nature, car notre but étant de pouvoir décrire des réglementations. Néanmoins, à titre d'illustration, nous vous présentons l'essentiel des six axes des éléments constitutifs des réglementations en matière de protection des données personnelles :

— **Information -** Le premier axe réglementaire concerne l'information de l'utilisateur. Dans tous les textes étudiés, on impose au responsable d'un traitement informatique portant sur des données personnelles d'informer les propriétaires de ces données d'un certain nombre de caractéristiques de ce traitement. Typiquement, le type d'information fourni est défini par les cinq autres axes réglementaires. Une réglementation peut par exemple imposer que lorsqu'un traitement mettant en jeu des données personnelles a lieu, les propriétaires de ces données soient informés de la nature du traitement.

— **Consentement -** Le deuxième axe réglementaire concerne l'accord, exprimé par le propriétaire des données, à la collecte et au traitement de ses données personnelles. Dans les textes étudiés, ce consentement est qualifié suivant les cas d'explicite ou indubitable. Dans la législation européenne, le « *consentement opt-in* » est de rigueur, c'est-à-dire que par défaut l'on considère que l'utilisateur n'autorise pas le traitement. Bien évidemment, les textes légaux prévoient (pour le consentement comme pour certains autres axes) des exceptions dans les cas mettant en jeu la santé publique, la sécurité nationale, l'instruction des affaires judiciaires [...]

— **Modification -** Ce troisième axe, regroupe plusieurs concepts liés. C'est à cet axe qui est rattaché le droit d'accès et de modification initialement introduit par la loi 78-17 ainsi que toute réglementation visant à donner à l'utilisateur les moyens de demander une mise à jour ou une suppression des informations personnelles collectées. Les réglementations en la matière sont généralement de deux ordres : la nécessité pour l'utilisateur de disposer d'un moyen d'effectuer de telles requêtes auprès du responsable du traitement, et l'obligation (généralement conditionnelle) pour ce dernier d'y accéder.

— **Justification -** Ce quatrième axe est de loin le plus complexe des six. Il a pour vocation de regrouper les réglementations traitant de la question de fond : « est-il justifié de collecter telle donnée et de l'utiliser dans le cadre de tel traitement ? ». Cet axe se réfère donc aux notions de finalité, de proportionnalité et de minimisation des données, principalement abordés par la directive européenne de 1995[40]. Les réglementations s'y rapportant auront donc notamment pour objet la restriction du type d'information collectée en fonction du traitement déclaré et l'encadrement de la réutilisation des informations collectées pour d'autres traitements. Les règles édictées en la matière sont souvent très dépendantes du domaine d'application, puisqu'elles ont pour but de signifier quel type d'information peut être utilisé pour quel type de traitement.

— **Conservation -** Le cinquième axe traite de la conservation des données personnelles après leur collecte. Les textes posent des limites (en général supérieures, parfois inférieures) aux durées de conservation en fonction du contexte : statut des acteurs, nature des données et des traitements. Dans le cas général, la législation européenne prévoit que les données personnelles ne doivent pas être conservées « plus longtemps que nécessaire », les modalités de cette règle générique étant précisées dans des cas particuliers ou laissées aux soins d'autres autorités de réglementation (contrats, réglementations sectorielles, textes de loi plus spécifiques...).

— **Transmission -** Le sixième axe concerne la transmission à des tiers des données déjà collectées. Les réglementations en la matière autorisent, interdisent ou limitent cette transmission (qui peut éventuellement prendre la forme d'une transaction commerciale). La règle générale veut que de telles transmissions soient interdites, à moins que l'utilisateur n'y ait expressément consenti.

Encore une fois, des exceptions sont ménagées pour permettre notamment la transmission de données personnelles aux pouvoirs exécutif et judiciaire lorsque cela est nécessaire.

II.2. LES MENACES DES DONNEES A CARACTERE PERSONNEL

Toutes les menaces relatives à la vie privée tournent au tour de l'utilisation non autorisée et/ou malveillante des données collectées (d'une manière légale ou illégale). Ces menaces peuvent être :

— **Divulgation des données personnelles (***Atteinte à la réputation et à l'intimité***) -** Avec l'émergence des réseaux sociaux, les services de partages des photos et des vidéos, trouver et accéder à des informations personnelles est devenu une opération très simple. Des informations comme la date de naissance, l'emploi, la situation familiale, les préférences musicales, les informations comportementales, etc. qui sont considérées par la majorité d'entre nous comme triviales et inoffensives peuvent être utilisées contre nous. En accédant à ces informations, les risques de préjudice, d'inégalité, de discrimination et de perte d'autonomie apparaissent facilement, les exemples dans ce cadre ne manquent pas[8]. Par exemple, nos amis et nos proches ont maintenant moins de difficulté à savoir où nous sommes, ce qui cause dans certains contextes des situations gênantes. Aussi les employeurs ont tendance à utiliser des informations en ligne pour éviter d'embaucher des personnes qui correspondent à certains profils. Si les informations divulguées sont sensibles, on peut faire face à des situations plus délicates, qui touchent directement la dignité et réputation, et arrivent jusqu'au harcèlement et chantage.

— **Vol et usurpation d'identité -** Le vol d'identité est l'un des crimes qui connaît la plus forte croissance. On peut considérer qu'il s'agit d'un vol d'identité, chaque fois qu'un criminel s'empare d'une partie des données d'une personne et les utilise à son propre profit. Étant donné que de nombreux organismes privés et gouvernements conservent des informations sur les individus dans des bases de données accessibles, les voleurs ont une occasion inépuisable de les récupérer et de les utiliser à mauvais escient. En général, le vol d'identité comporte le vol du numéro de sécurité sociale, du numéro de carte de crédit ou d'autres informations personnelles dans le but d'emprunter de l'argent, de faire des achats et d'accumuler des dettes. Dans certains cas, les voleurs retirent même de l'argent directement du compte bancaire de la victime[41]. Au-delà des pertes financières, il peut y avoir d'autres conséquences importantes et graves pour les victimes. Par exemple, si une personne utilise l'identité d'une autre personne pour commettre un crime. La victime peut se retrouver dans le cadre d'une enquête criminelle, et dans la difficulté de prouver son innocence. Et cela sans compter les effets désastres que cette incidence peut causer sur son état psychologique et mental et ces relations professionnelles et sociales.

— **Le Profilage -** Le profilage désigne le fait de compiler des dossiers d'information sur des individus afin de déduire des intérêts et des caractéristiques par corrélation avec d'autres profils et données[22]. Les informations utilisées dans le profilage contiennent : des données identificateurs tels-que : les adresses IP, les numéros d'identification des navigateurs web et les systèmes d'exploitations, etc. Et des données concernant les activités et le comportement des utilisateurs sur Internet, comme : les requêtes sur les moteurs de recherche, les sites visités, les relations et les communications sur les réseaux sociaux, les produits achetés sur Internet, etc. Le profilage n'est pas une menace en soi, il y a des grands avantages de l'utilisation de cette technique dans plusieurs domaines. Les systèmes de recommandation qui proposent aux clients des produits et des services qui correspondent à leurs préférences et leurs intérêts, est un bon exemple de l'utilisation bénéfique de cette technique. Le profilage devient une menace sur la vie privée dans deux cas où premièrement, si les données utilisées dans le profilage sont collectées d'une manière illégale en utilisant les diverses techniques de tracking et de surveillance. Deuxièmement, si les profils issus après le traitement des données collectées, sont utilisés pour des mauvaises fins, comme la discrimination par les prix, les publicités non sollicitées et nuisibles, les spams, etc.

II.3. LES TECHNIQUES D'ATTAQUES

Quel que soit le type de menace sur la vie privée, cette dernière commence soit par une collecte ou un accès non autorisé à des données personnelles, ou par des inférences faites à partir de la combinaison des données publiques provenant de plusieurs sources (ex. Liste des électeurs). Cette rubrique sera consacrée à présenter les techniques d'attaques les plus utilisées. Nous introduisons, en particulier, les techniques à base de :

— **Les Malwares -** Un malware désigne usuellement, une famille de programmes conçus à des fins malveillantes. Ces fins peuvent exécuter des programmes intrusifs, détruire des données, voler des informations sensibles et compromettre la crédibilité et la disponibilité de l'ordinateur, smartphone ou tablette de la victime. Cette famille de programme peut inclure les virus, les vers, les chevaux de Troie, les Spywares, les Bots, les Rootkits, les Ransomware[25], etc. Tous ces types de programmes sont largement utilisés pour l'accès non autorisé, le vol des données personnelles et sensibles, ainsi que les publicités non sollicitées et nuisibles [...] Notons que malgré les solutions anti-Malwares fournies par les grandes firmes de sécurité informatique (*Kaspersky Lab, Symantec, McAfee, etc.*), la détection et l'élimination des malwares restent toujours une problématique ouverte et un domaine actif de recherche[23].

— **Les Cookies -** Les cookies sont des petits fichiers texte qui résident sur les appareils des utilisateurs du Web. Les informations qu'ils contiennent sont définies et accessibles par les serveurs les sites Web visités. Dans leur principe de conception, les cookies sont conçus pour améliorer et faciliter l'expérience de navigation des internautes. À travers les cookies, les serveurs peuvent se souvenir et identifier certaines informations concernant les utilisateurs. Ces informations peuvent être : la date de visite, les items consultés et achetés, les préférences de configuration comme la langue et l'affichage, les scores de jeu, etc. mais aussi des informations sensibles telles que les mots de passe et les numéros de cartes de crédit. Le problème est que les cookies peuvent également être utilisés pour le tracking, l'enregistrement et l'analyse du comportement des utilisateurs. D'ailleurs, les cookies sont considérés comme étant la méthode de tracking la plus répandu[36]. Le problème provient particulièrement de ce qui est appelé les « **cookies tiers** »[1]. Un autre problème provient[24] des « **cookies de session** »[2].

— **Le Phishing** - L'hameçonnage (Le phishing) est considéré comme l'une des attaques les plus répandues, entraînant des pertes financières importantes pour les entreprises et les utilisateurs. La méthode la plus utilisée pour réaliser ce type d'attaque est à travers des e-mails frauduleux. Ces derniers, redirigent les victimes vers des sites et des liens forgés pour ressembler au maximum les sites cibles au phishing.

— **Attaques par Inférence** - On désigne les « attaque par inférence » par toute tentative d'inférer des nouvelles informations personnelles en combinat des données public et non sensibles comme les listes des électeurs, des données anonymisées (ex. par simple suppression des données nominatives : nom, prénom, NSS, ou par des techniques plus avancées) ainsi que des connaissances auxiliaires. Les techniques d'inférences sont diverses et variées, les principales catégories de ces techniques sont : les méthodes statistiques et probabilistes, les méthodes à base de Datamining et d'intelligence artificielle et les techniques de chaînages qui consistent à relier les enregistrements de deux ou plusieurs bases de données différentes contenant un ensemble

[1] L'origine de ces derniers est les composants tiers qui se trouvent dans la majorité des sites web populaires. Ces composants peuvent être des images, des pixels, des bannières publicitaires, ou bien d'autres formes de composants comme les boutons Facebook et Twitter. À chaque fois qu'un utilisateur visite une page Web contenant des composants tiers, les organismes propriétaires de ces derniers, et à travers les cookies, peuvent faire le lien entre l'utilisateur et la page visité. La collaboration entre les organismes tiers dans le cadre des réseaux publicitaires permet de construire un profil assez complet sur les préférences et les habitudes des utilisateurs du Web.

[2] Ce type de cookies permet à un site Web de garder une trace des mouvements des utilisateurs de page en page, l'objectif est de faire éviter les utilisateurs de fournir chaque fois les mêmes informations déjà fournies sur le site. Des informations comme : les items mis au panier, les achats validés et surtout les détails de l'authentification. En utilisant des techniques à base d'injection de code, comme le Cross-site scripting (XSS), un attaquant peut voler un cookie de session. Cela lui permet de se connecter à un site Web protégé par un nom d'utilisateur et un mot de passe et exécuter par la suite des actions malveillantes.

d'individus en commun[26]. Les attaques par inférences peuvent cibler les différentes types de données : les micro-données (tables contenant des informations structurées sur les individus comme l'âge, l'adresse, le niveau d'études, le statut professionnel, etc.), les données transactionnelles (ex. les enregistrements des clients et leurs achats) ainsi que les données spatiotemporelles (données de géolocalisation des individus et leurs déplacements). Les inférences faites sur ces types de données et qui menacent la vie privée des individus sont énormes.

II.4. TECHNIQUES DE PROTECTION DE LA VIE PRIVEE

Cette partie est consacrée aux principales technologies et approches de protection de la vie privée. Ces technologies sont principalement :

— **Les systèmes de gestion d'identité**[44] **-** Les systèmes de gestion d'identité sont définis comme étant des systèmes ou des « *Frameworks* » qui administrent la collecte, l'authentification ou l'utilisation des identités et les informations liées à ces identités[30]. Toutes ces opérations impliquent la divulgation de beaucoup d'informations personnelles pour assurer l'authenticité et la vérification de l'identité des utilisateurs de système. Cela augmente le risque des menaces sur la vie privée des utilisateurs en élargissant les possibilités de profilage, de suivi des activités des utilisateurs et le vol des informations. Le risque s'accroît encore si un individu utilise plusieurs systèmes avec différents entités de gestion d'identité, ce qui est souvent le cas. Cette situation conduit à un nombre croissant d'identités différentes que chaque utilisateur doit gérer.

Par conséquent, beaucoup de gens se sentent surchargés d'identités et souffrent de la fatigue des mots de passe. Pour renforcer la protection de la vie privée dans les IMS (*Instant Messaging System*), plusieurs solutions ont été proposées. La majorité de ces solutions se basent sur le principe de « Single-Sign-On » [28]. Ce principe repose sur le fait qu'un utilisateur se connecte à un système (le gestionnaire d'identité) et se voit automatiquement accorder l'accès à d'autres services. Plusieurs implémentations de ce mécanisme existent, parmi lesquelles, on peut citer : *OpenID, SAML, Facebook Connect, Microsoft Account, etc*. Malgré que ce type de solutions diminue la dissémination des informations personnelles sur plusieurs entités et évite la gestion d'un grand nombre de comptes en réduisant ainsi le phénomène de «*Mot de passe fatiguant* », un tel système est considéré par les Hackers comme un « *Big Phish* ». Si un Hacker compromet un compte Single-Sign-On, il obtient évidement un accès non autorisé à tous les systèmes liés. D'autres principes en faveur de la protection de la vie privée sont aussi implémentés dans les IMS tels que l'anonymat (pseudonymat), la non-chaînabilité et la minimisation de collecte des attributs identificateurs […] En général, ces principes sont implémentés à l'aide de plusieurs techniques telles que l'identité virtuelle[3] et les accréditations anonymes[4]. De nos jours, il existe plusieurs Systèmes implémentent ces principes, parmi lesquelles on cite : PRIME (*Privacy and Identity Management for Europe*), FIDIS (*Future of Identity in the Information Society*), Liberty Alliance et IDMIX (*Identity Mixer*).

— **Accréditations anonymes -** Les accréditations anonymes est un ensemble de techniques à base cryptographique, permettant à un utilisateur de prouver qu'il possède une propriété ou un justificatif délivré par une organisation (une accréditation), sans révéler quoi que ce soit sur lui-même ou autre information que la possession de l'accréditation. La forme la plus simple d'accréditations anonymes est lorsqu'un utilisateur veut prouver à un vérificateur (ex. fournisseur de service) qu'il possède un ou plusieurs attributs, comme par exemple : son âge exact, son adresse, etc. Dans ce cas, l'utilisateur doit fournir un certificat de la part d'un tiers de confiance (ex. Gouvernement), pour convaincre le vérificateur de l'exactitude des attributs demandés. La

[3] Le concept de l'identité virtuelle consiste à conserver une identité principale et de laisser l'IMS gérer et mapper cette identité à des identités virtuelles en fonction du contexte et de service demandé. Ces identités virtuelles doivent être suffisamment anonymes pour qu'il soit difficile d'établir des liens entre eux.

[4] Les accréditations anonymes sont un ensemble de techniques qui permettent à un utilisateur de prouver un droit d'accès à un service, mais sans révéler son identité ou des informations relatives à son identité.

solution la plus simple est de convaincre le vérificateur qu'un prédicat complexe sur les attributs est valide[17].

— **Communications IP anonymes** - Plusieurs technologies ont été développées pour permettre la non-traçabilité des communications sur un réseau IP, que ce soit pour des applications pair-à-pair fortement distribuées et à accès essentiellement anonymes, ou bien pour des applications client-serveur avec une notion de session très forte […] Les routeurs MIX (proposés par David Chaum), par exemple, permettent de cacher le lien existant entre les messages entrants et sortants, par l'utilisation de bourrage, de chiffrement aléatoire et de brouillage statistique (*émission de messages fictifs*). Ces techniques permettent d'éviter qu'un observateur extérieur puisse relier un message entrant à un message sortant en analysant son contenu ou en étudiant les séquences temporelles d'entrées et sorties.

— **Accès anonymes aux services** - Ce domaine concerne l'anonymisation des messages de l'utilisateur au niveau du protocole applicatif. En effet, dans le cas général la communication entre utilisateur et service comporte beaucoup d'informations identifiantes, et il est parfois possible de limiter la portée de ces informations sans détériorer la qualité du service. Une anonymisation efficace semble donc nécessairement passer par des relais mandataires (proxy) applicatifs chargés d'offusquer les informations sensibles, qui sont souvent spécifiques au service ou à l'application.

— **Autorisation préservant la vie privée-** Il existe des techniques permettant de séparer la phase d'authentification de la phase d'autorisation d'accès, afin que l'utilisateur puisse accéder de manière anonyme au service. Lors de la phase d'authentification, l'utilisateur prouve son identité auprès d'un tiers de confiance (*via l'utilisation d'un login et d'un mot de passe, d'un certificat cryptographique ou d'un challenge quelconque*). Le tiers de confiance peut également, en fonction du type de requête et des exigences des fournisseurs de service, vérifier que l'utilisateur respecte certaines caractéristiques. Le tiers émet ensuite une accréditation (*credential*) affirmant que l'identité de l'utilisateur, ainsi éventuellement que ses autres caractéristiques, ont été vérifiées. L'utilisateur se servira ensuite de cette accréditation (qui ne mentionne pas son identité, mais dont l'authenticité peut être vérifiée auprès du tiers de confiance) pour accéder à des services ou à des ressources. Ce type de protocole, de la même inspiration que le système de jetons d'accès du protocole Kerberos, permet ainsi d'une part à l'utilisateur d'accéder à un service sans dévoiler son identité, et d'autre part au gestionnaire du service de se convaincre que l'intermédiaire de confiance a bien vérifié les caractéristiques requises concernant tous les utilisateurs accrédités.

— **Gestion des données personnelles** - La gestion des données personnelles couvre les dispositifs de protection des données personnelles. Elle concerne notamment la protection des informations de profil, de personnalisation, les préférences utilisateur transmises à une application, les identifiants et les requêtes faites au nom de l'utilisateur. Cette technique fait référence à deux sous-axes : la minimisation de la collecte et l'auto-détermination des données, visant à assurer la protection des données personnelles indépendamment des systèmes et des tiers auxquels elles sont confiées.

II.5. TECHNOLOGIES DE PROTECTION DES DONNEES PERSONNELLES

Des propositions de plus en plus nombreuses sont présentées comme améliorant la protection de la vie privée. Dans cette partie, Nous nous proposons d'analyser les quelques outils et principes que l'on retrouve couramment dans les propositions existantes, et qui diffèrent du simple contrôle d'accès non spécifique à la protection des données personnelles :

— **Platform for Privacy Preferences** – Aussi connu sous le standard « *P3P* » du World Wide Web Consortium[36] est un outil désormais incontournable de la communication des sites web sur leur

politique de protection des données personnelles. Le standard P3P est une spécification de documents XML décrivant les politiques de traitement des données personnelles déclarées par un site web. Ces documents sont conçus pour être accessibles par un navigateur à partir de la page d'accueil du site. L'objectif de ce projet est de rationnaliser la manière dont les sites web communiquent sur leurs traitements. Les données présentes dans un document P3P couvrent les aspects suivants :

- L'identité de l'entité collectant les données ;
- La nature des données collectées ;
- La destination (ou justification) de la collecte de données ;
- L'identification des données pouvant être partagées avec des tiers ;
- L'identification de ces tiers ;
- La possibilité offerte ou non aux utilisateurs de modifier la manière dont leurs données sont traitées ;
- Les méthodes de résolution des conflits éventuels (et le ressort juridique compétent) ;
- La durée de rétention de chacune des informations collectées ;
- Un lien vers une version de la politique lisible par un humain.

Il faut bien comprendre que le standard P3P n'impose aucune politique minimale, il ne fait que fournir le moyen de l'exprimer. De plus, le standard P3P ne permet pas de vérifier que la politique est effectivement appliquée par le site web en question. Cependant, le standard P3P a pour seul objectif de résoudre le problème de l'information de l'utilisateur, à l'exclusion des cinq autres axes de la protection des données personnelles. On peut toutefois noter que les diverses extensions à P3P permettent également de traiter partiellement le problème du consentement de l'utilisateur. En effet, **le langage APPEL** (*A P3P Preferences Exchange Langage*) permet de spécifier des préférences du côté de l'utilisateur. Ainsi, le navigateur est capable de détecter automatiquement (via des moteurs fournis par le W3C) si une politique P3P est conforme aux préférences APPEL, le fait étant alors considéré comme un consentement a priori de l'utilisateur. Ce système est par exemple utilisé dans le cas simple de la décision d'acceptation d'un cookie par un navigateur.

Les concepteurs de systèmes de protection des données personnelles ont tout intérêt à s'appuyer sur le standard P3P, ou en tout cas à demeurer interopérable avec lui. En effet, il permet de résoudre de manière simple le problème de l'information de l'utilisateur, en étant capable de décrire les divers aspects relatifs au traitement des données. Si les listes de choix prédéfinies pour la spécification du type de traitement, de leur justification ou du type de données restent limitées, elles sont extensibles par le biais de schémas XML. De plus, le standard P3P est déjà largement utilisé par les sites web pour leur communication, et de nombreux outils sont capables de manipuler le formalisme d'une manière ou d'une autre. Toutes ces raisons poussent à favoriser au maximum l'interopérabilité avec le standard P3P, préférentiellement à d'autres langages de politiques moins génériques et moins répandus. Toutefois, il faut rester conscient des limitations de P3P. Tout d'abord, la restriction à un rôle d'information (*et éventuellement de consentement*). Enfin et surtout, P3P exprime la politique d'un site web indépendamment de tous les types de réglementations que nous avons pu identifier. Un utilisateur n'a alors aucun moyen de savoir si ces politiques respectent telle loi ou telle directive. Il reste donc ici un travail d'information et de raisonnement à effectuer.

— **Sticky policies** - Comme nous venons de le voir, des outils comme le standard P3P n'assurent pas réellement la protection des données. Une fois qu'une politique de traitement est déterminée, il faut donc que les processus de traitement, de transmission et de stockage des données se chargent de l'appliquer. Cette approche consiste à attacher aux informations sensibles les métadonnées de description de la politique de sécurité associée, et les applications s'engageant à respecter cette « politique collante ». Ces sticky policies[15] ont été introduites par Günter Karjoth et Matthias Schunter en 2002.

— **Gestion déportée des données sensibles** - Des propositions ont également été faites pour permettre aux utilisateurs de profiter de services en ligne tout en évitant à ces derniers de pouvoir tracer leurs activités. C'est un type d'application qui relève donc davantage de l'accès anonyme aux services et des autorisations préservant la vie privée, ainsi que d'autres dimensions de la protection de la vie Privée. Néanmoins, certaines de ces propositions se rapportent plus particulièrement à la gestion des données personnelles de l'utilisateur dans ces scénarios.
C'est le cas notamment du protocole[38] SAML2.0 établi par Liberty Alliance ou du protocole IDsec, établi par l'IETF. Il consiste en la déportation de la gestion des données utilisateur sur un serveur spécialisé, mettant en œuvre des mécanismes de contrôle d'accès sophistiqués, visant à s'assurer du bien-fondé des différentes demandes d'accès au profil qui lui sont faites[5]. Les approches de ce type ont apporté des idées intéressantes, notamment dans le cadre de la gestion des identités virtuelles telle proposée par le projet FC2 (*Fédération des Cercles de Confiances*) par exemple ; mais souffrent de limitations discriminantes. Tout d'abord, la localisation des données personnelles de l'utilisateur sur un serveur délocalisé et clairement identifié pose un problème de sécurité mis en avant par les concepteurs mêmes. C'est par exemple, le serveur gestionnaire, dépositaire de nombreuses données potentiellement sensibles, devient en effet une cible privilégiée pour des attaques informatiques. Cet aspect du problème milite fortement en faveur d'une gestion des données personnelles directement par leurs propriétaires, de manière distribuée. De plus, ce protocole ne s'inquiète que de l'accès initial aux données et ne fournit aucun moyen pour assurer leur protection étendue. Enfin, les possibilités offertes à l'utilisateur de spécifier des propriétés techniques à vérifier pour qu'un fournisseur de service puisse accéder à telle ou telle partie de son profil personnel sont très limitées en termes d'expressivité. En effet, pour traiter réellement de protection des données personnelles, il faudrait pouvoir définir des politiques capables de se référer aux six axes définis précédemment.

— **Agents utilisateurs** - Certaines propositions émanant du domaine des systèmes multi-agents impliquent des agents artificiels[6] dans la protection des données personnelles des utilisateurs. Dans ce contexte, les agents désignent des entités logicielles capables d'interagir de manière autonome avec d'autres entités ainsi qu'avec l'environnement dans lequel elles sont situées. Ces agents peuvent être des briques logicielles destinées à mettre en œuvre les mécanismes de contrôle lors du processing. Ils peuvent également se présenter sous la forme d'agents mobiles et se déplacer avec les données. Ces agents sont des assistants logiciels au service d'un utilisateur placé au centre de l'application. Ces agents personnels ou agents utilisateurs sont alors chargés de surveiller et de contrôler l'utilisation qui est faite des données, de manière que cette utilisation reste conforme avec la politique établie […] Cette approche permet de répondre au problème majeur posé par la gestion déportée des données personnelles par une reprise de contrôle de l'utilisateur sur ses informations, tout en décentralisant les fonctionnalités de raisonnement dans des entités autonomes. Les agents utilisateurs permettent d'interfacer les relations entre l'utilisateur humain et les différents services et applications, en lui confiant la responsabilité de certaines décisions (*comme par exemple dans le cas du consentement a priori*). Dans cette perspective, c'est l'agent utilisateur qui met en œuvre les différents mécanismes (*principalement de contrôle d'accès)* assurant la sécurité des données personnelles de l'utilisateur.

[5] Lors du déroulement d'une transaction entre l'utilisateur et le fournisseur de service, l'utilisateur s'identifie auprès du serveur gestionnaire de son profil, qui en retour lui procure un certificat de session (qui servira de jeton d'accès temporaire). Ce certificat est ensuite transmis au service, qui le présente au gestionnaire de profil, accompagné d'une requête concernant le profil de l'utilisateur et d'un certificat de créance sur ses propres propriétés techniques. Le gestionnaire de profil valide le certificat de session et examine le certificat de créance. Si le gestionnaire est satisfait par ce certificat, c'est-à-dire si la correspondance entre la requête et les propriétés, quelles qu'elles soient, du fournisseur de service correspondent aux exigences connues de l'utilisateur, alors les informations de profil sont transmises au service.

III. CADRE JURIDIQUE DE PROTECTION DES DONNEES PERSONNELLES

La protection des données à caractère personnel et de la vie privée est très ancienne. Cependant, ce sont les moyens de protection qui ont changé. Au début, on s'intéressait à la protection de la vie privée tel que défini à la fin du XVIIIème siècle, notamment à travers la déclaration des droits de l'homme et du citoyen de 1789, où la protection de la vie privée n'avait pas trouvé sa place en tant que tel[43], Ce n'est qu'après la seconde guerre mondiale qu'on a admis une conception élargie des droits de l'homme grâce à l'apparition de l'Internet et du commerce électronique qui constituent une véritable menace pour les données à caractère personnel.

En effet, le commerce électronique est apparu avec les échanges des données informatisées utilisés entre les entreprises. La vie privée était protégée par des instruments juridiques généraux. C'est vers la fin des années 60 que l'exigence de la protection des données à caractère personnel est apparue. Elle est liée au développement de l'informatique et la crainte de voir les techniques informatiques peser lourdement sur les libertés publiques […] C'est l'Allemagne qui fut le premier pays en 1970 à adopter une loi relative à la protection des données à caractère personnel connue sous l'appellation de « *Land de Hesse* », une loi relative au « *traitement automatisé des informations nominatives* » [41]. Les Etats-Unis adoptent le "*Privacy Act*" qui ne concerne que les fichiers détenus par les administrations fédérales[33]. Ce n'est qu'en 1978 que la France s'est dotée d'une loi protégeant les données à caractère personnel, il s'agit de la loi Informatique et Liberté avant d'adopter la loi numéro 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique[21] et la loi de 6 août 2004.

Toutes ces lois témoignent de l'importance de la question des données à caractère personnel devant cette multitude de textes nationaux et internationaux, qui ont vocation à s'appliquer pour la protection de la vie privée de chaque internaute sur Internet. Ce qui revient à se poser une question rhétorique de savoir si le cadre de la protection juridique des données à caractère personnel en RDC est-il suffisamment efficace et protège-t-il rentablement les internautes congolais ? Autrement dit, cette partie se focalisera sur les textes juridiques en vigueur en RDC offrant une protection a priori a posteriori efficace par sa nature et sa pratique.

III.1. FONDEMENT DU DROIT DE LA PROTECTION DES DONNEES PERSONNELLES

En matière de droit de la protection des données personnelles, il existe irrémédiablement trois principes fondamentaux qui découlent des textes universels relatifs à la protection des données personnelles :

— **Le principe de légalité[6] -** La légalité étant le caractère de ce qui est légal, donc conforme au droit, aucun traitement sur une donnée personnelle ne saurait transgresser la loi qui s'y applique. En d'autres termes, pour qu'un traitement soit possible, il doit, d'abord avoir été défini par une loi qui en précise les modalités d'exécution.

— **Le principe de finalité –** Ce principe dispose que les données à caractère personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités mais que Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé

[6] « Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou L'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

dans le respect des principes et des procédures prévues et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées.

— **Le principe de proportionnalité -** Ce principe est mis en évidence pour énoncer qu'un traitement ne peut porter sur des données personnelles que si ces données sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs.

Toutefois, il est nécessaire de signaler qu'un traitement ne peut porter sur des données à caractère personnel s'il n'a, au préalable, reçu le consentement de la personne concernée, sauf si sa finalité est constituée par l'une des situations suivantes :

— Le respect d'une obligation légale incombant au responsable du traitement ;
— La sauvegarde de la vie de la personne concernée ;
— L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
— L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;
— La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée[3].

III.2. REGLEMENTATIONS UNIVERSELLES DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Le champ d'application matériel des textes règlementaires en matière de données personnelles englobe tous les traitements, automatisés (via des supports informatiques ou numériques) ou non automatisés (manuels), de données à caractère personnel qui sont contenues ou susceptibles d'être répertoriées dans des fichiers. Quant à leur champ d'application géographique, les textes en question ont vocation à lier tous les responsables de traitement situés sur le territoire nationale se rapportant aux données personnelles.

Il faut signaler, cependant, que ces règles s'appliquent même à un responsable de traitement non résident dans l'espace congolais, toutes les fois que ce responsable a recourt à des moyens de traitement situés sur le territoire national congolais, auquel cas il est fait obligation à ce « responsable établi à l'étranger » de désigner un représentant basé, lui, sur le territoire dont les moyens de traitement ont été utilisés[2]. Cela dit, les textes évoqués ci-haut concrétisent essentiellement quatre droits fondamentaux de la protection des données à caractère personnel :

— **Le droit à l'information -** On entend par le droit à l'information, le droit que possède la personne concernée dans une opération des informations satisfaisantes et pertinentes concernant l'utilisation de ses données personnelles. Ce droit précise ce qu'il faut informer au préalable, ce qui suit :

- la nature de données à caractère personnel concernée par le traitement ;
- les finalités du traitement des données à caractère personnel ;
- le caractère obligatoire ou facultatif de leur réponse ;
- les conséquences du défaut de réponse ;
- le nom de la personne physique ou morale bénéficiaire des données, ou de celui qui dispose du droit d'accès et 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 des données à caractère personnel ;

- la durée de conservation des données à caractère personnel ;
- une description sommaire des mesures mises en œuvre pour garantir la sécurité des données à caractère personnel ;
- le pays vers lequel le responsable du traitement entend, le cas échéant, transférer les données à caractère personnel » …

— **Le droit d'opposition -** Indépendamment de l'idée de transparence, le droit d'opposition renforce la maîtrise des individus de leurs données personnelles. Le droit d'opposition est donc le complément du droit à l'information. Une fois la personne est informée de la collecte, elle pourra par la suite, soit accepter soit s'opposer à ce que ses données soient collectées. Ainsi, l'article 42 de la Loi N ° 7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dispose que « *La personne concernée, 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 valables, légitimes et sérieuses, sauf dans le cas où le traitement est prévu par la loi ou exigé par la nature de l'obligation* ». Le droit d'opposition s'exerce donc, « *à tout moment au traitement des données* ». Il en découle que ce droit peut s'exercer avant la collecte des données étant donné que l'article 6 de la loi de 2004 considère, curieusement[19], la collecte des données comme un traitement. La plus importante remarque que soulève cet article est qu'il subordonne l'exercice du droit d'opposition à l'existence de raisons valables, légitimes et sérieuses. Puis, il prévoit deux exceptions dans lesquelles la personne concernée est privée de ce droit. Plus grave encore, la personne concernée est privée de son droit d'opposition[7] « *Dans le cas où le traitement est prévu par la loi ou exigé par la nature de l'obligation* ». L'article 44 ajoute « *le consentement n'est pas requis lorsque la collecte…auprès de la personne concernée 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* » […] Le droit d'opposition devra s'exercer d'une manière aisée et gratuite surtout si les données sont collectées à des fins de direct pour une action en ligne. En pratique, Le droit d'opposition, consacré aussi par la directive 95/46/CE, connaît un regain d'intérêt dans le cadre d'Internet qui multiplie les occasions de collecte de données et leur commercialisation.

— **Le droit d'accès et de communication -** L'article 32 de cette loi de 2004 dispose que « *Au sens de la présente loi, on entend par droit d'accès, le droit de la personne concernée, de ses héritiers ou de son tuteur de consulter toutes les données à caractère personnel la concernant, ainsi que 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 interdit. Le droit d'accès couvre 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* ».

La loi donne une définition si large au droit d'accès qu'elle confond avec le droit de rectification puisqu'elle définit le droit d'accès comme le droit de corriger les données à caractère personnel. En fait, la personne a même le droit d'obtenir une copie de ses données. […] Le fait de donner au droit d'accès un domaine large est, certes, en faveur de la personne concernée. Cette faveur est renforcée par l'article 33 qui dispose que « *On ne peut préalablement renoncer au droit d'accès* ». Cette position est confirmée par la doctrine qui considère que le droit d'accès constitue «*[…] la pierre angulaire de la protection des données* » [7] dans la mesure où il permet une maîtrise de la

[7] Les raisons légitimes signifient que ces raisons ne doivent pas être contraires à la loi et aux bonnes mœurs. Quant aux raisons sérieuses et valables, on ne voie pas de différence entre les deux. On peut les interpréter comme étant des raisons existantes et indispensables. En plus, ces raisons posent le problème de leur appréciation, ce qui nécessite le recours à l'Instance Nationale de protection des données personnelles en cas de litige conformément à l'article 43 de la loi 2004 ce qui signifie aussi de plus en plus de temps perdu. Il est regrettable que la loi ait multiplié les exceptions de telle façon, qu'il est légitime de craindre que le principe devienne exception et que l'exception devienne principe. Les deux dernières exceptions sont, en effet, inadmissibles. Il est évident que la collecte des données, en elle-même, n'affecte pas les intérêts légitimes de la personne. Ce sont, en fait, les opérations postérieures à la collecte qui sont dangereuses.

personne sur ses données. En l'occurrence, toute personne doit pouvoir obtenir communication de ses données qui doivent être conforme au contenue des enregistrements[38]. La loi de 2004 a réglementé également les procédures d'exercice du droit d'accès. Ce dernier s'exerce conformément à l'article 32 sur toutes les données à caractère personnel. Et même en cas de pluralité de traitants ou de sous-traitants, l'article 36 dispose que «*[…] lorsqu'il y a plusieurs responsables du traitement des données à caractère personnel ou lorsque le traitement est effectué par un sous-traitant, le droit d'accès est exercé auprès de chacun d'eux* ». Toutefois, l'article 35 de la loi consacre des limites à ce droit en disposant que « *La limitation du droit d'accès de la personne concernée, de ses héritiers ou de son tuteur aux données à caractère personnel la concernant n'est possible que dans les cas suivant :*

— *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 de la personne concernée que d'une façon limitée ;*

— *si le motif recherché par la limitation du droit d'accès est la protection de la personne concernée elle-même ou des tiers* ».

Ces exceptions sont dangereuses étant donné l'ambiguïté de leurs expressions. Or, qu'est-ce qu'une atteinte limitée à la vie privée ? Et qui a l'autorité de dire qu'il s'agit d'une atteinte limitée ? En plus, il est à craindre que la deuxième exception soit utilisée pour empêcher le droit d'accès. La loi a réglementé la procédure d'exercice du droit d'accès. D'abord, ce droit est exercé par la personne concernée, ses héritiers ou son tuteur. On en déduit que c'est un droit personnel. Ce qui a poussé à dire que c'est un droit de la personnalité. Cependant, ce droit « *peut être utilisé pour protéger des intérêts patrimoniaux* » [34]. Ensuite, la demande d'accès est présentée « *[…] par écrit ou par n'importe quel moyen laissant une trace écrite. La personne concernée, ses héritiers ou son tuteur peuvent demander de la même manière l'obtention de copie des données dans un délai ne dépassant pas un mois à compter de la dite demande* » [3]. La demande doit être adressée au responsable des traitements ou au sous-traitant, selon le cas. Ces derniers doivent « *mettre en œuvre les moyens techniques nécessaires pour permettre à la personne concernée, ses héritiers ou à son tuteur l'envoi par voie électronique de sa demande […]* ».

— **Le droit de rectification[8] -** Le droit d'accès ne trouve toute son efficacité que si la personne concernée pourrait rectifier ses données. C'est ainsi que l'article 40 de la loi 2004 dispose que «*La personne concernée, ses héritiers ou son tuteur, peut demander de rectifier les données à caractère personnel la concernant, les compléter, les modifier, les clarifier, les mettre à jour, les effacer lorsqu'elles s'avèrent inexactes, incomplètes, ou ambiguës, ou demander leur destruction lorsque leur collecte ou leur utilisation a été effectuée en violation de la présente loi…* » […] Ce texte donne au droit de rectification un domaine étendu et permet même d'assurer une maîtrise complète de la personne sur ses données. Mais, ce droit pose le problème de la preuve et de l'exactitude des données. Ce problème n'a pas échappé à la loi de 2004. En effet, l'article 39 dispose que « *En cas de litige sur l'exactitude des données à caractère personnel, le responsable du traitement et le sous-traitant doivent mentionner l'existence de ce litige jusqu'à ce qu'il soit statué*».

IV. RESULTATS ET DISCUSSIONS

IV.1. LES MESURES DE PROTECTION DE DONNEES PERSONNELLES

[8] Cependant, le droit de rectification instaure également une garantie d'exécution, en faveur de toute personne en droit d'exiger une rectification, puisqu'il est spécifié que *« Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent* ». L'alinéa 3 conforte cette garantie : Il indique, en effet, qu' « En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord ».

Sur le plan fonctionnel, la sécurité des données personnelles, dont sont garant le responsable de traitement, repose sur trois mesures :

— **La mesure préventive** - Elle consiste :

- à assurer la sécurité matérielle et technique des traitements pouvant être réalisés sur ces données par une évaluation des risques potentiels que présentent les modalités de traitement adoptées ;
- à s'assurer, une fois les risques identifiés, à mettre en œuvre des règles techniques et organisationnelles appropriées pour empêcher aussi bien l'altération, la perte ou la destruction des données que toute forme illicite de traitement.

— **La mesure procédurale obligatoire** - Cette mesure ordonne à tout responsable de traitement et / ou à son sous-traitant de notifier à l'autorité de contrôle de toute violation de données personnelles, au plus tard, 24 heures après en avoir pris connaissance ; Cette notification répond à deux exigences :

- Il faut que le contenu de la notification ait été au préalable défini (déclinaison du principe de la légalité des infractions et des peines qui veut qu'un magistrat ne puisse appliquer une peine qui n'ait déjà été prédéfinie par la Loi) ;
- la trace documentaire de ladite violation doit être conservée (en guise de justificatif ou preuve).

— **La mesure informative** - La personne dont la ou les données ont été violées ayant légitimement le droit de savoir que ses données, l'autorité de contrôle, une fois qu'elle a reçu la notification de la violation dénoncée, peut imposer que soit informée la personne concernée. Là également, la communication doit sacrifier à la condition que son contenu ait été prédéfini. Mais dans le cas où elle dispose des preuves que des mesures de protection technologiques appropriées ou mesures correctives été appliquées aux données et que ces dernières ont effectivement recouvré leur intégrité, l'autorité de contrôle peut juger non nécessaire la communication de la violation à la personne concernée.

VI.2. PRISE EN CHARGE DE LA VIOLATION DES DONNEES PERSONNELLES

Avant de parler de quelconque prise en charge de la violation des données personnelle, il est nécessaire de faire allusion tout d'abord aux personnes impliquées dans cette violation des données. La violation n'est envisageable que dans le cadre de la fourniture au public de services de communications électroniques, ce sont les fournisseurs de services de communications électroniques au public qui sont visées par une quelconque violation des données personnelles. Il s'agit en premier chef des opérateurs de communications électroniques, qui, rappelons-le, offrent des services de téléphonie fixe ou mobile, acheminent des données et fournissent l'accès à internet à travers des réseaux fixes, mobiles et satellitaires. Mais les dispositions des lois de protection des données à caractère personnel précitées ne nous permettent pas d'écarter une autre catégorie d'acteurs, notamment les fournisseurs de services de communication au public en ligne ; il s'agit, par exemple :

— des éditeurs de services de vidéos à la demande ;
— des exploitants de plateformes de jeux en ligne ;
— des exploitants de réseaux sociaux (LinkedIn, Facebook, Twitter, etc.) ;
— des éditeurs de journaux et programmes télévisés en ligne.

Mais il s'agit, également, par extension, de certains professionnels dont les activités nécessitent qu'ils collectent forcément des données personnelles de leurs clients, tels que :

— les banquiers ;
— les assureurs des services (cours et tribunaux, universités, etc.) ;

— et les autres entités privées qui exploitent d'une manière ou d'une autre des réseaux informatiques sur lesquels sont soit acheminés soit archivés des données personnelles.

Sur la base des informations fournies ci-haut, il est évident que les responsables de traitement ne sont donc pas directement concernés. Mais cela suffit-il à en déduire qu'ils ne peuvent, en aucun cas, être responsables d'une violation de donnée personnelle ? […] Néanmoins, nous nous posons tout de même la question de savoir si un responsable de traitement, qui, par définition détermine les finalités et les moyens des traitements et doit en principe être d'une probité à toute épreuve, ne pourrait être amené, pour raison quelconque, à se rendre coupable d'une violation de donnée à caractère personnel consistant, par exemple, en une divulgation non autorisée d'information à caractère secret. Cette question rhétorique trouve sa réponse, au faites que ce dernier est indirectement compromis au regard des connaissances misent à sa disposition lors du premier contact avec les données à caractère personnel de la personne concernée.

Après avoir fait l'ébauche des personnes impliquées dans la violation des données à caractère personnel, il est dorénavant temps, d'aborder les suppliques d'une éventuelle prise en charge des violations des données par les entreprises. La prise en charge des violations de données personnelles ne se fait seulement après coup, une fois l'acte consommé ; ainsi, la prise en charge vise tout simplement à créer un cadre et des procédures propices à leur évitement.

Retenons que la prise en charge commence tout d'abord par entreprendre un certain nombre d'actions (mesures) à entreprendre pour éviter ou réduire les risques de violations. Bien entendu, ces actions doivent en principe empêcher la commission de la moindre violation au sein d'une entreprise ou d'une administration, comme par exemple :

— Informer par tout moyen et tout support (notes, circulaires, réunions) la personne responsable de l'état du droit (conséquences) et de l'état de l'art sur les données personnelles ;

— Réaliser un audit juridique et technique des procédures de protection des données personnelles de l'entreprise en prévoyant des mesures de correction.

Ensuite, la prise en charge passe à sa deuxième phase, celle de la gestion de la violation proprement dite. Ainsi, une fois qu'une violation de données s'est révélée au sein d'une entreprise ou d'une entité quelconque, les personnes compétentes doivent au plus vite procéder à :

— Un inventaire des données violées ;

— La transmission de l'inventaire à l'organe de protection des données personnelles en charge dans le pays ;

— Mettre en place un outil et une méthodologie de remontée toutes informations pertinentes et d'alertes.

Enfin, la troisième phase de la prise en charge consiste à proposer les sanctions à la non-information des personnes concernées et aux traitements irréguliers. Des sanctions pécuniaires très sévères peuvent être appliquées aux entreprises se livrant à une obstruction, une dissimulation ou une rétention d'éléments constitutifs de violation de données à caractère personnel. C'est ainsi qu'une entreprise qui ne met pas en place, en son sein, un service de « *Droit d'accès* », qui ne répond pas à des demandes légitimes formulées par des personnes (ses employés), notamment se sachant ou se pensant sujettes à un traitement illicite de données personnelles ou qui exige, en contrepartie de réponses aux demandes qui lui sont faite, de percevoir des frais pour les réponses aux informations demandées, s'expose à une amende pouvant aller jusqu'à 0,5 % de son chiffre annuel, encore plus dissuasives, une amende de 1 % de son chiffre d'affaires annuel peut être infligée à toute entreprise qui se livrerait à l'un des manquements suivants à l'endroit des personnes vis-à-vis desquelles elle n'a pas été diligente par rapport à leurs demandes telles que :

— Défaut d'information, transmission d'informations incomplètes ou non suffisamment transparentes ;
— Empêchement, entrave, obstruction d'accès, défaut de rectification des données, défaut de communication des informations aux destinataires ;
— Non-respect du droit à l'oubli numérique ou de l'effacement de données ;
— Défaut de communication de copie des données sous forme électronique ;
— Défaut de mise à jour de la documentation intéressant les personnes concernées ou transmission de données non mises à jour ;
— Défaut de définition insuffisante des obligations des responsables conjoints.

Le plus haut degré dans l'échelle des sanctions, portant le niveau d'amende à l'encontre de toute entreprise défaillante ou négligente en matière de protection des données à caractère personnel est de 2 % de son chiffre d'affaires annuel, et est réservé aux manquements les plus graves, tels que :

— Les traitements de données effectués soit sans base juridique, soit obtention du consentement des personnes auxquels ils se rapportent ;
— Les traitements de catégories particulières de données (données sensibles, par exemple) en violation des dispositions légales et règlementaires ;
— Le non-respect d'une opposition formulée par une personne concernée ;
— Le non-respect des conditions du profilage ;
— Le non-respect des obligations ;
— L'absence de désignation d'un représentant ;
— Les traitements des données en violation du règlement ;
— L'omission de signaler ou notifier une violation de données ou l'inexécution, en temps utile, d'une mesure corrective ;
— L'absence de réalisation d'une analyse d'impact ;
— L'absence de désignation d'un délégué à la protection des données ;
— Le fait de réaliser ou de donner l'instruction de réaliser un transfert vers un pays non autorisé ;
— Le non-respect de l'obligation de répondre à l'autorité de contrôle.

VI.3. LES PÉRIMÈTRES RÈGLEMENTAIRES DE LA VIE PRIVEE

VI.3.1. LES PRINCIPES RELATIFS AU TRAITEMENT DE DONNÉES

Avant d'engager un traitement des données et lorsque celui-ci contient des données à caractère personnel, le responsable du traitement doit s'engage dans un examen approfondi sur plusieurs facettes :

— **La licéité du traitement (le fondement du traitement)** – ici, le responsable du traitement de données doit vérifier si le cadre de traitement est licite c'est-à-dire, respecte l'une des conditions ci-après :
  - La personne a consenti au traitement de ses données ;
  - Le traitement est fondé sur une base légale ;
  - Le traitement est lié à l'exécution d'un contrat ;
  - Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne ;
  - Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ;
  - Le traitement répond à un intérêt légitime pour le responsable de traitement.

— **La finalité du traitement** – ici, le responsable de traitement de données vérifie s'il y a une correspondance spécifique entre l'objectif poursuivi et les missions de l'établissement de l'entité.

— **La pertinence et la proportionnalité des données** – ici, le responsable de traitement de données vérifie s'il y a une exclusive corrélation avec les finalités.

— **La sécurisation et la protection des données** – ici, le responsable de traitement est tenu de prendre toutes les dispositions pour protéger les données et empêcher qu'elles soient détournées, réutilisées à des fins non prévues, afin de respecter l'intégrité et la confidentialité des données.

— **La conservation limitée des données** – ici, le responsable de traitement de données doit rassuré que les données ne peuvent être conservées que pour une durée prédéfinie et limitée ; la finalité du traitement détermine la durée de conservation. A l'issue du traitement, les données sont soit anonymisées soit conservées pour une réutilisation ultérieure à des fins de recherche scientifique uniquement.

— **La transparence des informations sur l'utilisation des données** – Les informations qui portent sur la finalité du traitement, le nom et les coordonnées du responsable du traitement, le nom et les coordonnées du délégué à la protection des données, les durées de conservation sont communiquées en toute transparence aux personnes concernées par le responsable du traitement des données.

Outre ces principes du traitement des données, il s'agit de s'assurer du respect du fondement de la protection des données personnelles afin de conduire sa recherche.

VI.3.2. ANALYSE D'IMPACT SUR LA VIE PRIVÉE

Cette analyse permet d'évaluer le risque d'un traitement de données sur la vie privée des personnes concernées. L'analyse est réalisée par le responsable du traitement de la protection des données et le responsable de la sécurité des systèmes d'information. Elle est obligatoire lorsque le traitement est susceptible d'engendrer des risques élevés et doit particulièrement être réalisée dès lors que le traitement remplit au moins deux des critères de la liste énumérée ci-dessous :

— Surveillance automatique ;
— Données sensibles ;
— Traitement à grande échelle ;
— Croisement de données ;
— Personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
— Evaluation/scoring (y compris profilage) ;
— Décision automatique avec effet légal ;
— Usage innovant ou utilisation NTIC ;
— Exclusion du bénéfice d'un droit, d'un contrat ;
— Etc.

CONCLUSION

Avec la multiplication des dispositifs de mise en relation et le développement des applications informatiques, la question de la protection des données à caractère personnel a émergé en parallèle à la question de l'exploitation frauduleuse de ces données par les entreprises concurrentes et/ou par des pirates afin d'une utilisation abuse, d'un éventuel chantage et d'une possible atteinte à la vie privée. Dans la présente recherche, il a été question de présenter et discuter les contours de la sphère privée et de la protection des données à caractère personnel en relation avec les TIC tel qu'il apparaît au quotidien, et notamment dans les réglementations opposables internautes en République Démocratique du Congo. Nous avons ainsi limité notre champ d'application à la protection des données personnelles en informatique en nous basant sur un cadre juridique de protection approprié aux internautes congolais.

Par ailleurs, la protection de la vie privée est devenue l'une des préoccupations majeures des utilisateurs partout dans le monde et en RDC, particulièrement, ce qui nous a motivés à traiter ce sujet sur plusieurs niveaux, touchant ainsi les différentes phases de cycle de vie des données circulants sur Internet. Ainsi, face aux manques des solutions de représentation de la législation congolaise et de sa mise en application selon les contextes d'usage des données, notre première contribution a été de déterminer un cadre contextuel portant sur la protection des données à caractère personnel, qui nous a permis d'exprimer des politiques de protection des données personnelles et les préférences d'utilisateur suivant les axes législatifs tels que l'information de l'utilisateur, son consentement, sa capacité à accéder aux données et à les modifier, la justification de la collecte et du traitement, la conservation des données et enfin leur transmission à des tiers.

Ensuite, l'application de ces politiques de protection a été rendue possible par la définition d'un cadre juridique de contrôle d'accès aux données personnelles, qui est une extension de la structure de contrôle d'accès classique. Cette structure inclut des modules destinés à la gestion de la protection des données personnelles en termes de contrôle d'usage et de négociation.

Par conséquent pour que ces politiques appliquées soient adaptées au contexte de chaque correspondance électronique, nous avons également déterminé une référence symptomatologique qui prend en compte la nature des données personnelles en question, leurs destinataires potentiels, et leur usage en cours. Cette référence symptomatologique formalisée par une ontologie favorise la prise en compte et le traitement des informations liées aux entités de chaque contexte transactionnel. Cette conception va premièrement favoriser le partage d'un vocabulaire commun de connaissances entre les utilisateurs et les responsables de traitement. Ensuite, l'adaptation dynamique au contexte situationnel de chaque transmission pourra permettre l'adéquation à la génération de politiques de protection sensibles au contexte. Enfin, elle va favoriser l'analyse à différents niveaux d'abstraction des politiques de protection des données, en s'appuyant sur les éléments de base tels que la nature des données personnelles à traiter, leur destination et les contraintes d'usage qui s'appliquent sur elles.

REMERCIEMENTS

L'équipe du présent projet de recherche tient à exprimer sa profonde gratitude envers tous ceux qui ont permis de parachever cette nouvelle prospection, en l'occurrence des différentes entreprises et internautes congolais. L'équipe tient également à remercier spécialement le responsable de ce projet le Professeur Docteur YENDE Raphael Grevisse, dont la contribution s'est avérée plus que satisfaisante lors de la rédaction et de l'interprétation des aboutissements de la présente recherche.

REFERENCES

[1] A.F. Westin, "*Privacy and freedom*", New York USA, 1967

[2] Article 5, « *de la Loi N ° 7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Modifié par Loi n°2004801 du 6 août 2004 art.* », JORF 7 août 2004

[3] Article 7, « *Loi I & L Modifié par Loi n°2004-801 du 6 août 2004 art.* », JORF 7 août 2004

[4] Burkina Faso, « *Loi N° 010-2004/an portant protection des données à caractère personnel* », 2004

[5] Côte d'Ivoire, « *Loi N ° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel* », 2013

[6] D.F. Ferraiolo, R. Sandhu, S. Gavrila, D.R. Kuhn, and R.C, "*Proposed NIST Standard for Role-Based Access Control*", ACM TISSEC, 2001

[7] D.MARTIN, « *La directive 95/46/CE (protection des données) et sa transposition en droit français* », Gaz. Pal., 1998, 1er sem., p.608.

[8] Daniel J Solove, "*A taxonomy of privacy*", vol. 154, page 477, Hein-Online, 2006

[9] Décret N ° 2010-150 du 06 juillet 2010 *portant création, organisation et fonctionnement de l'Agence Nationale du Registre des Populations et des Titres Sécurisés* (ANRPTS)

[10] Décret N ° 2011-929 du 29 juin 2011 *modifiant le décret ~ 2009 -392 du 20 avril 2009 portant nomination des membres de la commission de protection des données à caractère personnel*, 2009

[11] Décret N ° 2012-934 du 19 septembre 2012 *portant organisation et fonctionnement de l'autorité de régulation des Télécommunications/TIC* de Côte d'Ivoire, 2012

[12] DELEUZE G., « *Post-scriptum sur les sociétés de contrôle* », dans Pourparlers (1972-1990), Paris, Minuit, pp. 240-247.

[13] Directive *n° 99/93/CE, JOCE 19 janvier 2000,* n° L. 13/12.

[14] France, « *Loi n° 7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Version consolidée au 23 avril 2016)* », 2016

[15] G. Karjoth and M. Schunter, "*A privacy policy model for enterprises*", IEEE Computer Security Foundations Workshop IEEE, IEEE Computer Society Press, 2002

[16] G. Müller, "*Introduction of privacy and security in highly dynamic systems*", Communicat of the ACM, p49, 2006

[17] Gregory Neven, "*A quick introduction to anonymous credentials*", 2008

[18] Guillaume PIOLLE, « *Protection des données personnelles dans le système d'information* », Centrale Supélec / Inria, équipe CIDRE, 2018.

[19] H.MAISL, « *Etat de la législation française et tendance de la jurisprudence relatives à la protection des données personnelles* », R.I.D.C. 3. 1987. P.577

[20] ISO/IEC, "*Information technology - security techniques - evaluation criteria for it security, part 2: Security functional requirements*". Technical Report 15408-2, ISO, 1999.

[21] J.O., n°143 du 22 juin 2004, p.11168, texte n°2, disponible sur : http://www.Legifrance.gouv.fr. ; voir également : L. GRYNBAUM, « Projet loi pour la confiance dans l'économie numériques et un petit effort et rigueur juridique pour un contrat électronique fiable », D., 2003, n°11, p.746.

[22] Jan Henrik Z, Oscar Garcia M & Klaus W, "P*rivacy in the Internet of Things: threats and challenges"*, vol. 7, no. 12, pages 2728–2742, Wiley Online Library, 2014.

[23] Jinrong Bai & Junfeng Wang, "*Improving malware detection using multi-view ensemble learning*", vol. 9, no. 17, pages 4227–4241, Wiley-Online Library, 2016.

[24] June Jamrich P, « *Nouvelles Perspectives sur les concepts informatiques* », Course Technology Press, 2015.

[25] Juniper : Détails techniques sur Wanna- Cry. *https://www.informatiquenews.fr/juniper-details-techniques-wannacry-51980, 2017*, consulté 14 mars 2020.

[26] K Wang, R Chen, BC Fung & PS Yu, "*Privacy-preserving data publishing: A survey on recent developments*", ACM Computing Surveys, 2010

[27] Kheira Dari Bekara, « *Protection des données personnelles côté utilisateur dans le e-commerce* », Institut National des Télécommunications, 2012.

[28] Kukic Ado, "*The definitive guide to single sign on*", Auth0, 2016

[29] Mamadou Alpha KANE, « *Données à caractère personnel et communications électroniques en Mauritanie : Une régulation par l'autorité de régulation multisectorielle ou par une autorité administrative indépendante* », ARCEP, 2016

[30] Marit H, Ari S & Alissa C, "*Privacy and identity management*", vol. 6, no. 2, IEEE, 2008

[31] Mauritanie, « *Loi N ° 2011-003 du 12 janvier 2011 abrogeant et remplaçant la Loi N ° 96-019 du 19 juin 1996 portant Code de l'Etat Civil* », 2011

[32] Mauritanie, « *Loi N ° 2013-025 du 15 juillet 2013 portant sur les communications électroniques* », 2013

[33] M-P.F-TROUSSEAU et G.HAAS, *« Internet et protection des données personnelles* », Paris, Litec, 2000,

[34] P. ANCEL, « *La protection des données personnelles aspects de droit privé français* », R.I.D.C., 3-1987

[35] Parlement Européen, « *Guide de la protection des données à caractère personnel* », Paris, 2008.p.36.

[36] Raymond CWW, Jiuyong Li, Ada WCF & Ke Wang, "*anonymity: an enhanced k-anonymity model for privacy preserving data publishing*", In Proceedings of the 12th international conference on Knowledge discovery and data mining, pages, 2006.

[37] S. Baase A, "*Social, Legal, and Ethical Issues in Computing*", Prenctice-Hall. 2003

[38] S.GUINCHARD, M.HARICHAUX et R. de TOURDONNET, « *Internet pour le droit : connexion- recherche droit* », Paris, 2ème éd., MONTCHRESTIEN, E.J.A., 2001, p.176.

[39] Sénégal, « *Loi n° 2008 – 12 sur la Protection des données à caractère personnel* », 2008

[40] The European Parliament and the Council, *Directive 1995/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; In European Union,* editor, Official Journal of the European Communities, October 1995

[41] U.BRUHANN, « *La directive européenne relative à la protection des données : fondement, histoire, points forts* », R.F.A.P., n°89, 1999.

[42] WISSEM JARRAYA, « *La protection des données personnelles dans le commerce électronique* », Rapport de recherche, Faculté de droit de Sfax, 2013

[43] X. AGOSTINELLI, « *Le droit à l'information face à la protection civile de la vie privée* », Paris, Librairie de l'Université, 1994, p. 88

[44] Y. Deswarte, et C.A. Melchor, « *Sécurité des Systèmes d'Information, sur Technologies de Protection de la Vie Privée sur Internet* », Hermès, Paris. France. 2006.